Bundesministerium
für Wirtschaft
und Energie

Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie

IT-Sicherheit für die Industrie 4.0

Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten

Abschlussbericht

Impressum

Herausgeber
Bundesministerium für Wirtschaft
und Energie
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Gestaltung und Produktion
PRpetuum GmbH, München

Stand
Januar 2016

Zertifikat seit 2002
audit beruf**und**familie

Das Bundesministerium für Wirtschaft und Energie ist mit dem audit berufundfamilie® für seine familienfreundliche Personalpolitik ausgezeichnet worden. Das Zertifikat wird von der berufundfamilie gGmbH, einer Initiative der Gemeinnützigen Hertie-Stiftung, verliehen.

Diese und weitere Broschüren erhalten Sie bei:
Bundesministerium für Wirtschaft und Energie
Referat Öffentlichkeitsarbeit
E-Mail: publikationen@bundesregierung.de
www.bmwi.de

Zentraler Bestellservice:
Telefon: 030 182722721
Bestellfax: 030 18102722721

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

4PL	Viert-Partei-Logistik (englisch Fourth-Party-Logistics)
AAA	Authentication, Authorization, Accountig
AES	Advanced Encryption Standard
ANSI	American National Standards Institute (USA)
ASP	Application Service Providing
AVA	Ausschreibung, Vergabe und Abrechnung
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BMBF	Bundesministerium für Bildung und Forschung
BMI	Bundesministerium des Innern
BMWi	Bundesministerium für Wirtschaft und Energie
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAN	Controller Area Network (Industriebussystem)
CC	Common Criteria
CEN	Comité Européen de Normalisation
CISPA	Cyber Intelligence Sharing and Protection Act
CPMS	Corrugated Packaging Management System
CPPS	Cyber Physical Production System
CPS	Cyber Physical Systems
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DFD	Datenflussdiagramm
DFKI	Deutsches Forschungszentrum für Künstliche Intelligenz
DIN	Deutsches Instutut für Normung
DKE	Deutsche Kommission Elektrotechnik Elektronik Informationstechnik
DMZ	Demilitarisierte Zone (in IT-Netzen)
DoS	Denial of Service
DRM	Digital Rights Management
EBCA	TeleTrusT European Bridge CA
ENISA	Europäische Agentur für Netz- und Informationssicherheit (englisch: European Network and Information Security Agency)
EOS	End of support; auch End of service
ERM	Enterprise Rights Management
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute
EU	Europäische Union

EWR	Europäischer Wirtschaftsraum
FDI	Field Device Integration
GATS	Allgemeines Abkommen über den Handel mit Dienstleistungen (englisch: General Agreement on Trade in Services)
GATT	Allgemeines Zoll- und Handelsabkommen (englisch: General Agreement on Tariffs and Trade)
GMA	Gesellschaft Mess- und Automatisierungstechnik
GUI	Graphical User Interface
HMI	Human-Machine Interface
I4.0	Industrie 4.0
IACS	Industrial Automation and Control System
ICS	Industrial Control System
IdM	Identity Management
IDMS	Identity Management System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIC	Industrial Internet Consortium
IIRA	Industrial Internet Reference Architecture
IITU	International Telecommunication Union
IoS	Internet of Services
IoT	Internet of Things
IP	Internet Protocol
IPP	Intellectual Property Protection
IPS	Intrusion Prevention System
IRM	Industrial Rights Management
ISA	International Society of Automation
ISA99	ISA Komitee für „Industrial Automation and Control Systems (IACS) Security“
ISMS	Informationssicherheits-Managementsystem
ISO	International Organization for Standardization
IT	Informationstechnik
ITU	International Telecommunication Union
KMU	Kleine und mittlere Unternehmen
LAN	Local Area Network
LIN	Local Interconnect Network
MaRisk	Mindestanforderungen an das Risikomanagment
MES	Manufacturing Execution System
MITRE	Massachusetts Institute Of Technology Research And Engineering
MOS	Media Oriented Systems (Industriebussystem)
NDA	Non Disclosure Agreement (Vertraulichkeitsvereinbarung)

NIST	National Institute of Standards and Technology (USA) (deutsch: Nationales Institut für Standards und Technologie)
NVD	National Vulnerability Database
OASIS	Organization for the Advancement of Structured Information Standards
OPC	ursprünglich: Object Linking and Embedding for Process Control; heute interpretiert als: Openness, Productivity and Connectivity oder Openness Productivity and Collaboration
OPC DA	OPC Data Access
OPC UA	OPC Unified Architecture
OSGi	Open Services Gateway initiative
PAT	Process Analytical Technology
PAuswV	Personalausweisverordnung
PCS	Process Control System, PCS
PGP	Pretty Good Privacy
PI	Profinet International
PKI	Public-Key-Infrastruktur (englisch: Public Key Infrastructure)
PLC	Programmable Logic Controller (= SPS)
PLIM	Production Line IT Security Monitoring
PLS	Prozessleitsystem, engl. Distributed Control System, DCS oder Process Control System, PCS
RAMI 4.0	Referenzarchitekturmodell Industrie 4.0
RDP	Remote Desktop Protocol
RFID	Radio-frequency identification
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SCADA	Supervisory Control and Data Acquisition
SDL	Specification and Description Language
SigG	Signaturgesetz
SigV	Signaturverordnung
SLA	Service Level Agreement
SOA	Serviceorientierte Architektur (englisch: service-oriented architecture)
SOC 2	Service Organization Control 2
SPS	Speicherprogrammierbare Steuerung (= PLC)
SSL	Secure Sockets Layer
SSPS	Speicherprogrammierbare Steuerung in Software – Software-SPS oder Soft-SPS
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of privilege
SW	Software
TBINK	Technischer Beirat internationale und nationale Koordinierung der DKE
TCG	Trusted Computing Group
TCP	Transmission Control Protocol
TeleTrusT	TeleTrusT – Bundesverband IT-Sicherheit e.V.
TLS	Transport Layer Security

TMG	Telemediengesetz
TPM	Trusted Platform Module
USB	Universal Serial Bus
VDA	Verband der Automobilindustrie
VDE	Verband der Elektrotechnik, Elektronik und Informationstechnik
VDI	Verein Deutscher Ingenieure
VLAN	Virtual Local Area Network
VM	Virtuelle Maschine
VPN	Virtual Private Network
WLAN	Wireless LAN
WTO	World Trade Organization
WWW	World Wide Web
XML	Extended Markup Language
ZVEI	Zentralverband Elektrotechnik- und Elektronikindustrie

Hinsichtlich juristischer Abkürzungen wird auf das Abkürzungsverzeichnis[1] von Jura-Companion.de verwiesen.

1 Jura-Companion.de, Juristische Abkürzungen – Abkürzungsverzeichnis, http://jura-companion.de/abkuerzungsverzeichnis/juristische-abkuerzungen.html, zuletzt abgerufen am 16.12.2015.

Autoren

Autoren-Kernteam
Dr. Daniel Bachlechner, Fraunhofer ISI
Dr. Thorsten Behling, WTS Legal Rechtsanwalts-gesellschaft mbH
Esther Bollhöfer, Fraunhofer ISI
Thomas Dexheimer, Fraunhofer SIT
Prof Dr. Georg Borges, Universität des Saarlandes
Michael Gröne, Sirrix AG
Peter Handel, Fraunhofer ESK
Dr. Thorsten Henkel, Fraunhofer SIT
Jana Post, WTS Legal Rechtsanwaltsgesellschaft mbH
Michael Stiller, Fraunhofer ESK
Gerhard Sutschet, Fraunhofer IOSB
Dr. Thomas Usländer, Fraunhofer IOSB
Michael Voeth, Robert Bosch GmbH
Heiko Weber, Software AG
Andreas Wigger, WTS Legal Rechtsanwalts-gesellschaft mbH

Review-Beteiligte
Dr. Detlef Hühnlein, ecsec GmbH
Jens Mehrfeld, Bundesamt für Sicherheit in der Informationstechnik
Dr. Norbert Schirmer, Sirrix AG
Prof. Dr. Jörg Schwenk, Ruhr-Universität Bochum/ Horst Görtz Institut für IT-Sicherheit (HGI)
Christian Stüble, Sirrix AG

Expertenbeirat

Stefan Bauer, WITRON Logistik + Informatik GmbH
Klaus Bauer, TRUMPF Werkzeugmaschinen GmbH + Co. KG
Alfons Botthof, VDI/VDE Innovation + Technik GmbH
Wolfgang Dorst, BITKOM
Andreas Dümmler, ARBURG GmbH + Co KG
Tobias Gschwend, Otto Bihler Maschinenfabrik GmbH & Co. KG
Andreas Harner, DKE/VDE
Karl Haug, Felss Systems GmbH
Steffen Heyde, TeleTrusT – Bundesverband IT-Sicherheit e.V.
Stefan Hoppe, OPC Foundation
Dr. Detlef Houdeau, Infineon Technologies AG
Dr. Lutz Jänicke, Innominate Security Technologies AG
Benjamin Jurke, DMG Mori GmbH
Dr. Wolfgang Klasen, Siemens AG
Lukas Klotz, DMG Mori GmbH
Markus Preisinger, Felss Systems GmbH
Siegfried Schülein, infoteam Software AG
Martin Schwibach, BASF SE
Dr. Inessa Seifert, VDI/VDE Innovation + Technik GmbH
Dr. Walter Speth, Bayer Technology Services GmbH
Christian von Rützen, Dachser GmbH & Co. KG
Richard Wagner, Otto Bihler Maschinenfabrik GmbH & Co. KG

Vorbemerkungen

Die Verwendung des Begriffes „Sicherheit“ meint im Kontext der Studie immer IT-Sicherheit (englisch: (IT-)„security“) und nicht die deutsche Übersetzung des englischen Wortes „safety“.

Alle Personenbezeichnungen in der vorliegenden Studie beziehen sich ungeachtet ihrer grammatikalischen Form in gleicher Weise auf Frauen und Männer.

Management Summary

Hintergrund der Studie

Die Vision von Industrie 4.0 (kurz I4.0) beschreibt eine neue Art der wirtschaftlichen Produktion, die durch eine durchgängige Digitalisierung und die stärkere innerbetriebliche sowie überbetriebliche Vernetzung geprägt ist. Für die Zuverlässigkeit solcher Systeme und zum Schutz sensibler Unternehmensdaten ist ein hohes Maß an IT-Sicherheit unabdingbar. Der Schutz vor Cyberattacken betrifft neben einzelnen Teilnehmern ganze Wertschöpfungsnetzwerke, die vielfach global organisiert sind. IT-Sicherheit wird, als eine Dimension der Produktqualität der in Deutschland produzierenden Unternehmen, der entscheidende „enabling" Faktor für die Umsetzung der Vision „Industrie 4.0" sein.

Ziel der Studie

Das Bundesministerium für Wirtschaft und Energie (BMWi) hat ein interdisziplinäres Expertenteam[2] unter Leitung der Sirrix AG security technologies beauftragt, zusammen mit einem Expertenbeirat aus der Industrie die unterschiedlichen Themenfelder der IT-Sicherheit für die Industrie 4.0 im Kontext von neuen globalisierten Wertschöpfungsnetzwerken zu untersuchen. Erstmalig stellt diese Studie konkrete Handlungsvorschläge für Adressaten aus Politik, Industrie und Standardisierungsgremien vor, die aus aktuellen, tatsächlich vorhandenen Fallbeispielen verschiedener Branchen[3] abgeleitet wurden. Dabei werden die bisher bestenfalls punktuell und disjunkt betrachteten Themenfelder Technik, Organisation und Recht ganzheitlich und auf einander abgestimmt betrachtet und bewertet. Auf Basis der Fallbeispiele und einer Bedrohungs-/Risikoanalyse wurden Handlungsvorschläge, für Unternehmen, Branchenverbände, Standardisierungsorganisationen sowie zur Ausrichtung der Wirtschafts-, Technologie- und Förderpolitik, aufgezeigt. Ein wichtiger Fokus der Studie liegt auf spezifischen Herausforderungen – auch in politischer Hinsicht – bei internationalen Datentransfers und länderübergreifenden Kooperationen.

Zielgruppe der Studie

Die Studie richtet sich an alle interessierten Personen aus dem Bereich der industriellen Produktion und wurde so verfasst, dass insbesondere Personen außerhalb des Fachexpertenkreises alle Informationen verstehen können. Als Zieladressatenkreis werden Entscheider in Unternehmen (insb. KMU) und Branchenverbänden, in Wirtschafts-, Technologie- und Förderpolitik, beim Gesetzgeber und in Aufsichts- und Regulierungsbehörden sowie in Standardisierungs- und Normierungsorganisationen erachtet. Die Politik ist insbesondre hinsichtlich ihrer Rolle in der notwendigen Moderation von Verhandlungsprozessen, bei der Förderung und der Gesetzgebung adressiert.

Überblick über wesentliche Ergebnisse

Risiken/Herausforderungen

Neue Risiken und Herausforderungen ergeben sich aus den folgen drei Kerneigenschaften von I4.0:

1. Die Vernetzung von Industrieanlagen und deren Komponenten wird künftig nicht nur organisations- und länderübergreifender, sondern vor allem auch dynamischer stattfinden als bisher. Um die IT-Sicherheit zu gewährleisten, muss eine belastbare Grundlage von Vertrauen und Verlässlichkeit geschaffen werden, die sich über alle Teilnehmer der Wertschöpfungsnetzwerke erstreckt.

2. Die Menge an Daten, die von einem Teilnehmer einem anderen Teilnehmer aus funktionalen Gründen absichtlich mitgeteilt oder zugänglich gemacht werden, nimmt zu. Darunter befinden sich auch solche Daten, die nicht nur aus Sicht eines einzelnen Unternehmens als Geschäftsgeheimnis gelten, sondern an die aufgrund staatlicher Gesetze eine besonders hohe Anforderung an die Vertraulichkeit besteht.

2 Sirrix AG, Fraunhofer Gesellschaft e.V. (Institute ESK, IOSB, ISI, SIT), Software AG, Robert Bosch GmbH, WTS Legal Rechtsanwaltsgesellschaft mbH, Prof. Dr. Georg Borges (Universität des Saarlandes), ecsec GmbH und Prof. Dr. Jörg Schwenk (Ruhr-Universität Bochum/HGI) und assoziierte Partner Bundesamt für Sicherheit in der Informationstechnik (BSI) und TeleTrusT – Bundesverband IT-Sicherheit e.V.

3 Fallbeispiele: „Automobilbau – Inbetriebnahme produktionsrelevanter Echtzeitsysteme unter Zeitdruck", „Anlagen-/Maschinenbau – Fernwartung", „Chemische Industrie – Netzwerksegmentierung in der Produktion", sowie „Grenzüberschreitende Logistik-Prozesse – Integration von Logistikprozessen".

3. Entscheidungen werden bei I4.0 zunehmend von autonomen Systemen getroffen. Diese IT-Sicherheitsrelevanten Entscheidungen und die daraus resultierenden Änderungen von Abläufen und Teilnehmer-Konfigurationen können sich aufgrund von Ereignissen aus unterschiedlichsten Domänen und Partnersystemen ergeben sowie aus der Analyse von Daten aus unterschiedlichsten Quellen.

Maßnahmen, Hemmnisse und neue Konzepte

Vorhandene technische IT-Sicherheitsmaßnahmen können grundsätzlich einen guten Basisschutz im Kontext von I4.0 bilden. Dieser Basisschutz ist jedoch nach entsprechender Risikoanalyse immer in Abhängigkeit von der jeweiligen Sicherheitsarchitektur zu betrachten und umzusetzen. Für einige dieser Maßnahmen gibt es derzeit jedoch weder entsprechende am Markt verfügbaren Produkte noch vollumfängliche Konzepte, sondern oft nur individuell geschaffene Speziallösungen. Bezüglich der Anforderungen an den Schutz der Konstruktions- und Fabrikationsdaten sind notwendige Basistechnologien verfügbar, z. B. zur Verschlüsselung, es ist aber beispielsweise noch ungeklärt, wie Verfügbarkeitsansprüche der Produktion mit bestehenden IT-Sicherheitskonzepten verbunden werden können. Hier besteht dringender Forschungs- und Entwicklungsbedarf. Darüber hinaus müssen Konzepte und Lösungen erarbeitet werden, wie der Aufbau und der Betrieb von Basistechnologien und -methoden, z. B. einer Public-Key-Infrastruktur (PKI), auf Produktionsumgebungen abgebildet werden können. Ähnlich sieht es im Bereich der hardware-basierten Vertrauensanker für Produktionssysteme – digitale Identitäten – aus. Vorhandene Entwicklungen sollten gefördert und als Ziel entsprechend in Forschungsprogramme aufgenommen werden. Auch die Fragestellung nach einer Methode zur kontinuierlichen IT-Sicherheitsüberwachung von Produktionssystemen steht eher am Anfang. Zurzeit sind keine anwendbaren Konzepte bekannt. Bezüglich der fortschreitenden Konvergenz von Safety und Security besteht zudem erhöhter Forschungsbedarf für Integrationskonzepte und das Management möglicher Wechselwirkungen. All diese Fragestellungen müssen dringend adressiert werden und bedürfen unmittelbarer Unterstützung seitens der politischen Entscheider, sei es durch weitere F&E-Förderungen, gesetzliche Regelungen oder flankierenden Maßnahmen zur Akzeptanz in der Wirtschaft und Bevölkerung.

Viele der organisatorischen IT-Sicherheitsmaßnahmen, die heute für das industrielle Umfeld empfohlen und dort auch vielfach bereits umgesetzt sind, sind auch für die I4.0 geeignet. Durch die Überwindung von Unternehmensgrenzen entstehen jedoch zahlreiche neue Schnittstellen und neue Prozesse werden benötigt. Es bedarf organisatorischer Maßnahmen, die in ihrer Gesamtheit am ehesten zu erfassen sind, wenn der bevorstehende Wandel als zentrales Innovationsthema im Unternehmen betrachtet und aus allen Perspektiven gleichrangig angegangen wird. Da es insbesondere für KMU weder möglich noch sinnvoll ist, alle geforderten Kompetenzen selbst aufzubauen, muss in einigen Bereichen vorübergehend oder dauerhaft auf Dienstleister zurückgegriffen werden. Diese können unterstützen und einen Beitrag leisten, aber nicht die Verantwortung abnehmen. Daher sind KMU gefordert, sich selbst eine umfassende Strategie zu erarbeiten und das Unternehmen auf allen Ebenen auf die I4.0-Herausforderungen vorzubereiten. Ein guter Ansatzpunkt dazu ist der Rückgriff auf Erfahrungsberichte, Best-Practice-Sammlungen und Handlungsleitfäden. Ein weiterer zentraler Punkt ist das Vorantreiben der Standardisierung unter Einbeziehung von KMU.

Fragestellungen, die derzeit in der juristischen Literatur vermehrt betrachtet werden (v. a. Datenschutz) betreffen nur teilweise die faktischen Probleme der KMU bei der Umsetzung von I4.0. Vordringlich sind hier strukturelle Maßnahmen im Rechtsraum nötig, um Unsicherheiten über konkrete Anforderungen zu beseitigen, wirksame Durchsetzungsmechanismen zu schaffen, zu einer einheitlichen Vertragspraxis zu gelangen und Standards und Zertifikate zu etablieren auf deren Basis Unternehmen ihre Leistungen anbieten und weiterentwickeln können. Das IT-Sicherheitsgesetz gibt Impulse für die Entwicklung der IT-Sicherheitsregulierung, zeigt aber den Bedarf an einer Weiterentwicklung des rechtlichen Rahmens für IT-Sicherheit deutlich auf. Die auf einer gesetzlichen Regelung beruhende Zertifizierung von IT-Sicherheit und insbesondere die Herausbildung von transparenten, öffentlichen Standards für IT-Sicherheit sind geeignet, eine Verbesserung von IT-Sicherheit in der Fläche zu erreichen. Es fehlt derzeit aber an einem tragfähigen Konzept, sodass auch hier erhebliche Anstrengungen erforderlich sind. Die Nutzung der Erkenntnisse aus der Datenschutz-Zertifizierung könnte hier aber einen guten Einstieg bilden. Die Definition des Rechtsrahmens für IT-Sicherheit muss möglichst auf europäischer oder internationaler Ebene erfolgen. Entsprechende Maßnahmen sind anzustoßen, werden voraussichtlich aber Zeit benötigen. Um kurz- und mittelfristig rechtssichere Lösungen zu erarbeiten, sind Maßnahmen des nationalen Gesetzgebers geboten.

Hinsichtlich der Standardisierung sollte im Rahmen der Arbeiten zu einem I4.0-Referenzmodell eine Strukturierung des Themas IT-Sicherheit vorgenommen werden und damit die Klassifikation der notwendigen Standardisierungsarbeiten erfolgen. Zahlreiche Standards sind auch auf den Bereich der industriellen Produktion übertragbar, bedürfen allerdings der Fokussierung auf das Zusammenspiel von IT-Sicherheitsanforderungen und Schutzzielen mit anderen nicht-funktionalen Anforderungen wie Ausfallsicherheit, Echtzeit und Verfügbarkeit. Eine belastbare Bewertung der Relevanz bestehender technischer IT-Sicherheitsstandards für den Bereich industrielle Produktion/I4.0 ist erst möglich anhand der Struktur und den ausgewählten Technologien von I4.0-Referenzarchitekturen. Regulierungs- und Standardisierungsarbeiten müssen die globale Marktsituation von I4.0 berücksichtigen und können deshalb von vornherein nur in einem kooperativen, international ausgerichteten Verbund von Industrie, Forschungseinrichtungen, Verbänden und politischen Institutionen bearbeitet werden.

Handlungsvorschläge

Im Rahmen dieser Studie wurden 36 spezifische Handlungsvorschläge erarbeitet, die die zielgerichtete Umsetzung von I4.0 unterstützen. Diese Vorschläge sollen den Anwendern und der Politik dabei helfen, für konkrete Szenarien zu erkennen, an welchen Stellen Handlungsbedarf besteht. Zudem sollen sie bei der Identifizierung und Etablierung von Maßnahmen unterstützen, um vorhandenen Risiken und Bedrohungen sowie rechtlichen und organisatorischen Hemmnissen zu begegnen.

Es folgen nun die Handlungsvorschläge[4], sortiert nach den primären Zielgruppen und ihrer Priorisierung:

Unternehmen und Branchenverbände

- Top-down-Förderung von Vertrauen in das Konzept und die Vision von I4.0
- Musterverträge zur Kooperation und Sicherheitsanforderungen
- Integrierte Methodik für Safety & Security
- Verschlüsselung sensibler Daten
- Hinterfragen etablierter Strukturen und Prozesse im Rahmen des Risikomanagements
- Musterdatenschutzklauseln und -einwilligungen
- Integritätsprüfungen
- Orientierung an Erfahrungsberichten, Best-Practices und Handlungsleitfäden
- Muster-Non-Disclosure-Agreements
- Verwendung hardware-basierter Sicherheitsanker
- Umsetzung bewährter organisatorischer IT-Sicherheitsmaßnahmen
- Entwicklung von Komponenten mit Secure Plug & Work Fähigkeiten
- Einsatz von Assistenzsystemen zur Entlastung von Mitarbeitern
- Aufbau von Public-Key-Infrastrukturen oder Single-Sign-On
- Einsatz von Promotoren zur Förderung von Änderungsprozessen
- Entwicklung von Anomalie-Erkennungssystemen
- Durchführung einer gezielten Personalentwicklung
- Durchführung von Pilotprojekten in einem etablierten Umfeld

4 Hier nur Überschriften, die detaillierte Betrachtung inklusive Herleitung, konkrete Zielgruppen und ihr Zusammenspiel, Zielzustand und Zeiträumen finden sich unten im Text.

Politik/Gesetzgeber und Aufsichts- und Regulierungsbehörden (Wirtschafts-, Technologie- und Förderpolitik)

- Einigung auf sinnvolle Vorgaben im Hinblick auf Strukturen und Prozesse (Mindeststandards)
- Einheitliche rechtliche Pflichten zur IT-Sicherheit und prüffähige Standards
- Förderung der Entwicklung von Bewertungs- und Entscheidungs-Unterstützungsmodellen
- Rechtssicherheit durch datenschutzrechtliche Rechtsgrundlagen für Datenströme bei I4.0
- Rechtlicher Rahmen für IT-Sicherheitszertifizierung
- Konzeption geeigneter Aus- und Weiterbildungsangebote
- Ausbau behördlicher Kompetenzen und Kooperation im Bereich IT-Sicherheit
- Bereitstellung einer Kommunikationsplattform zur Diskussion und Aufklärung mit Fokus auf KMU
- Musterklauseln und Mustereinwilligungen für I4.0 hinsichtlich Haftung sowie Datenschutz und Betriebs- und Geschäftsgeheimnisse
- Erforschung von Maßnahmen zur Vermeidung von menschlichem Fehlverhalten im Kontext von Angriffen
- Orientierungsrahmen für angemessene technisch-organisatorische Maßnahmen durch Datenschutzsiegel
- Herausarbeitung von Hindernissen die durch (internationales) Exportrecht bei I4.0 gemeinhin entstehen können
- Forschung und Konzeption zum Rechtsrahmen für IT-Sicherheit
- Länderübergreifende einheitlichen Schutzstandards in Bezug auf Geheimnisschutz

Standardisierungs- und Normierungsorganisationen

- Erarbeitung integrierter Standards für Safety & Security
- Erarbeitung einer Struktur für IT-Sicherheitsstandards
- Integration technischer Standards mit ISMS-Standards[5]
- Engineering von sicheren IT-Systemen

Eine Vielzahl von Handlungsvorschlägen muss kurzfristig im Zeitraum von wenigen Jahren angegangen werden. Hier sind sowohl die Wirtschafts-, Technologie- und Förderpolitik, Standardisierungsorganisationen als auch die Unternehmen selbst gefragt, welche in vielen Bereichen eng zusammenarbeiten müssen oder voneinander abhängig sind.

5 Informationssicherheits-Managementsystem (ISMS)

1. Einleitung

Laut VDE-Trendreport 2015[6] wird die gegenwärtige Vision von Industrie 4.0 (I4.0) bis zum Jahr 2025 Realität geworden sein. Schon heute bestimmen IT-Infrastrukturen in zunehmendem Maße die industriellen Prozesse und sind in fast allen Bereichen unverzichtbar. Zukünftig werden komplexe IT-Infrastrukturen – bestehend aus mobilen und stationären Komponenten – die gesamte industrielle Wertschöpfungskette durchdringen und heute kaum vorstellebare Flexibilitäts- und Effizienzsteigerungen ermöglichen.

Für die Zuverlässigkeit solcher Systeme und zum Schutz betriebs- und personengebundener Daten ist ein hohes Maß an IT-Sicherheit unabdingbar. Der Schutz vor Cyberattacken zur illegalen Aneignung von Daten oder zur Sabotage IT-basierter industrieller Prozesse betrifft neben einzelnen Teilnehmern ganze Wertschöpfungsketten bzw. -netzwerke, die vielfach global organisiert sind. Die heute weitgehend noch fehlende IT-Sicherheit wird laut VDE-Trendreport 2015 derzeit als das weitaus größte Hindernis für den Einzug von I4.0 in die produzierenden Betriebe Deutschlands gesehen. An gleicher Stelle wird auch zu Recht darauf hingewiesen, dass insbesondere IT-Sicherheit, als eine Dimension der Produktqualität und Alleinstellungsmerkmal der in Deutschland produzierenden Unternehmen, eine wichtige technologische Voraussetzung und der entscheidende „enabling“ Faktor für die Umsetzung der Vision „Industrie 4.0“ sein wird.

Obwohl IT-Sicherheit sich in der Öffentlichkeit und in der Wirtschaft längst als wichtiges Thema etabliert hat und das Bewusstsein bezüglich der potenziellen Risiken weit verbreitet erscheint, ist es unbestreitbar, dass insbesondere kleine und mittlere Unternehmen (KMU) bei der Umsetzung entsprechender Vorkehrungen einen deutlichen Nachholbedarf aufweisen. Das Bundesministerium für Wirtschaft und Energie (BMWi) hat daher im Rahmen seines Technologieprogramms „AUTONOMIK für Industrie 4.0“[7] die Studie „IT-Sicherheit für die Industrie 4.0 – Produktion, Produkte, Dienste – von morgen im Zeichen globalisierter Wertschöpfungsketten“ beauftragt, um eine Einschätzung zu erhalten, wie es um die Lage der IT-Sicherheit im Kontext der Zukunftsvision „Industrie 4.0“ bestellt ist, welche Ausgangslage hinsichtlich Aktivitäten und Bedrohungen besteht und welche Maßnahmen ggf. ergriffen werden können, um das IT-Sicherheitsniveau zu verbessern. Ein Hauptziel dieser Studie war daher die Erarbeitung von Handlungsvorschlägen für die Industrie, insbesondere KMU, als auch für die Wirtschafts- und Förderpolitik sowie Regulierungsbehörden.

Angesichts der hohen Komplexität, der noch nicht vollständig absehbaren Ausgestaltung der zukünftigen I4.0 und der notwendigen IT-Sicherheit ist für die Erstellung dieser Studie ein interdisziplinäres Autorenteam gebildet worden, um Know-how aus den unterschiedlichen Wissensbereichen Recht, Organisation und Technik zusammenzuführen.

Das interdisziplinäre Autorenteam verfügt über die folgenden Schwerpunkte:

Angewandte Forschung sowie Normung und Standardisierung: **Fraunhofer Gesellschaft e.V.** mit Experten aus vier Instituten (ESK, IOSB, ISI, SIT).

IT-Sicherheitsindustrie: **Sirrix AG security technologies**.

Anbieter von Produkten im Umfeld Industrie 4.0 sowie Experten bei der Modellierung von Industrieprozessen: **Software AG**.

Integrator und Betreiber von Produkten im Umfeld Industrie 4.0: **Robert Bosch GmbH**.

Rechtliche Implikationen: **WTS Legal Rechtsanwaltsgesellschaft mbH und Prof. Dr. Georg Borges (Universität des Saarlandes)**.

Reviews: **ecsec GmbH und Prof. Dr. Jörg Schwenk (Ruhr-Universität Bochum/Horst Görtz Institut für IT-Sicherheit (HGI))**.

Unterstützt wurde dieses Autorenteam durch einen umfangreichen Expertenbeirat, insbesondere durch zwei assoziierte Partner:

IT-Sicherheitsbehörde: **Bundesamt für Sicherheit in der Informationstechnik (BSI)**.

IT-Sicherheitsverband: **TeleTrusT – Bundesverband IT-Sicherheit e.V.**

6 Zusammenfassung der Studienergebnisse des VDE-Trendreports Elektro- und Informationstechnik 2015, https://www.vde.com/de/Verband/Pressecenter/Pressemeldungen/Fach-und-Wirtschaftspresse/2015/Documents/25-15_Hannover%20Messe_lang.pdf, abgerufen am 10.07.2015; VDE-Trendreport 2015 Elektro- und Informationstechnik, Schwerpunkt: Industrie 4.0, Innovationen – Märkte – Nachwuchs.

7 AUTONOMIK für Industrie 4.0 - Produktion, Produkte, Dienste im multidimensionalen Internet der Zukunft, http://www.autonomik.de/de/1003.php, abgerufen am 21.12.2015.

Das Autorenteam hat sich unter Leitung der Sirrix AG aus folgenden Organisationen zusammengesetzt:

Abbildung 1–1: Autorenteam, zusammengesetzt aus den Disziplinen Recht, Technik und Organisation

Sirrix AG security technologies

BOSCH

software AG

wts TAX LEGAL CONSULTING

Fraunhofer SIT

Fraunhofer IOSB

RUHR UNIVERSITÄT BOCHUM RUB

Fraunhofer ESK

esec

Fraunhofer ISI

Quelle: Sirrix AG

Zielgruppe der Studie

Die Studie richtet sich an alle interessierten Personen aus dem Bereich der industriellen Produktion, sie wurde auf besonderen Wunsch des Auftraggebers so verfasst, dass insbesondere Personen außerhalb des Fachexpertenkreises alle Informationen verstehen können. Als Zieladressatenkreis werden Entscheider in Unternehmen und Branchenverbänden, in Wirtschafts- und Förderpolitik, beim Gesetzgeber und in Aufsichts- und Regulierungsbehörden sowie in Standardisierungs- und Normierungsorganisationen erachtet. Für die Politik hinsichtlich ihrer Rolle in der notwendigen Moderation von Verhandlungsprozessen, bei der Förderung und der Gesetzgebung. Eine Differenzierung nach Branchen (Hintergrund: andere Sprachwelten) wurde nur vereinzelt dort vorgenommen, wo dies sinnvoll erschien.

Die Studie verfolgt das Ziel, diesem primären Zieladressatenkreis gerecht zu werden. Technische Detailanalysen treten daher gegenüber der Darstellung der übergreifenden technisch-organisatorisch-rechtlichen Zusammenhänge zurück.

1.1 Der Begriff Industrie 4.0 aus Sicht der IT-Sicherheit

Zunächst ist festzuhalten, dass es derzeit noch keine weltweit allgemeine anerkannte und durchgängige Definition dessen gibt, was „Industrie 4.0“ (bzw. im internationalen Bereich derjenige Teil des „Internet of Things“ und der „Cyber Physical Systems“, welche die industrielle Produktion und ihre Wertschöpfungsketten betreffen) ausmacht und umfasst. Im Rahmen der Aufgabenstellung dieser Studie ist der Fokus der Betrachtung die „Smart Factory“ und ihre Schnittstellen zu den „Smart Products“, „Smart Logistics“ und „Smart Business“.

Für diese Studie legen wir daher die Begriffsdefinition von Industrie 4.0 aus dem Kapitel 2 des Abschlussberichtes[8] des Arbeitskreises Industrie 4.0 zugrunde (nachfolgend kurz „acatech-Studie“ genannt). Demnach „fokussiert Industrie 4.0 auf die Produktion intelligenter Produkte, Verfahren und Prozesse“ als Bestandteil der Entwicklung hin zum „Internet of Things“ (IoT) und „Internet of Services“ (IoS). Besonders relevant im Kontext dieser Studie ist zudem die Definition der Plattform Industrie 4.0: „Der Begriff Industrie 4.0 steht für die vierte industrielle Revolution, einer neuen Stufe der Organisation und Steuerung der gesamten Wertschöpfungskette über den Lebenszyklus von Produkten. Dieser Zyklus orientiert sich an den zunehmend individualisierten Kundenwünschen und erstreckt sich von der Idee, dem Auftrag über die Entwicklung und Fertigung, die Auslieferung eines Produkts an den Endkunden bis hin zum Recycling, einschließlich der damit verbundenen Dienstleistungen.

Basis ist die Verfügbarkeit aller relevanten Informationen in Echtzeit durch Vernetzung aller an der Wertschöpfung beteiligten Instanzen sowie die Fähigkeit aus den Daten den zu jedem Zeitpunkt optimalen Wertschöpfungsfluss abzuleiten. Durch die Verbindung von Menschen, Objekten und Systemen entstehen dynamische, echtzeitoptimierte und selbst organisierende, unternehmensübergreifende Wertschöpfungsnetzwerke, die sich nach unterschiedlichen Kriterien wie beispielsweise Kosten, Verfügbarkeit und Ressourcenverbrauch optimieren lassen.“[9]

Die Vision von I4.0 umfasst eine Entwicklung, von der angenommen wird, dass sie sich über Jahrzehnte erstrecken wird. Einzelne Aspekte dieser Vision (z. B. vorausschauende Fernwartung) sind zwar heute bereits Wirklichkeit oder zumindest in Ansätzen vorhanden. Der größere Teil ist aber noch Zukunftsmusik. Daher „existiert“ Industrie 4.0 – abgesehen von einzelnen, meist öffentlich geförderten kleinen Pilotprojekten – heute noch nicht. Die Beteiligten sind sich dabei weitgehend einig, dass es sich um einen evolutionären Prozess handeln wird.

Die Paradigmen, über deren Gültigkeit nach dem heutigen Wissensstand weitgehender Konsens besteht und die in der acatech-Studie zu Industrie 4.0 als die Treiber identifiziert wurden, die zu der Vision von I4.0 führen, werden nach der allgemeinen Lebenserfahrung über einen Zeitraum von Jahrzehnten durch technische Innovationen und die wirtschaftliche und politische Dynamik weiteren Änderungen unterworfen sein. Nicht alles wird also genau so kommen, wie dort skizziert.

Die grundlegende Entwicklung zur weiteren horizontalen und vertikalen Integration der Produktionsprozesse, die den Kern von I4.0 ausmacht, darf jedoch als sicher vorausgesetzt werden. Offen sind die Geschwindigkeit und das Ausmaß mit der sich diese Entwicklung vollziehen wird.

Umfragen bei Unternehmen[10] zeigen dabei vor allem eines sehr klar: Die Lösung der offenen Probleme bei Datensicherheit, Datenschutz und Privatsphäre wird als der Erfolgsfaktor mit der höchsten Priorität für die weitere Entwicklung dieser digitaler Infrastrukturen eingeschätzt.

1.2 Neues durch Industrie 4.0

Industrie 4.0 entsprechend der Vision der acatech-Studie und der Plattform Industrie 4.0 ist heute noch in keinem Unternehmen annähernd voll verwirklicht. Zukünftige Vorgänge, die in der derzeitigen Situation von vernetzten industriellen Prozessen tatsächlich stattfinden, können jedoch auf Basis existierender Publikationen zu I4.0 „extrapoliert“ werden. Dies kann sowohl in Richtung weiter zunehmender Vernetzung über Länder-, Standort-, und Unternehmensgrenzen, als auch zunehmender autonomer Abläufe in Produktion und Logistik und zunehmender Verfügbarkeit von großen und teils sensitiven Datenbeständen geschehen. Eine zentrale Herausforderung für die Industrie von morgen durch zunehmende Digitalisierung, Dynamik und Komplexität ist die Fähigkeit der I4.0-IT-Architektur, sich an Änderungen anzupassen – sei es, dass neue Anlagen oder Produktionsprozesse in das System und dessen Netzwerk eingebracht werden oder bestehende Produktionssysteme und zugehörige Netzwerke verändert und nach außen geöffnet werden.[11] Eine wesentliche Veränderung durch I4.0 ist die Entstehung von dynamischen, echtzeitoptimierten und sich selbst organisierenden, unternehmensübergreifenden Ad-hoc-Wertschöpfungsnetzwerken.

8 Forschungsunion/acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, April 2013.
9 Umsetzungsstrategie Industrie 4.0 – Ergebnisbericht der Plattform Industrie 4.0, April 2015, Seite 8.
10 Z. B. „Digitalisierung. Achillesferse der deutschen Wirtschaft“, Zukunftsstudie Münchner Kreis Band VI, 2015, S.15.
11 Vgl. Secure Plug and Work - Ein Beitrag zum Zukunftsprojekt Industrie 4.0, Fraunhofer IOSB, http://www.iosb.fraunhofer.de/servlet/is/47385/, abgerufen am 21.12.2015.

Hauptcharakteristika der I4.0-Wertschöpfungsketten sind hierbei die

- Ab- bzw. Auflösung der klassischen Automatisierungspyramide
- Verteilung der Wertschöpfungsprozesse auf verschiedene Akteure
- Hohe Dynamik der Kooperationsdauer der im Wertschöpfungsprozess beteiligten Partner
- Unterschiedliche technologische, betrieblich-organisatorische wie auch rechtliche der Partner: sehr kleine Unternehmen (wie z. B. ein-zwei bis-fünf-Mitarbeiter-Ingenieurbüro) und international agierende Großkonzerne

Die Ablösung der klassischen Automatisierungspyramide und die Verteilung des Wertschöpfungsprozesses auf verschiedene Akteure führen zu neuen Herausforderungen hinsichtlich IT-Sicherheit und bedingen neue IT-Sicherheitsmanagementprozesse, die nun über die Unternehmensgrenzen hinweg etabliert werden müssen. Unternehmensübergreifende Bedrohungsanalysen und Vertrauensbeziehungen werden notwendig. Es sind Fragen zu beantworten wie bspw.:

- Wie soll ein IT-Sicherheitsmanagementprozess in einem Ad-hoc-Wertschöpfungsnetz gestaltet werden?
- Bei wem liegt die Verantwortung/Haftung für die Gewährleistung der IT-Sicherheit in einem Wertschöpfungsnetzwerk?
- Müssen die beteiligten Akteure bestimmte IT-Sicherheitsmaßnahmen umsetzten, um ein Teil eines Wertschöpfungsnetzes zu werden?
- Oder können die IT-Sicherheitsmaßnahmen an externe Dienstleister übertragen werden? Unter welchen Voraussetzungen?
- Welche Auswirkungen haben die dynamischen Kooperationsbeziehungen in einem Wertschöpfungsnetzwerk auf die klassischen IT-Sicherheits-Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität?
    - Wie ist die Ausfallsicherheit der Produktionsanlagen zu bewerten? (Verfügbarkeit)
    - Wie ist die Echtzeitverarbeitung der produktionsrelevanten Daten zu bewerten? (Verfügbarkeit)
    - Wie ist die funktionale Sicherheit (Safety) hinsichtlich der Integrität eines Systems sowie die Verfügbarkeit von Sicherheitsfunktionen zu bewerten?
- Kommen neue Schutzziele durch I4.0 hinzu?
- Welche organisatorischen, rechtlichen und technologischen Rahmenbedingungen müssen für die dynamischen, unternehmensübergreifenden und vor allen Dingen sicheren (auch unter Berücksichtigung von Security & Safety) Wertschöpfungsnetzwerke geschaffen werden, um die genannten Schutzziele zu erreichen?
- Welche neuen Anforderungen, z. B. hinsichtlich Benutzerfreundlichkeit, entstehen durch I4.0, wie bspw. eine weitverbreitete Forderung nach Plug & Operate?

1.3 Ziele der Studie

Vor dem Hintergrund dieser Herausforderungen hinsichtlich IT-Sicherheit für die Industrie 4.0 stellt sich die Frage danach, was zu berücksichtigen ist: Welche Bedrohungen sind absehbar? Welche proaktiven IT-Security-Maßnahmen sind zum Schutz vor diesen Bedrohungen zu ergreifen? Welche reaktiven Maßnahmen sind nach einem IT-Security-Vorfall bzw. Schadensfall zu ergreifen? Und sind diese Maßnahmen über heutige Best-Practice-Ansätze abdeckbar oder existieren Hindernisse? Welche Sicherheitskonzepte existieren und welche Ansätze für neue Sicherheitskonzepte, die einen Rahmen vorgeben können, müssen durch Unternehmen und die Politik verfolgt werden?

Das Hauptziel der Studie ist die Ableitung von rechtlichen, organisatorischen und technischen Handlungsvorschläge für Unternehmen sowie Wirtschafts- und Förderpolitik und Regulierungsbehörden hinsichtlich der IT-Sicherheit von zukünftigen Wertschöpfungsnetzwerken als Ergebnis der vertikalen Integration von Industriesteuerungsanlagen (ICS/IACS) durch I4.0. Basierend auf einer Herleitung über ausgewählte, relevante Fallbeispiele aus der Industrie.

Im Gegensatz zu anderen Werken, insbesondere IT-Sicherheitsstandards und Technischen Richtlinien oder z. B. dem Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI), verzichtet die vorliegende Studie nach Möglichkeit auf die Darstellung technischer Details. Vielmehr stehen neben technologischen Herausforderungen in der Studie die organisatorischen und rechtlichen Fragestellungen sowie die Handlungsvorschläge im Vordergrund.

Der für ein sicheres Zusammenspiel von I4.0-Komponenten unerlässliche Informationsaustausch zwischen den unterschiedlichen Disziplinen ist ein wichtiges Ziel. Diesen soll die vorliegende Studie anregen. Die interdisziplinäre Betrachtung wird insbesondere benötigt, um I4.0 überhaupt in der Praxis einsetzen zu können, da Unternehmen sonst aufgrund von rechtlichen (oder nur psychologischen) Unsicherheiten und (gefühlten) Risiken auf den praktischen Einsatz von I4.0 verzichten würden.

Ein weiteres Ziel ist es, die Grenzen und Regeln hinsichtlich IT-Security zu definieren.

Daraus soll sich ein Empfehlungskatalog ergeben, insbesondere mit Vorschlägen für die Politik und den Gesetzgeber sowie den Mittelstand.

1.4 Abgrenzung

Das Ergebnis dieser Studie zielt drauf ab, Handlungsvorschläge sowohl für den Mittelstand und auch die politischen Entscheider bereitzustellen, mittels derer beide Gruppen Richtungsentscheidungen auf Ihrem Weg zu I4.0 treffen können. Für die KMU ist es wichtig erkennen zu können, welche IT-Sicherheitsfaktoren zukünftig in den Vordergrund treten werden und entsprechende strategische Ausrichtungen vorzunehmen. Die Politik soll in die Lage versetzt werden, Technologielücken und Forschungsbedarfe zu identifizieren, damit durch gezielte Fördermaßnahmen den Defiziten und Bedarfen entgegen gewirkt werden kann.

Dabei geht die vorliegende Studie von Fallbeispielen aus, die aus verschiedenen Branchen der Industrie bereitgestellt wurden. Diese Beispiele wurden in dieser Studie in Bezug auf ihre organisatorischen, rechtlichen und technischen Aspekte darauf hin untersucht, welche IT-Sicherheitsansprüche für eine I4.0-Umsetzung daraus abgeleitet werden können.

Es soll nicht versäumt werden, darauf hinzuweisen, dass diese Vorgehensweise ganz entscheidenden Einfluss auf alle Ergebnisse dieser Studie hat. Die herangezogenen Fallbeispiele legen in Bezug auf Qualität der technischen Beschreibungen und auch auf Detailtiefe und Vollständigkeit die Randbedingungen für alle weiteren Erhebungen fest. Im Vorgriff auf den Inhalt der Studie soll an dieser Stelle ebenfalls nicht unerwähnt bleiben, dass die entsprechenden Beistellleistungen aus der Wirtschaft recht unterschiedliche Informationsdichten, Detailgrade und Aussagekraft aufweisen, so dass bestimmte Ableitungen heute nur in dem jetzt darstellbaren Reifegrad zur Verfügung gestellt werden können.

Darüber hinaus sollte bei der Bewertung der Studienergebnisse berücksichtigt werden, dass I4.0 und dessen im Kontext dieser Studie zu betrachtende Neuerungen heute noch in keinem Unternehmen annähernd voll verwirklicht sind und daher auch die gewählten Fallbeispiele aus der Praxis nur Vorgänge beschreiben können, die in der derzeitigen Situation von vernetzten industriellen Prozessen tatsächlich stattfinden. Diese müssen zum Zweck der Betrachtung neuer IT-Sicherheitsbedrohungen im Sinne von 1.2 entsprechend extrapoliert werden. Gleichzeitig müssen Vorgänge, welche vertrauliche Prozesse und Informationen aus der Industrie betreffen für die Beschreibung der Fallbeispiele entsprechend verallgemeinert werden.

Die Studie richtet sich an alle interessierten Personen aus dem Bereich der industriellen Produktion, primär jedoch an Entscheider in Unternehmen und in der Wirtschafts- und Förderpolitik, welche wissen möchten, was im Kontext IT-Sicherheit hinsichtlich der zentral werdenden Vernetzung durch I4.0 in den nächsten Jahren zu tun sein wird, um darauf aufbauend ihre, teils sehr langfristig angelegten Entscheidungen treffen zu können. Sie enthält die notwendigen Hinweise und Vorschläge, jedoch nicht bereits die hierfür zu schaffenden Werkzeuge, also bspw. keine Art Grundschutzhandbuch für Industrieanlagen. Wenn die Leser der Studie die Handlungsvorschläge, egal ob technischer, organisatorischer oder rechtlicher Art, angehen, müssen sie sich an externe Fachkompetenz wenden, oder Expertise im eigenen Haus aufbauen.

Aus den oben genannten Gründen kann die vorliegende Studie nur einen Ausschnitt des breiten Themenspektrums IT-Sicherheit im Kontext der gegenwärtigen Vision „Industrie 4.0“ darstellen. Dies ist beabsichtigt und beim Design der Architektur der Studie berücksichtigt worden. Die vorliegende Studie erhebt aus diesem Grund keinen Anspruch auf Vollständigkeit.

1.5 Vorgehensweise und Methodik

Die Vorgehensweise der Studie folgt dem methodischen Ansatz, aus dem Spannungsfeld zwischen den neuen Herausforderungen und Bedrohungen und den vorhandenen Maßnahmen und Konzepten geeignete Handlungsvorschläge abzuleiten.

Abbildung 1–2: Vorgehensweise und Methodik anhand der Struktur der Studie

Quelle: Sirrix AG

Dieses Kapitel umfasst eine Erläuterung der Vorgehensweise und Methodik anhand der Struktur der Studie (vgl. Abbildung 1–2).

Zu Beginn wird im Kapitel 2 **„Thematische Einführung“** ein Überblick über das Themenfeld IT-Sicherheit in der I4.0 vor dem Hintergrund der eingangs genannten Neuerungen verschafft.

Im nachfolgenden Kapitel 3 **„Existierende Wissensbestände“** werden die für IT-Sicherheit in der I4.0 relevanten existierenden Wissensbestände zusammengefasst. Dies umfasste eine konzentrierte und strukturierte Bestandsaufnahme der aktuellen Wissensbasis mittels existierender Studien, Reformbestrebungen, Aktivitäten von Interessenverbänden und sonstiger maßgeblicher Gremien in Richtung I4.0 mit dem Ziel, diese Wissensbasis zur Identifizierung von neuen Risiken und Herausforderungen nutzbar zu machen. Über öffentlich verfügbare Quellen hinaus flossen auch Erkenntnisse aus Workshops und Gesprächen mit Anwenderunternehmen (insb. KMU) in die Studie ein. In rechtlicher Hinsicht wurden zentrale Aspekte von I4.0 auf der Grundlage eines abstrahierten Modells untersucht, das rechtlich relevante Kernelelemente der internationalen Zusammenarbeit in I4.0 abbildet.

Das angemessene Schutzniveau von I4.0-Anlagen wird eng in Anlehnung an konkrete Sicherheitsbedarfe der Industrie ermittelt. Dazu werden, wie in Kapitel 4 **„Herausforderungen, Bedrohungen & Risiken“** dargestellt wird, die Fallbeispiele „Automobilbau“, „Anlagen-/Maschinenbau“, „Chemische Industrie“, sowie „Grenzüberschreitende Logistik-Prozesse“ analysiert und auf IT-Sicherheitsaspekte hin bewertet. Darüber hinaus wurde eine Extrapolation der Erkenntnisse in Richtung der für I4.0 zu erwartenden Anpassungen erzeugt. Die hier identifizierten Aspekte wurden dazu in ein so genanntes Teilnehmer- und Kommunikationsmodell überführt. Parallel wurde eine Methodik beschrieben, mittels derer dann entsprechende Bedrohungs- und Risikomodellierungen für alle Fallbeispiele erzeugt wurden. Dieses so genannte Referenzmodell, also Teilnehmer- und Kommunikationsmodell sowie Risiko- und Bedrohungsmodell, werden in Kapitel 4.2 entsprechend dargestellt. Die Operationalisierung der Modelle auf die Fallbeispiele führt zu einem Spektrum von Bedrohungen, die im Abschnitt 4.5.1.5.4 auf die Domänen „Rechenzentrumsbetrieb“, „Internetkommunikation“, „Maschinenbetreiber“, „Maschinenhersteller“ und „Fernwartungsdienstleister“ abgebildet wurden.

Die identifizieren Aspekte werden in Kapitel 5 **„IT-Sicherheitsmaßnahmen sowie Implementierungshindernisse“**

entsprechend der Vorgaben der jeweils als relevant erachteten Standards und Regelwerke auf verfügbare und angemessene Gegenmaßnahmen hin analysiert und bewertet. Für den technischen und organisatorischen Teil insbesondere hinsichtlich des BSI ICS-Security-Kompendiums (Industrial Control System Security Kompendium), welches gut zu den gewählten Fallbeispielen passt und auf alle relevanten Standards (insb. ISO/IEC 2700x, ISA/IEC 62443) referenziert sowie weiterer Literatur, Leitfäden und Best Practices. Für den rechtlichen Teil insb. hinsichtlich Datenschutz- und Exportkontrollrecht sowie hinsichtlich der strukturellen Merkmale der rechtlichen Anforderungen an die IT-Sicherheit (bspw. Gesetzgebung, Rechtsprechung, Behördliche Normsetzung und Kontrolle sowie der Vertragspraxis und Zertifizierung). Als Ergebnis liegt eine Matrix vor (Kreuztabelle, ICS-Security, Anhang 8.1.2), welche die gegenwärtigen Lücken bezüglich der IT-Sicherheitsbedrohungen aufzeigt sowie eine Beschreibung der Hemmnisse bei der Umsetzung der etablierten Maßnahmen als auch Handlungsvorschläge hinsichtlich fehlender neuer Konzepte.

Nachfolgend wird in Kapitel 6 **„Vorhandene und neuartige Sicherheitskonzepte“** eine Identifizierung bzw. Entwicklung geeigneter Konzepte zur Erzielung eines angemessenen Sicherheitsniveaus in I4.0 vorgenommen. Dabei wurden sowohl Überlegungen zu gänzlich neuen Konzepten angestellt, als auch zur Übertragbarkeit existierender Konzepte aus anderen Anwendungsfeldern, die sowohl die Lücken der zuvor betrachteten Leitfäden und Best Practices, wie des ICS-Security-Kompendiums, adressieren, als auch die erweiterten Ansprüche von I4.0 berücksichtigen.

Hierauf aufbauend werden in Kapitel 7 **„Ableitung von Handlungsvorschlägen“** die zentralen Herausforderungen und Handlungsmöglichkeiten zusammengefasst, Hinweise zu Kosten-Nutzen-Betrachtungen von IT-Sicherheit gegeben und 32 Handlungsvorschläge für die (Wirtschafts-/Technologie-/Förder-)Politik, den Gesetzgeber und Aufsichts-/Regulierungsbehörden einerseits und Unternehmen und Branchenverbände sowie Standardisierungsorganisationen andererseits abgeleitet, welche das wesentliche Ergebnis der Studie darstellen.

Einbindung des Beirates

Der im Zuge der Studie zusammengestellte Beirat aus namhaften Experten aus der Industrie[12] wurde im Zuge eines Initialworkshops im November 2014 zur Vorstellung und Diskussion des Studiendesigns als auch im Zuge eines Expertenworkshops zur Hannover Messe 2015 zur Vorstellung und Diskussion der zentralen Handlungsvorschläge eingebunden. Die genutzten Fallbeispiele stammen von über den Beirat eingebundenen Industrieunternehmen. Erste Schlussfolgerungen wurden dem Beirat zur Kommentierung übersendet, die Rückmeldungen flossen in die Studie ein. Der Beirat wurde zudem um Stellungnahme zur finalen Entwurfsfassung gebeten. Eine Vielzahl von – teils auch kritischen – Rückmeldungen wurden aufgenommen und in der finalen Studienfassung berücksichtigt. Die im Beirat vertretene Begleitforschung des BMWi-Forschungsprogramms „AUTONOMIK Industrie 4.0“, das Institut für Innovation und Technik (iit) in der VDI/VDE-Innovation + Technik GmbH, führte zudem im Januar 2015 einen Workshop – „Softwarearchitekturen für die Industrie 4.0“ – durch, in welchem die Studie vorgestellt und Hinweise auf Herausforderungen aus weiteren konkreten Fallbeispielen aus den Autonomik-Projekten aufgenommen wurden.

Die Studie wurde im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) von August 2014 bis Juli 2015 erstellt. Der Inhalt und die Empfehlungen wurden unabhängig durch die Auftragnehmer erarbeitet und reflektieren nicht notwendigerweise die Meinung des BMWi.

12 ARBURG GmbH + Co KG, BASF SE, Bayer Technology Services GmbH, Dachser GmbH & Co. KG, DMG Mori GmbH, Felss Systems GmbH, Infineon Technologies AG, infoteam Software AG, Innominate Security Technologies AG, OPC Foundation, Otto Bihler Maschinenfabrik GmbH & Co. KG, Siemens AG, TRUMPF Werkzeugmaschinen GmbH + Co. KG und WITRON Logistik + Informatik GmbH.

2. Thematische Einführung

Zahlreiche Publikationen belegen, dass in vielen Unternehmen weder das grundlegende Konzept von Industrie 4.0 (I4.0), noch die Implikationen des Wandels hin zu einer industriellen Produktion der Zukunft, die sich durch einen hohen Grad an Vernetzung und Automatisierung auszeichnet, bekannt sind.[13] Darüber hinaus sind vor allem viele KMU gegenüber I4.0 kritisch bis negativ eingestellt.[14] Größere Unternehmen stehen dem Wandel meist offener gegenüber, da sie zur internen Steuerung und Informationsverdichtung bereits digitale Technologien einsetzen, es gewöhnt sind, zur Erschließung neuer Märkte digitale Kanäle zu nutzen und den mit I4.0 verbundenen Investitionsaufwand leichter bewältigen können.[15] Mit der Entscheidung für die I4.0 müssen im Unternehmen in der Regel nicht nur Investitionsentscheidungen getroffen, sondern gleichzeitig auch organisatorische, technische und rechtliche Herausforderungen bewältigt werden. Häufig erfordert der Wandel hin zu einer industriellen Produktion der Zukunft die Begleitung durch spezialisierte Dienstleister.

Die besonderen Herausforderungen im Zusammenhang mit I4.0 sind zu einem großen Teil darauf zurückzuführen, dass digitale Technologien in der Produktion einen immer größeren Stellenwert haben und in der Regel nicht nur ein Unternehmensstandort zu berücksichtigen ist. Um das Potenzial von I4.0 nutzen zu können, sind meist mehrere Standorte, die über verschiedene Länder verteilt sein können, miteinander vernetzt. Auch die Vernetzung eines Verbundes von miteinander kooperierenden, aber auch im Wettbewerb stehenden, Unternehmen (z. B. entlang einer Wertschöpfungskette) wird in Betracht gezogen, wobei durchaus denkbar ist, dass einzelne Kooperationspartner ad-hoc und nur für kurze Zeit eingebunden werden. Während einerseits im Einsatz digitaler Technologien, in der Öffnung von Unternehmen nach außen und der standort- und unternehmensübergreifenden Vernetzung von Produktionsanalagen großes Potenzial gesehen wird, ergeben sich andererseits im Hinblick auf die IT-Sicherheit zahlreiche Änderungen bei der Bedrohungslage. Die Änderungen zeigen sich sowohl im Zusammenhang mit bekannten Bedrohungen, die wenn sie zu einem Sicherheitsvorfall führen, deutlich weitreichendere Folgen haben können, als auch im Zusammenhang mit für ein Unternehmen gänzlich neuen Bedrohungen, die erst durch die Entscheidung für die I4.0 relevant werden. Neben Effizienzsteigerungen und einer Flexibilisierung der industriellen Produktion wachsen auch die Möglichkeiten und Anreize für auf Sabotage und Spionage ausgerichtete Angriffe. Darüber hinaus dürfen neben Angriffen durch Innen- und Außentäter bei der Betrachtung der IT-Sicherheit in der I4.0 auch mögliche Schäden durch menschliches oder technisches Fehlverhalten sowie sonstige Ereignisse nicht vernachlässigt werden.

In der hochgradig automatisierten Produktion der I4.0 fallen große Mengen an Daten an. Einerseits müssen Anlagen Steuerbefehle erhalten und sich untereinander sowie mit anderen Systemen und Produkten abstimmen. Andererseits entstehen im Laufe der Zeit umfassende Logs. Diese Daten, die ein enormes Wissen über Anlagen, Kunden und Märkte enthalten, werden in Datenbanken zusammengeführt und für vielfältige Zwecke eingesetzt. Einzelne Unternehmen, aber nicht selten auch ganze Verbünde von miteinander in länderübergreifenden Wertschöpfungsnetzwerken kooperierenden Unternehmen, sind auf die Vertraulichkeit, Integrität und Verfügbarkeit dieser Daten, die tiefe Einblicke in die Produktion erlauben und damit meist auch sensible Unternehmensgeheimnisse darstellen, angewiesen. Genau das macht diese Daten aber auch zu einem interessanten Ziel für Angriffe.[16] Darüber hinaus ist die Rolle des Menschen als Akteur innerhalb der industriellen Produktion einem Wandel unterworfen. Mensch-zu-Maschine- und Maschine-zu-Maschine-Kommunikation gewinnen immer mehr an Bedeutung. Menschen müssen sich zunehmend in einem stark regelgebunden Umfeld zurechtfinden und haben zukünftig eine überwiegend überwachende Funktion. Auch dieser sich sehr rasch vollziehende Wandel sollte im Zusammenhang mit Fragen der IT-Sicherheit nicht außer Acht gelassen werden.

13 Arnold, R. C. G.; Schiffer, M.; Pols, A.; Thylmann, M. (2013): Wirtschaft digitalisiert. Welche Rolle spielt das Internet für die deutsche Industrie und Dienstleister? 2. Aufl. Hg. v. IW Consult GmbH und BITKOM – Bundesverband Informationswirtschaft, Telekomunikation und neue Medien e.V. Köln, Berlin, FLYACTS GmbH (2014): Industrie 4.0: Grundlagenwissen, Experteninterviews und Pioniere – Studie 06/2014. http://www.flyacts.com/media/Publikationen/Industrie_4.0_Grundlagenwissen_Experteninterviews_Pioniere.pdf und IDC (2014): Industrie 4.0 durchdringt verarbeitendes Gewerbe in Deutschland, Investitionen für 2015 geplant.

14 FLYACTS GmbH (2014): Industrie 4.0: Grundlagenwissen, Experteninterviews und Pioniere – Studie 06/2014. http://www.flyacts.com/media/Publikationen/Industrie_4.0_Grundlagenwissen_Experteninterviews_Pioniere.pdf

15 Blanchet, M.; Rinn, T.; Thaden, G. von; Thieulloy, G. de (2014): THINK ACT. Industry 4.0 The new industrial revolution – How Europe will succeed. Hg. v. ROLAND BERGER STRATEGY CONSULTANTS GMBH. München.

16 Vgl. Brentani, Ulrike de (2001): Innovative versus incremental new business services: Different keys for achieving success. In: Journal of Product Innovation Management 18, S. 169–187, Brentani 2001, S. 173.

3. Existierende Wissensbestände

Die aktuellen Wissensbestände zur IT-Sicherheit industrieller Produktionsanlagen (englisch: Industrial Control Systems (ICS) oder Industrial Automation and Control Systems, (IACS)), von Teilkomponenten und zu IT-Prozessen von damit zusammenhängenden Wertschöpfungsketten können folgendermaßen kategorisiert werden:

1. Bestandsaufnahmen der derzeitigen Ist-Situation (Ausgangslage).

2. Bestehende verbindliche technische und organisatorische Normen und Regelungen, die aus heutiger Sicht für die IT-Sicherheit auch bei Industrie 4.0 (I4.0) in Zukunft relevant sein werden.

3. Arbeitsergebnisse von Normierungsgremien, die sich mit den für I4.0 künftig notwendigen Erweiterungen befassen, aktuell aber noch nicht den Status einer verbindlichen Norm besitzen.

4. Empfehlungen zur IT-Sicherheit insbesondere von Industrieverbänden und Anwenderarbeitskreisen.

5. In den Industriebranchen anerkannte „Good Practices".

6. Ergebnisse von Forschungsprojekten im Bereich I4.0 (international im Bereich Internet of Things (IoT) bzw. Cyber Physical Systems (CPS)), in denen der Aspekt der IT-Sicherheit eine wesentliche Rolle gespielt hat.

7. Nationale Gesetze und Verordnungen sowie internationale Abkommen, die für den Datenschutz und die IT-Sicherheit in der Industrie insbesondere auch im grenzüberschreitenden Datenverkehr von Bedeutung sind.

Darüber hinaus werden in diesem Kapitel auch die wichtigsten nationalen und internationalen Gremien und Institutionen mit Bezug zur IT-Sicherheit in der industriellen Produktion sowie deren Aktivitäten benannt.

3.1 Technische und organisatorische Aspekte

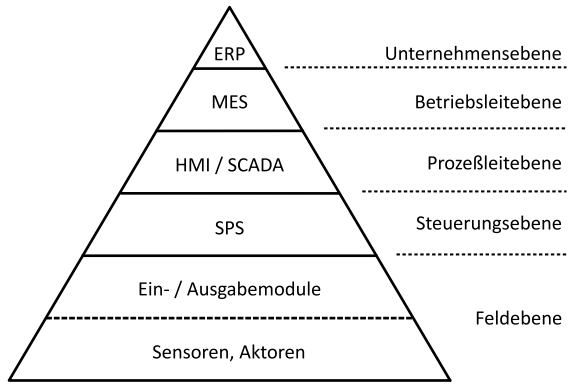
3.1.1 Ausgangslage

Mit dem Begriff „Industrie 4.0" verbindet sich eine Entwicklung in der industriellen Produktion und der dafür erforderlichen Gestaltung der Wertschöpfungsketten, die wesentlich durch den zunehmenden Vernetzungsgrad und durch zunehmend autonomes Agieren von Maschinen gekennzeichnet ist.

Ein Problem hinsichtlich IT-Sicherheit entsteht in Automatisierungsindustrie und Logistik dadurch nicht neu. Die Bedrohungen werden jedoch vielfältiger und die Risiken erhöhen oder verändern sich.

Bereits heute existieren Kommunikationsbeziehungen zwischen den Ebenen der so genannten Automatisierungspyramide (siehe Abbildung 3 1) und zwischen den Komponenten untereinander. Bereits heute sind die Komponenten und deren Kommunikationskanäle angreifbar.

Abbildung 3–1: Klassische Automatisierungspyramide



Quelle: Fraunhofer ESK

Dementsprechend wurden sowohl auf nationaler (z. B. Bundesamt für Sicherheit in der Informationstechnik (BSI), VDI/VDE)[17] als auch auf internationaler Ebene (z. B. IEC, ISA) bereits seit einiger Zeit Richtlinien für die technische und organisatorische Verwirklichung von IT Sicherheit bei industriellen Steuerungssystemen entwickelt und herausgegeben.

17 ICS-Security Kompendium, hrsg. v. Bundesamt für Sicherheit in der Informationstechnik (2013); VDI/VDE Richtlinie 2182, VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (2007).

Die Bedrohungen wurden jedoch bislang insofern als beherrschbar betrachtet, als die Produktionsanlagen IT technisch gesehen Inseln bildeten, die nur begrenzt Angriffspunkte für Angriffe von außen boten. Logistikprozesse hingegen spielten sich bislang hauptsächlich auf der Ebene der Office-IT ab.

Darüber, wie IT-Sicherheit im Bereich der Automatisierungs- und Steuerungssysteme in der Produktion in deutschen Unternehmen heutzutage gelebt wird, lässt sich keine generelle Aussage treffen.

Großunternehmen verfügen zumeist über ein – auch personell – gut aufgestelltes IT-Sicherheitsmanagement, das auch über die hinreichende Kompetenz, hinreichenden Befugnisse und den hinreichenden Durchgriff innerhalb der Firma verfügt. Aufgrund ihrer Größe sind sie auch in der Lage, Lieferanten und Kooperationspartner dazu zu veranlassen, sich an vorgegebene Verfahren anzupassen.

Großunternehmen entwickeln oft auch unabhängig vom Reifegrad entsprechender Standardisierungs- und Normierungsbemühungen entweder selbst so genannte „Best Practices“ oder setzen in der Branche existierende und anerkannte vorbildliche Praktiken um. Ein Beispiel hierfür ist das auf ISA99 basierende „Defense-in-Depth-Konzept“[18] des Unternehmens Siemens.

Vielen kleinen und mittleren Unternehmen (KMU) fehlen jedoch die Ressourcen, um ein vergleichbares System zu etablieren und zu unterhalten. Investitionen in IT-Sicherheit in Form von vorbeugenden Maßnahmen technischer und organisatorischer Art genießen nur eine untergeordnete Priorität, solange im Unternehmen noch keine gravierenden Sicherheitsvorfälle bemerkt worden sind, die der Firma einen spürbaren Schaden zugefügt haben. Die Umsetzung der bestehenden Regelwerke zur IT Sicherheit wird als zu komplex wahrgenommen. Obwohl aus diesen Regelwerken nur ein für das jeweilige Unternehmen passendes und hinreichendes Subset umgesetzt werden müsste, fehlen die Kenntnisse, genau diese Anteile zu identifizieren und ökonomisch sinnvoll zu implementieren.[19]

3.1.1.1 Das Erbe der bestehenden Automatisierungssysteme

Bei der Automatisierung in der industriellen Produktion wurde bereits in den 1970er-Jahren mit der Vernetzung begonnen. Die hierfür entwickelten, meist proprietären Kommunikationsprotokolle[20] berücksichtigten Aspekte der IT-Sicherheit allerdings nicht oder allenfalls rudimentär.

In den Produktionsanlagen der Industrie werden aufgrund der dort vorherrschenden langen Investitionszyklen noch lange Zeit Komponenten verwendet werden, die mit diesen Protokollen arbeiten und gegenüber Sicherheitsgefährdungen über keine eigenen Abwehrmechanismen verfügen.

Hinzu kommt, dass Komponenten wie z. B. Sensoren in Produktionsanlagen einerseits meist nur über begrenzte Ressourcen (Energie, Prozessorleistung, Speicherkapazität) verfügen und andererseits Echtzeitanforderungen genügen müssen, so dass der Einsatz von in der Office-IT üblichen IT-Sicherheitsmechanismen grundsätzlich nicht zielführend ist.

Das Institut für Verteilte Systeme der Technischen Universität Hamburg-Harburg hat 2013 einen Übersichtsartikel[21] über die wesentlichen bisherigen Forschungsaktivitäten auf dem Gebiet der Sicherheit industrieller Steuerungsanlagen veröffentlicht. Darin wird letztlich konstatiert, dass die Schwachstellen der heutigen Systeme zwar bekannt und gut verstanden sind, die Sicherheitsanforderungen und die vorgeschlagenen Lösungen aber bei existierenden Anlagen meist jenseits der technischen und ökonomischen Möglichkeiten liegen. Eine sicherheitstechnische Nachrüstung solcher Systeme wird daher nur in Ausnahmefällen zu erwarten sein.

Eine technische und organisatorische Betrachtung der IT-Sicherheit für I4.0 hat folglich immer im Auge zu behalten, dass alle dort implementierten Sicherheitsvorkehrungen kompromittiert werden können, solange in den jeweiligen Netzen auch hergebrachte („legacy“) Komponenten enthalten sind.

18 Industry White Paper V1.0, Industrial Security – Security Konzept zum Schutz industrieller Anlagen, August 2013, http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/whitepaper_security_2013_de.pdf

19 Der Bayerische IT-Sicherheitscluster e.V. in Regensburg hat speziell für kleine und mittlere Unternehmen mit ISA+ und ISIS12 (http://www.it-sicherheit-bayern.de/produkte-dienstleistungen/isis12.html) einen gegenüber den BSI-Grundschutzkatalogen und ISO/IEC 270001 reduzierten Maßnahmenkatalog und ein Vorgehensmodell entwickelt, das für KMUs einen Einstieg in ein IT-Sicherheitsmanagement bietet. Dabei wird zunächst die grundlegende IT-Sicherheit eines KMU insgesamt adressiert. Die speziellen Aspekte der industriellen Produktionsnetze sind hierbei noch nicht berücksichtigt.

20 Für einen Überblick über die Vielfalt dieser Kommunikationssysteme siehe http://www.feldbusse.de/trends/trends.shtml

21 Krotofil, M. Gollmann, D. ; Industrial Control Systems Security: What is happening? 11th IEEE International Conference on Industrial Informatics (INDIN), 2013.

3.1.1.2 Messbarkeit

IT-Sicherheit bedeutet für ein Unternehmen zunächst Aufwand. Jeder Unternehmer wird daher wissen wollen, was ihn eine bestimmte Investition in IT-Sicherheit kostet und welche Kosten mit welcher Wahrscheinlichkeit entstehen könnten, wenn er diese Investition unterlässt.

Eine wichtige Frage, die in diesem Zusammenhang geklärt werden muss, ist daher die Messbarkeit von IT-Sicherheit.

Eine gängige Aussage von IT-Sicherheits-Spezialisten gegenüber ihren Kunden ist oft, hundertprozentige Sicherheit sei grundsätzlich nicht erreichbar, aber man könne mit 20 Prozent des Aufwandes 80 Prozent an Sicherheit erreichen (Pareto-Prinzip). Hier stellt der Praktiker im Unternehmen natürlich sofort die Frage „20 Prozent von was?". Da der Aufwand, den man für die IT-Sicherheit treiben kann, nach oben hin prinzipiell offen ist, fehlt hier eine Kalibrierung der Größen „Aufwand" und „Sicherheit".

Um dem Management von Unternehmen das Thema IT-Sicherheit greifbar zu machen, ist daher vor allem die Entwicklung von nachvollziehbaren Metriken erforderlich. Solche praktisch anwendbaren Metriken existieren heute nicht.

Vergleicht man Investitionen in IT-Sicherheit im Sinne einer Versicherung mit Aufwendungen zur Vorsorge gegen andere Gefährdungen, so lässt sich feststellen, dass es bereits an der Datengrundlage fehlt, die zu belastbaren quantitativen Aussagen führen kann.

Gesetzt den Fall, diese Datengrundlage ist eines Tages vorhanden, so müssen auf deren Basis – auch für kleine und mittlere Unternehmen – handhabbare Verfahren entwickelt werden, die Sicherheitslage in ihrer Produktions-IT-Infrastruktur zu ermessen und die dieser Situation angemessenen Schutzmaßnahmen zu definieren.

3.1.1.3 Neuere Entwicklungen

Auf internationaler Ebene wird die Entwicklung hin zu immer weitergehender Vernetzung mit den Begriffen „Internet of Things" (IoT) und „Cyber Physical Systems" (CPS) bezeichnet, die über die Anwendung in der Industrieproduktion hinaus auch den öffentlichen und persönlichen Bereich umfasst (z. B. Home Automation/Gebäudevernetzung, Smart Grids, Verkehrssysteme).

Hinsichtlich der IT-Sicherheit wurde hierbei sowohl in Deutschland als auch international das Hauptaugenmerk zunächst auf die Auswirkungen dieser Vernetzung im Bereich der so genannten „kritischen Infrastrukturen"[22] gelegt. Insbesondere bei der Energieversorgung wurden bereits erhebliche Anstrengungen zur Standardisierung und Regelung der IT-Sicherheit unternommen. In diesem Bereich existieren bereits die detailliertesten Richtlinien. Auch wenn sich Bedrohungs- und Risikopotenziale und die Priorisierung von Schutzzielen, z. B. bei Energieversorgungssystemen, nicht eins zu eins auf die Industrieproduktion übertragen lassen, so sind doch die beteiligten vernetzten Komponenten häufig ähnlich.

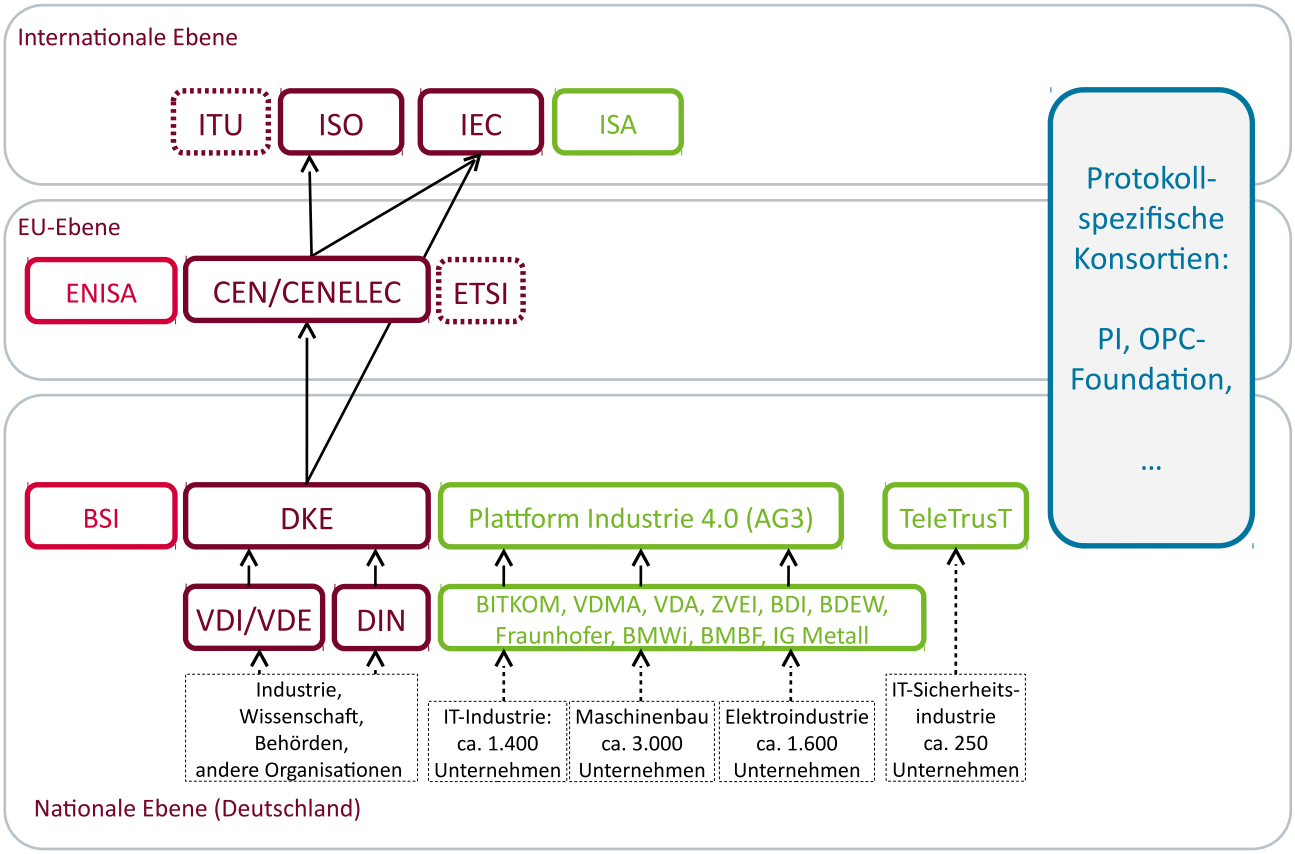
3.1.1.4 Übersicht über die wichtigsten Gremien und Institutionen

Bei den Gremien und Institutionen sind drei Ebenen (national, EU und weltweit) zu unterscheiden, innerhalb dieser Ebenen amtliche Institutionen (Ministerien, Ämter), Normierungsgremien mit teilweise staatlich oder supranational übertragenem Auftrag, sowie Branchen-, Hersteller- und Anwenderzusammenschlüsse.

Bei den nachfolgenden Schilderungen zu den Aktivitäten zur IT-Sicherheit für I4.0 in der Wirtschaft und bei öffentlichen Institutionen haben wir uns auf die Schnittmenge von Aktivitäten zur IT-Sicherheit und Aktivitäten hinsichtlich I4.0 konzentriert. Es gibt daneben eine große Vielfalt von Aktivitäten zu I4.0 bzw. zur IT-Sicherheit, bei denen der jeweils andere Aspekt eine Nebenrolle spielt. Diese werden, um den Fokus der Studie nicht zu verwässern, nicht aufgeführt.

22 Zur Definition "kritischer Infratrukturen", siehe http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/BevoelkerungKrisen/Sektoreneinteilung.pdf

Abbildung 3–2: Übersicht über die wichtigsten mit IT-Security bei IoT/CPS/I4.0 befassten Institutionen



Quelle: Fraunhofer ESK

Tabelle 3–1: Übersicht über Schwerpunkte und wichtige Ergebnisse beteiligter Organisationen

Organisation	Regionalität	Zweck	Schwerpunkt(e), wichtige Ergebnisse
Plattform Industrie 4.0	Deutschland	Koordinierung der I4.0 Aktivitäten in Deutschland	AG 3 für IT-Sicherheit bei I4.0; Ergebnisbericht vom April 2015; Erarbeitung von IT-Security für Referenz-architektur (RAMI4.0)
VDI/VDE	Deutschland	Fachgesellschaft	I4.0: Erarbeitung von Referenzarchitekturen (RAMI4.0)
DKE	Deutschland	Normierung	Erstellung konsensbasierter verbindlicher Normen, I4.0: Umsetzung IEC 62443 auf nationaler Ebene durch DKE 931.1
Bitkom e.V.	Deutschland	Branchenverband	Bewusstseinsschärfung für IT-Sicherheit bei I4.0
Verband der Automobil-industrie e.V. (VDA)	Deutschland	Branchenverband	Branchenspezifische Interessensvertretung in Gremien, die sich mit IT-Sicherheit für I4.0 befassen, Bewusstseins-schärfung, Schulung
Verband Deutscher Maschinen- und Anlagenbau e. V. (VDMA)	Deutschland	Branchenverband	Branchenspezifische Interessensvertretung in Gremien, die sich mit IT-Sicherheit für I4.0 befassen, Bewusstseins-schärfung, Schulung
Zentralverband Elektrotechnik- und Elektronikindustrie e.V. (ZVEI)	Deutschland	Branchenverband	Branchenspezifische Interessensvertretung in Gremien, die sich mit IT-Sicherheit für I4.0 befassen, Bewusstseins-schärfung, Schulung
TeleTrusT – Bundesverband IT-Sicherheit	Deutschland	Branchenverband	Bewusstseinsschärfung für IT-Sicherheit bei I4.0

→

Tabelle 3–1: Übersicht über Schwerpunkte und wichtige Ergebnisse beteiligter Organisationen (Fortsetzung)

Organisation	Regionalität	Zweck	Schwerpunkt(e), wichtige Ergebnisse
PROFIBUS und PROFINET International	international	Anwendervereinigung	Security-Richtlinie mit Umsetzung von Konzepten der IEC 62443
Bundesamt für Sicherheit in der Informationstechnik (BSI)	Deutschland	Behörde	Richtlinien, Grundschutzkataloge, Sicherung kritischer Infrastrukturen
Allianz für Cyber-Sicherheit	Deutschland	Vereinigung von Akteuren aller Art im Umfeld IT-Sicherheit	Aufbau einer Wissensbasis, Erfahrungsaustausch
Deutsche Akademie der Technikwissenschaften (acatech)	Deutschland	beratende Wissenschaftsorganisation	Handlungsempfehlungen für Politik und Wirtschaft
ENISA	EU	Behörde	Handlungsempfehlungen für IT-Security bei IACS
International Organization for Standardization	international	Normierung	ISO/IES 2700x Normen-Serie
International Electrotechnical Commission (IEC)	international	Normierung	IEC 62443
International Society of Automation (ISA)	international	Normierung	ISASecure Program
OPC-Foundation	international	Anwenderforum	OPC-UA Security Model
Industrial Internet Consortium (IIC)	USA/ international	Industrieintiative	Erarbeitung von Referenzarchitekturen (Industrial Internet Reference Architecture (IIRA))
Smart Factory 1.0	China	Regierungsinitiative	Umsetzung von I4.0 Verfahren mit vorhandenen Technologien zum schnellen Nutzen für die chinesische Industrie
Bundesministerium für Wirtschaft und Energie (BMWi)	Deutschland	Politik, Förderprogramme	Digitale Agenda 2014–17, Digitale Wirtschaft, AUTONOMIK für I4.0
Bundesministerium für Bildung und Forschung (BMBF)	Deutschland	Politik, Förderprogramme	Zukunftsprojekt Industrie 4.0, Programme für „Zivile Sicherheit“, „IKT 2020“
Europäische Kommission	EU	Politik, Förderprogramme	Forschungsförderung im Rahmenprogramm Horizon 2020
Kompetenzzentren für IT-Sicherheit: EC-SPRIDE, KASTEL, CISPA	Deutschland	Grundlagenforschung	Langfristige Strategien zur IT-Sicherheit

3.1.2 Aktivitäten der Wirtschaft und von Behörden in Deutschland

Zum aktuellen Wissensbestand bei der Informationssicherheit in der industriellen Automatisierung und Produktion auf technischer und organisatorischer Ebene haben mittlerweile sowohl national als auch international viele unterschiedliche Institutionen beigetragen.

Dazu gehören die bislang veröffentlichten Standards und Normen und Leitlinien. Sie werden durch Berichte und Studien ergänzt, welche z.T. branchenspezifisch die derzeitige Situation beschreiben sowie Handlungsnotwendigkeiten und Handlungsoptionen aufzeigen. Weitere Veröffentlichungen befassen sich mit speziellen Aspekten im Umfeld der IT-Sicherheit, wie Datenschutz oder Produktschutz.

Die genannten Behörden und Verbände organisieren zudem Fachtagungen und allgemeine Informationsveranstaltungen, in denen die Ergebnisse dieser Aktivitäten vorgestellt und diskutiert werden.

3.1.2.1 Plattform Industrie 4.0

Die Plattform Industrie 4.0 wurde von den drei Branchenverbänden BITKOM (ITK-Industrie), VDMA (Maschinen- und Anlagenbau) und ZVEI (Elektrotechnische Industrie) gegründet, um die Entwicklung hin zur zunehmenden Vernetzung von Produktion und Logistik in der deutschen Industrie zu koordinieren. Auf der Hannover Messe Industrie 2015 wurde die Plattform Industrie 4.0 in eine Dialogplattform unter der Regie des Bundeswirtschaftsministeriums überführt.[23, 24] An dieser neuen Plattform sind über

23 http://www.plattform-i40.de/presse/plattform-industrie-40/gemeinsame-plattform-industrie-40-startet
24 http://www.bmwi.de/DE/Themen/Industrie/industrie-4-0.html

die Spitzenverbände der Industrie hinaus die Bundesministerien für Wirtschaft und Energie und für Bildung und Forschung, die Fraunhofer Gesellschaft und die IG Metall beteiligt.

Mit dem Thema IT-Sicherheit befasst sich innerhalb der Plattform vornehmlich die AG 3 „Sicherheit vernetzter Systeme". Das Arbeitsprogramm, das sich die AG 3 bis Ende 2015 vorgenommen hat beinhaltet

- die Definition von Anforderungen an sichere Identitäten für Produkte, Prozesse und Maschinen,
- Identifikation von Bewertungsverfahren zur Überprüfung der IT-Sicherheit von einzelnen Komponenten (existierende Standards und Best Practices plus Identifikation von zusätzlichen Anforderungen),
- Identifikation von Bewertungsverfahren bei der Vernetzung von Komponenten und Systemdomänen,
- die Erstellung von Anforderungen aus Sicht der IT-Sicherheit an eine Referenzarchitektur von I4.0,
- Stimulierung von Forschungsprojekten und Normierungsaktivitäten.

Darüber hinaus hat sich die AG 3 in einem eigenen Arbeitspaket vorgenommen, der Managementebene von betroffenen Unternehmen die Bedeutung der IT-Sicherheit unter dem Gesichtspunkt des betriebswirtschaftlichen Nutzens greifbar zu machen.

Daneben existiert eine Arbeitsgemeinschaft, die sich mit den rechtlichen Rahmenbedingungen befasst nun als AG 4.

Eine Vernetzung mit anderen Akteuren auf nationaler oder internationaler Ebene besteht institutionell derzeit nicht, sondern kommt lediglich durch personelle Überschneidungen zustande.

Die nun „Verbändeplattform" genannte Vorgängerorganisation legte im März 2015 einen Bericht über die bislang erzielten Ergebnisse vor[25].

Zum Thema „Sicherheit vernetzter Systeme" wird dabei im Tenor insbesondere auf die Notwendigkeit einer Harmonisierung der IT-Security von Office-IT-Netzen und IACS-Netzen hingewiesen.

Der Neuentwicklung und Anpassung von Normen komme dabei eine besondere Bedeutung zu: „Die für Industrie 4.0 neuen Anforderungen und Maßnahmen sind entsprechend in Normen auszuarbeiten. Ob dies besser durch neue Normen oder Überarbeitung und Ergänzung existierender Normen umsetzbar ist, muss auch im Kontext anderer Normungsthemen im Rahmen von Industrie 4.0 bewertet werden."

Besonderes Augenmerk müsse dabei auch den im IACS-Bereich wichtigen Wechselwirkungen zwischen IT-Sicherheit und funktionaler Sicherheit („Safety") gewidmet werden, die im Bereich der Office-IT keine entsprechende Bedeutung haben.

Initiative „Industrial Data Space"

Auf der CeBit 2015 kündigte der Präsident der Fraunhofer-Gesellschaft zusammen mit der Bundesforschungsministerin eine Initiative zur Schaffung eines international offenen Datenraumes für die Wirtschaft als Ergänzung zu den Aktivitäten der Plattform I4.0 an. Diese Initiative wird von den Bundesministerien für Wirtschaft und Energie, für Verkehr und Infrastruktur und für Inneres sowie führenden Unternehmen und Wirtschaftsverbänden unterstützt. Ziel ist der Aufbau eines sicheren Datenraumes und „dessen Finanzierung und grundlegende Geschäftsmodelle marktkonform zu befördern". Die „Initiative Industrial Data Space" schafft einen virtuellen Raum und die zugehörigen Dienste, um einen sicheren Multi-Sourcing-Datenaustausch on Demand und auf Basis bestehender Netze zu ermöglichen. Der Industrial Data Space versteht sich als komplementärer Partner der echtzeitnahen und echtzeitfähigen Technologien im Sinne des Internet der Dinge oder der vierten industriellen Revolution.[26]

Erste Use Cases des Vorhabens sollen auf der Cebit 2016 präsentiert werden.

25 http://www.bmwi.de/BMWi/Redaktion/PDF/I/industrie-40-verbaendeplattform-bericht
26 https://www.fraunhofer.de/content/dam/zv/de/presse-medien/2015/industrial-data-space-eckpunkte.pdf

3.1.2.2 VDI/VDE

Der Verein Deutscher Ingenieure (VDI) und der Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE) haben in ihrer Unterorganisation „Gesellschaft Mess- und Automatisierungstechnik (GMA)“ den Fachausschuss 7.21 „Industrie 4.0“ errichtet. Dieser Ausschuss hat sich zunächst vorgenommen die Begriffe, Konzepte und Referenzmodelle für I4.0 mit dem Ziel einer „konsensbasierten Regelsetzung“[27] festzulegen.

Der Fachausschuss 5.22 „Security“ des VDI gibt die Richtlinie VDI/VDE 2182 „Informationssicherheit in der industriellen Automatisierung“ heraus (erstmals veröffentlicht im August 2007). Diese Richtlinie dient dem Zweck, eine „einheitliche, praktikable Vorgehensweise zwischen Herstellern, Integratoren und Betreibern von Automatisierungssystemen und -geräten abzustimmen, um die IT-Sicherheit der Anlagen über ihren gesamten Lebenszyklus zu gewährleisten“[28]. Sie enthält jedoch noch keine Vorgaben oder Empfehlungen, die sich auf Sachverhalte beziehen, die durch I4.0 neu in Erscheinung treten.

3.1.2.3 DKE

Die Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (DKE) ist die nationale Organisation für die Erarbeitung von Normen und Sicherheitsbestimmungen in dem Bereich der Elektrotechnik, Elektronik und Informationstechnik in Deutschland. Sie ist als „Fachbereich Normung“ des VDE und als Normenausschuss des Deutschen Instituts für Normung e.V. (DIN) Teil beider Organisationen.

Die DKE erstellt die verbindlichen Sicherheitsnormen für elektrotechnische Produkte und ist der nationale Vertreter in den korrespondierenden internationalen Normierungsgremien wie IEC, CEN, CENELEC und ETSI.

Derzeit überführt die DKE das internationale Regelwerk IEC 62443 (siehe Kapitel 3.1.3.3) in eine deutsche Norm, deren Veröffentlichung als DIN 62443 Anfang 2015 geplant ist.

Zum aktuellen Stand dieser Arbeiten siehe Internet-Webseiten des DKE (www.dke.de/de/std/Industrie40/Seiten/IEC62443.aspx).

Das Gremium „TBINK-AK IT Security“ (TBINK = Technischer Beirat internationale und nationale Koordinierung der DKE) beschäftigt sich mit dem Thema Funktionale Sicherheit und IT-Security, um branchenübergreifend die diversen Ansätze zu harmonisieren. Vertreten sind neben der Automatisierungsbranche u.a. auch die Kerntechnik, die Weiße Ware, Eisenbahnbranche und Flugsicherung. Die Ergebnisse des Arbeitskreises sollen in eine VDE Anwendungsregel einfließen.

3.1.2.4 Branchenverbände: BITKOM

Im Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) ist die IT- und Telekommunikationsbranche in Deutschland zusammengeschlossen. BITKOM treibt das Thema IT-Security bei I4.0 als einer der konstituierenden Branchenverbände der Plattform Industrie 4.0. Darüber hinaus hat der Verband einen eigenen Dialogkreis Industrie 4.0[29] eingerichtet, in dem jedoch keine eigenen spezifischen Aktivitäten zum Thema IT-Sicherheit bei I4.0 laufen.

Themen zur IT-Sichereit im allgemeinen werden in der Arbeitsgruppe Informations- und Cybersicherheit[30] (bisher ohne spezifische Unterarbeitsgruppen zu I4.0), das Thema Wertschöpfungketten und Logistik wird in der Arbeitsgruppe Digital Supply Chain[31] (bisher ohne spezifische Unterarbeitsgruppen zur IT-Sicherheit) behandelt.

Auch der Arbeitskreis Anwendung elektronischer Vertrauensdienste[32] arbeitet an einem Thema, dem für die IT-Sicherheit gerade bei I4.0 grundlegende Bedeutung zukommen wird.

Im Rahmen seiner BITKOM-Akademie[33] bietet der Verband auch Seminare zum Thema IT-Sicherheit an.

27 VDI/VDE-GMA: Industrie 4.0, Statusreport, Gegenstände, Entitäten, Komponenten (April 2014), Kap. 8.
28 VDI/VDE 2182 Blatt 1 Informationssicherheit in der industriellen Automatisierung – Allgemeines Vorgehensmodell, Kapitel 1.
29 https://www.bitkom.org/Bitkom/Organisation/Gremien/Industrie-4.0.html
30 https://www.bitkom.org/Bitkom/Organisation/Gremien/Informations-und-Cybersicherheit.html
31 https://www.bitkom.org/Bitkom/Organisation/Gremien/Digital-Supply-Chain.html
32 https://www.bitkom.org/Bitkom/Organisation/Gremien/Anwendung-elektronischer-Vertrauensdienste.html
33 https://www.bitkom-akademie.de/seminare/it-sicherheit

3.1.2.5 Branchenverbände: Verband der Automobilindustrie

Der Verband der Automobilindustrie (VDA) repräsentiert eine Industriebranche, in der der Entwicklung Richtung I4.0 bereits heute eine hohe Bedeutung zugemessen wird[34].

Beim VDA bestehen unterschiedliche Arbeitskreise, die sich mit dem Thema IT-Sicherheit beschäftigen. Mit Bezug auf die Produktion ist hier insbesondere der AK „IT Sicherheit in der Automobilindustrie" zu nennen, der sich mit dem Informationssicherheitsmanagement gemäß ISO 27001 bei den Mitgliedsunternehmen befasst. Anfang 2015 hat sich der Arbeitskreis in neun Arbeitsgruppen zu unterschiedlichen Themen, wie Prototypenschutz oder Kollaboration, über Internetplattformen neu organisiert. Ergebnisse werden erst im Laufe des Jahres 2015 erwartet.

Eine eigene Schwerpunktaktivität zu den spezifischen Aspekten der IT-Sicherheit der industriellen Automatisierungs- und Steuerungssysteme im Sinne von Industrie 4.0 (IEC 62443) wurde bislang nicht aufgenommen. Da aber die meisten Mitgliedsfirmen neben der VDA-Mitgliedschaft auch über eine Mitgliedschaft im VDMA verfügen, liegt es auch nahe, diese Aktivitäten dort anzusiedeln, wo die Hersteller und Anwender dieser Anlagen zusammenkommen.

3.1.2.6 Branchenverbände: Verband Deutscher Maschinen- und Anlagenbau

Im Verband Deutscher Maschinen- und Anlagenbau (VDMA) sind ca. 3000 Unternehmen des Maschinen- und Anlagenbaus in Deutschland zusammengeschlossen und er gehört zu den Trägern der Plattform Industrie 4.0.

Der VDMA selbst hat eine Arbeitsgemeinschaft „Produkt- und Know-how-Schutz eingerichtet (protecting)", die sich auch mit Themen im Umfeld I4.0 befasst.

Ende 2013 wurde die vom VDMA geförderte INS Studie „Status quo des Know-how-Schutzes im Maschinen- und Anlagenbau (Nov. 2013)"[35] vorgestellt. Gleichzeitig wurde unter dem Titel „IT-Sicherheit meets Industrie 4.0"[36] gemeinsam mit dem Bundesministerium für Bildung und Forschung (BMBF) eine Initiative für ein gemeinsames Vorgehen von Wirtschaft und Wissenschaft etabliert, um Konzepte für einen wirksamen IT-Schutz für vernetzte Infrastrukturen im Bereich der Produktion zu entwickeln.

Mit der weltweiten Organisation Global Standards One (GS1) wurde weiterhin eine Kooperation für sichere Wertschöpfungsketten vereinbart, „um Erfahrungen aus anderen Branchen im Bezug zu Kennzeichnungstechnologien und Identifikationsstandards sowie deren Umsetzung, zum Vorteil der Unternehmen des deutschen Maschinen- und Anlagenbaus, zu nutzen. Konkret werden Aktivitäten zur Weiterentwicklung und Ausgestaltung vorhandener Identifikationsstandards sowie deren branchentypische Implementierung beiderseitig unterstützt, z. B. durch die kooperative Erarbeitung von Anwendungsempfehlungen."[37]

3.1.2.7 Branchenverbände: Zentralverband Elektrotechnik- und Elektronikindustrie e. V.

Im Zentralverband Elektrotechnik- und Elektronikindustrie e.V. (ZVEI) sind ca. 1.600 Unternehmen der Elektrotechnik- und Elektronikindustrie zusammengeschlossen. Der ZVEI gehört zu den Trägerorganisationen der Plattform Industrie 4.0.

Neben den in der Plattform Industrie 4.0 konzentrierten Arbeiten zur IT-Sicherheit finden insbesondere im Fachverband Sicherheit weitere Aktivitäten in diesem Themenbereich statt.

So hat er z. B. im November 2013 ein Positionspapier „Cyber-Sicherheit und Schutz vor Wirtschaftsspionage" veröffentlicht und ist Partner der Allianz für Cyber-Sicherheit des BSI.

3.1.2.8 Branchenverbände: TeleTrusT – Bundesverband IT-Sicherheit e. V.

Beim TeleTrusT – Bundesverband IT-Sicherheit e.V. handelt es sich um eine Interessensorganisation von Firmen aus der IT Sicherheitsindustrie. Auch diese Organisation hat

34 „Die deutschen Early Adopters von Industrie 4.0 sind vor allem unter Automobilzulieferern mit einer Unternehmensgröße plus 500 Mitarbeiter zu finden. Wohl auch deshalb, weil der Wettbewerb in dieser Branche schon heute die schnelle Umsetzung von Kundenanforderungen und eine bedarfssynchrone Produktion verlangt" (H. Reichardt, Freudenberg IT), http://www.automotiveit.eu/mittelstand-entdeckt-industrie-4-0/news/id-0043378

35 http://pks.vdma.org/documents/105969/779856/Studie%20INS%20Know-how-Schutz/dd15e8a8-8e0a-49ac-8005-f949d50bf53a

36 http://www.vdivde-it.de/KIS/aktuelles/it-sicherheit-meets-industrie-4.0

37 http://pks.vdma.org/article/-/articleview/5078421

begonnen, sich dem Thema IT-Sicherheit in der industriellen Automatisierung und Produktion zu widmen.

Im TeleTrusT beschäftigt sich die nun schon seit einigen Jahren existierende und regelmäßig tagende (mittlerweile über 18 Sitzungen) AG „Smart Grids/Industrial Security“ mit dem Thema I4.0.

Dazu sind derzeit zwei Papiere in Arbeit, wovon sich eines mit dem Verhältnis von Safety and Security beschäftigt, während das andere sich eher allgemeinen IT-Security-Themen für Industrie 4.0 mit dem Ziel von Handlungsempfehlungen für das Management in Politik und Wirtschaft sowie für Produktmanager (Awareness) und den dabei zentralen Forderungen von TeleTrusT beschäftigt.

Derzeit liegen bis auf eine Pressemitteilung[38] noch keine veröffentlichten Ergebnisse vor.

TeleTrusT sieht in I4.0 große Chancen für den Industriestandort Deutschland und forderte daher im Oktober 2014 schnelles Handeln in den folgenden Punkten:

- Besondere Berücksichtigung von Security by Design, Privacy by Design und Safety by Design bei Planung und Entwicklung von I4.0;
- Förderung einer politischen Allianz zwischen deutscher IT-Sicherheitswirtschaft und deutschem Maschinenbau im Rahmen der Digitalen Agenda der Bundesregierung;
- Durchführung von Maßnahmen zur ‚Awareness‘-bildung und Schaffung gesetzlicher Rahmenbedingungen zur Umsetzung von IT-Sicherheit in ‚Industrie 4.0‘;
- Stärkere Berücksichtigung von IT-Sicherheit und Safety in der Ausbildung von Ingenieuren auch im Maschinenbau.

Die vorhandenen Chancen lassen sich laut TeleTrusT nur nutzen, wenn I4.0 auch sicher ist. IT-Sicherheit ist laut TeleTrusT „ein neuer entscheidender Faktor für den Werterhalt der Marke „Made in Germany““.

TeleTrusT führte bis September 2015 in Kooperation mit der Hochschule Ostwestfalen-Lippe eine nichtrepräsentative Umfrage zu „IT-Sicherheit bei Industrie 4.0“ durch, an der insgesamt 126 Unternehmen – sowohl Hersteller, Integratoren als auch Betreiber – teilgenommen haben. TeleTrusT fragte den Stand der Informationssicherheit bei I4.0-Projekten ab und schlussfolgerte, dass die IT-Sicherheit bei den meisten I4.0-Projekten bereits beachtet wird. Die Umfrage zeigt aber, dass der Grad der Umsetzung in den jeweiligen Projekten sehr unterschiedlich bewertet wird. Die Aussagen lassen den Schluss zu, „dass IT-Sicherheit jedenfalls bei den meisten befragten Unternehmen noch nicht dort angekommen ist, wo auch Bundeswirtschaftsminister Sigmar Gabriel sie gerne sähe“. Laut TeleTrusT müssen die betroffenen Unternehmen ihre IT-Systeme besser schützen und ein ausgeprägteres IT-Sicherheitsbewusstsein entwickeln.[39]

3.1.2.9 PROFIBUS und PROFINET International (PI)

PI versteht sich zwar als weltweite Interessengruppe, die Hersteller, Integratoren und Anwender der Technologien PROFIBUS und PROFINET vereinigt, wird aber de facto von der deutschen Industrie unter der maßgeblichen Führung von Siemens getragen und getrieben.

Im November 2013 hat die Projektgruppe 10 „PN Security“ die „PROFINET Security Richtlinie“ veröffentlicht, die ein Konzept zum Schutz aller Automatisierungskomponenten vorstellt und einen „Leitfaden für Anwender und Betreiber industrieller Netzwerke, speziell mit dem Ethernet-basierten PROFINET“[40] darstellt.

3.1.2.10 Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn ist laut Gesetz vornehmlich für die Sicherheit der IT-Infrastruktur des Bundes zuständig. Darüber hinaus kümmert sich das BSI um alle Aspekte der IT-Sicherheit, die nationale Interessen berühren, insbesondere um die Sicherheit kritischer Infrastrukturen (u.a. Energie- und

38 Zukunft des Industriestandortes Deutschland: IT-Sicherheit als Qualitätsmerkmal für „Made in Germany“/ Jetzt Rahmenbedingungen für sichere „Industrie 4.0“ schaffen, https://www.teletrust.de/uploads/media/PM-141006-TeleTrusT-Industriestandort_Deutschland.pdf, zuletzt abgerufen am 12.2.2015.

39 IT-Sicherheit bei „Industrie 4.0“: Botschaft angekommen, Umsetzung hapert; Umfrageergebnisse zu IT-Sicherheit bei Industrie 4.0/ Bestandsaufnahme des aktuellen Sicherheitsniveaus bei Industrie 4.0-Projekten, Pressemitteilung TeleTrusT, https://www.teletrust.de/uploads/media/PM-150916-TeleTrusT-Industrie4_0-Umfrageergebnis.pdf, vom 16.09.2015.

40 PROFINET Security Richtlinie, Version 2.0 (Nov. 2013), PROFIBUS Nutzerorganisation e.V. Karlsruhe (Hrsg.)

Wasserversorgung, Verkehrssysteme, Öffentliche Sicherheit und Ordnung, Gesundheitsversorgung).

Für die IT-Sicherheit in der deutschen Industrieproduktion und den damit verbundenen Wertschöpfungsketten gibt es bis jetzt außerhalb dieser „kritischen Infrastrukturen" keine gesetzliche Grundlage für Vorgaben durch das BSI in Sinne von durch die Industrie zwingend einzuhaltenden Vorschriften. Da sowohl das geistige Eigentum der Industrie als auch die Verfügbarkeit von Maschinen und Anlagen als „kumulativ kritisch"[41] betrachtet werden können, gibt das BSI jedoch in diesem Bereich in Absprache mit den einschlägigen Gremien der Industrieverbände Empfehlungen heraus.

Das BSI hat mit seinem „ICS Security Kompendium"[42] ein umfassendes Grundlagenwerk für die IT-Sicherheit bei industriellen Steuerungssystemen aufgelegt. Es besteht aus zwei Teilen. Der erste richtet sich an die Betreiber von industriellen Steuerungsanlagen, der zweite an deren Hersteller.

Der erste Teil wurde 2013 veröffentlicht und richtet sich an Betreiber von industriellen Steuerungsanlagen. Der zweite Teil richtet sich an Hersteller von ICS-Komponenten.

Zur Unterstützung der Analyse und Implementierung von IT-Sicherheitsmaßnahmen im industriellen Kontext wird durch das BSI ein Werkzeug zur Verfügung gestellt:

- Light and Right Security ICS (LARS ICS): Ein Werkzeug für den leichtgewichtigen Einstieg in industrielle Cyber-Security[43]

Darüber hinaus definiert das BSI IT-Grundschutzkataloge.

3.1.2.11 Allianz für Cyber-Sicherheit

Die „Allianz für Cyber-Sicherheit" (www.allianz-fuer-cybersicherheit.de) wurde auf Initiative des BSI gegründet. An ihr nehmen mittlerweile über 1.100 Institutionen (Unternehmen, Behörden, Institute etc.) teil. Ziele sind dabei der Aufbau einer Wissensbasis und der Erfahrungsaustausch unter den Mitgliedern.

Die Allianz für Cyber-Sicherheit befasst sich intensiv mit Themen der IT-Sicherheit im industriellen Umfeld und hat (Stand Januar 2015) bereits eine Reihe von Veröffentlichungen zu Themen herausgebracht wie:

- „Sicherer Einsatz von ICS-spezifischen Apps",
- „Fernwartung im industriellen Umfeld"
- „Leitfaden-Cyber-Sicherheits-Check"

Zur Unterstützung der Analyse und Implementierung von IT-Sicherheitsmaßnahmen werden durch die Allianz für Cybersicherheit Werkzeuge zur Verfügung gestellt. Beispiele dafür sind im industriellen Bereich:

- Light and Right Security ICS (LARS ICS): Ein Werkzeug für den leichtgewichtigen Einstieg in industrielle Cyber-Security
- ICS-Security Awareness-Toolkit[44]

Neben für die Allgemeinheit öffentlich verfügbaren Informationen stellt die Allianz für Mitglieder auch Warnmeldungen und Schwachstelleninformationen (sowohl eigene als auch solche von Partnerorganisationen im Ausland) zur Verfügung.

3.1.2.12 Deutsche Akademie der Technikwissenschaften (acatech)

Der acatech „Arbeitskreis Industrie 4.0" veröffentlichte im April 2013 seine „Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0", in dem die IT-Sicherheit in diesem Umfeld als erfolgskritischer Faktor für eine erfolgreiche Implementierung der damit einhergehenden Technologien und Verfahren identifiziert wurde und entsprechende Handlungsempfehlungen gegeben wurden.[45]

41 Unter „kumulativ kritisch" ist zu verstehen, dass zwar ein einzelner Schadensfall nicht als kritisch betrachtet werden muss, entsprechende gleichartige Vorfälle in großer Zahl bzw. daraus resultierende Kaskaden-Effekte hingegen zu erheblichem Schaden für die deutsche Wirtschaft führen können.

42 BSI, Allgemeine Empfehlungen Industrial Control System Security, https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/empfehlungen_node.html, zuletzt abgerufen am 17.07.2015.

43 LARS ICS: Ein Werkzeug für den leichtgewichtigen Einstieg in industrielle Cyber-Security, https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Tools/LarsICS/LarsICS.html, zuletzt abgerufen am 19.11.2015.

44 Allianz für Cyber-Sicherheit bietet ICS-Security Awareness-Toolkit an, http://www.secupedia.info/aktuelles/allianz-fuer-cyber-sicherheit-bietet-ics-security-awareness-toolkit-an-2328, zuletzt abgerufen am 15.7.2015.

45 Abschlussbericht des Arbeitskreises Industrie 4.0, S. 50 ff.

Aktuell (2012–2015) läuft unter der Regie von acatech das Projekt „Industrie 4.0 – Internationaler Benchmark, Zukunftsoptionen und Handlungsempfehlungen für die Produktionsforschung (INBENZHAP)“, das sich die Bearbeitung folgender Fragen vorgenommen hat[46]:

- Wie ist der Entwicklungsstand in führenden Industrienationen?
- Werden in Deutschland die Voraussetzungen gegeben sein, die Rolle des Leitanbieters wahrzunehmen? Treten neue Anbieter von I4.0-Ausrüstung in die Wettbewerbsarena?
- Hat Deutschland mittelfristig das Potenzial für einen Leitmarkt? Wo eröffnen sich attraktive Märkte für I4.0?

Dabei steht auch das Thema der Informationssicherheit auf der Agenda.

3.1.3 Aktivitäten auf internationaler Ebene

3.1.3.1 ENISA

Bei der European Network and Information Security Agency (ENISA) handelt es sich um das Pendant zum BSI auf EU-Ebene. Sie betreibt insbesondere ein europaweites Monitoring von IT-Sicherheitsvorfällen. Ihre Aufgaben sind aber im Vergleich zum BSI viel stärker auf Koordinierung und Beratung beschränkt.

Ihre Veröffentlichungen beziehen sich vornehmlich auf allgemeine Aspekte der IT-Sicherheit und auf die Sicherheit kritischer Infrastrukturen. Speziell mit der IT-Sicherheit bei ICS und SCADA hat sich die ENISA in zwei Studien befasst.

Die erste unter dem Titel „ Good practices for an EU ICS testing coordination capability“[47] widmet sich dem Zweck, einheitliche und konsistente Testmöglichkeiten zur Überprüfung der Sicherheit von von industriellen Steuerungssystemen zu etablieren. Dazu gehört auch unter dem Titel „ICS Security Related Working Groups, Standards and Initiatives“[48] eine gute Übersicht über die weltweit laufenden Arbeiten.

Ein zweiter Report aus dem Jahr 2012[49] enthält Handlungsempfehlungen an die Mitgliedsstaaten der EU zur Adressierung der IT-Sicherheit von industriellen Steuerungssystemen. Er basiert auf einer Analyse der aktuellen Sicherheitssituation und einer Befragung der betroffenen Interessenvertreter aus der Industrie.

Die Reports adressieren jedoch vor allem die aktuellen Sicherheitsprobleme, durch I4.0-Konzepte neu hinzukommenden Probleme werden in beiden Studien nicht tiefer beleuchtet.

2014 veröffentlichte die ENISA weiterhin eine Studie zur Zertifizierung der IT-Sicherheitskenntnisse von ICS und SCADA Experten.

3.1.3.2 International Organization for Standardization

Bei der Internationalen Organisation für Normung – kurz ISO (englisch: International Organization for Standardization) handelt es sich um eine der drei international anerkannten Institutionen, die weltweit auf Konsens basierende Normen und Standards festlegt. Die ISO befasst sich dabei mit allen Bereichen mit Ausnahme der Elektrotechnik, für die die IEC (s. 3.1.3.3) zuständig ist, und außer der Telekommunikation, die in die Kompetenz der Internationalen Fernmeldeunion (ITU) fällt.

Im Bereich der IT-Sicherheit ist insbesondere die ISO/IEC-Standardarisierungsreihe 270xx von großer Bedeutung, die von der ISO gemeinsam mit ihrer Schwesterorganisation IEC verantwortet wird. Die Standardisierungsreihe ISO/IEC 270xx umfasst derzeit mehr als 20 Einzelnormen, die sich vornehmlich auf die organisatorischen Aspekte eines standardisierten IT-Sicherheits-Managements richten.

Bereits heute ist es im Geschäftsleben für viele Unternehmen von Bedeutung, gegenüber ihren Kunden eine Zertifizierung

46 Webseite des Projektes: http://www.acatech.de/?id=2352
47 https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/good-practices-for-an-eu-ics-testing-coordination-capability
48 https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/good-practices-for-an-eu-ics-testing-coordination-capability/ics-security-related-working-groups-standards-and-initiatives/at_download/file
49 https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states/at_download/fullReport

ihres IT-Sicherheitsmanagements nach ISO/IEC 27001 vorweisen zu können.

Die Normenreihe ISO/IEC 270xx enthält bislang keine Richtlinien oder Empfehlungen, die für die industrielle Produktion und ihre Wertschöpfungsketten spezifisch wären. Spezifischere Richtlinien und Empfehlungen für die IT-Sicherheit im Produktionsumfeld sind jedoch in der Regel bezüglich ihrer Sicherheitsmanagementaspekte aus ISO/IEC 270xx abgeleitet. Sie müssen sich schlussendlich in das Gesamtkonzept für die IT-Sicherheit in einem Unternehmen einfügen.

3.1.3.3 International Electrotechnical Commission

Das Technical Committee 65 (Industrial-process measurement, control and automation) ist das Dach-Kommittee der International Electrotechnical Commission (IEC) für IACS Angelegenheiten.

Zu den Aufgaben des TC65 gehört die Erstellung und Betreuung eines Rahmenwerkes für Netzwerk- und Systemsicherheit.

Die IEC hat sich dementsprechend in ihrer Normenreihe IEC 62443 mit der IT-Sicherheit für industrielle Steuerungssysteme befasst.

IEC 62443 gilt derzeit als der einzige umfassende Ansatz für standardisierte IT-Sicherheitsrichtlinien für industrielle Steuerungssysteme. In vielen Ländern laufen derzeit Anstrengungen diese Standards auf nationaler Ebene umzusetzen (z. B. bei DKE in Deutschland und NIST in USA).

Aufgabe des Unterarbeitskreises SC65C (Subcommitte 65 C, Industrial networks) ist unter anderem, sich um eine Überarbeitung der Feldbus-Standards hinsichtlich der IT-Sicherheit entsprechend den Empfehlungen der IEC 62443 zu kümmern.

Ein Anfang 2014 neu gegründeter Unterarbeitskreis „Ad-Hoc Group „Framework Toward Coordinating Safety, Security“ widmet sich auf Initiative von Japan den Wechselwirkungen und gegenseitigen Abhängigkeiten von funktionaler Sicherheit und IT-Sicherheit

3.1.3.4 International Society of Automation

Die International Society of Automation (ISA) ist eine ursprünglich US-amerikanische Organisation, die im Laufe der Zeit immer mehr internationalisiert wurde und seit 2008 ihren heutigen Namen trägt. Im Bereich der Industrieautomatisierung ist die ISA heute eines der maßgeblichsten internationalen Gremien.

Besondere Bedeutung auf dem Feld der IT-Sicherheit für die industrielle Automatisierung erlangt die ISA durch das von ihrem ISA Security Compliance Institute organisierte „ISASecure Program“. Mit diesem Programm wird versucht, den im IEC 62443 Standard definierten „IAC[50] Security Lifecycle“ in die Praxis umzusetzen.

3.1.3.5 NAMUR

Bei der „User Association of Automation Technology in Process Industries“ (NAMUR) handelt es sich um einen internationalen Zusammenschluss von über 130 Firmen als Interessensvertretung der Prozessindustrie auf dem Gebiet der Automatisierungstechnik.

Zum Thema IT-Sicherheit hat der Arbeitskreis 4.18 „Automation Security“ im Juni 2015 eine Empfehlung „Automation Security Agenda 2020 – Design, Implementierung und Betrieb industrieller Automatisierungssysteme“ veröffentlicht (NE153).[51, 52] Bereits aus dem Jahre 2006 existiert außerdem ein Arbeitsblatt „IT-Sicherheit für Systeme der Automatisierungstechnik: Randbedingungen für Maßnahmen beim Einsatz in der Prozessindustrie“ (NA115), dessen Ziel es ist, „aus Anwendersicht die Randbedingungen im Bereich Automatisierungstechnik für IT-Sicherheitsprodukte darzulegen“.

3.1.3.6 OPC-Foundation

Die OPC-Foundation spezifiziert mit OPC-UA (ursprünglich: Object Linking and Embedding for Process Control - Unified Architecture, heute steht OPC einfach für „Openess, Productivity, Collaboration) ein Protokoll, das für die Kommunikation zwischen den Komponenten in industriellen Produktionsanlagen eine zunehmende Verbreitung findet.

50 IAC = Industrial Automation and Control
51 http://www.namur.net/nc/en/recommendations-and-worksheets/current-nena.html?tx_nena_pi1%5Bda%5D=423
52 http://www.chemanager-online.com/themen/mess-automatisierungstechnik/automation-security-agenda-2020

Das Thema der IT-Security wird hier in der Spezifikation „OPC-UA Part2: Security Model“ adressiert. OPC-UA gehört damit zu den ersten IACS-spezifischen Protokollen, bei dem von Beginn der Entwicklung an der IT-Sicherheitsaspekt eine zentrale Rolle spielte.

OPC-UA Security befasst sich mit der Authentifizierung von Clients und Servern, der Integrität und Vertraulichkeit der ausgetauschten Nachrichten und der Prüfbarkeit von Funktionsprofilen.

OPC UA bietet integrierte Security by Design und die Möglichkeit der Modellierung von Diensten und ist derzeit die einzige Referenzempfehlung für Kommunikationstechnologien des Lenkungskreises der Plattform Industrie 4.0.

3.1.3.7 Industrial Internet Consortium

Das Industrial Internet Consortium (IIC) ist ein Zusammenschluss vornehmlich US-amerikanischer Firmen, das sich mit den Auswirkungen von IoT und CPS auf die Industrie beschäftigt. Der Begriff „Industrial Internet“ ist hier synonym zum deutschen „Industrie 4.0“ zu verstehen. Diese Vereinigung, die sich inzwischen auch für die Beteiligung nicht-amerikanischer Firmen und Institutionen (aus Deutschland z. B. Bosch, Detecon, Infineon, SAP, Siemens, Fraunhofer, TU Darmstadt) geöffnet hat, hat im April 2015 eine Referenz-Architektur (Industrial Internet Reference Architecture, IIRA) verabschiedet. Das IIC ist in verschiedenen Arbeitsgruppen organisiert. Eine dieser Arbeitsgruppen ist die 2014 gegründete „Security Working Group“[53], die sich laut Fortschrittsbericht vom Mai 2015 zum Ziel gesetzt hat, ein Framework für IT Sicherheit und Datenschutz für die IIRA zu erstellen. Dieses Framework ist Stand Juli 2015 noch in Arbeit. Dabei sollen folgende Hauptpunkte adressiert werden:

- Identifizierung der möglichen Bedrohungen und Erstellung von entsprechenden IT Sicherheitsempfehlungen.
- Identifizierung von Sicherheitslücken und Erstellung von daraus resultierenden Anforderungen zur Weiterleitung an die Standardisierungsgremien.
- Handlungsempfehlungen für die Unternehmen, durch welche Maßnahmen sie mindestens einen IT-Sicherheits-Grundschutz erreichen können.
- Empfehlungen, wie Unternehmen ihr eigenes Niveau an IT-Sicherheit und Datenschutz messen, beurteilen und dokumentieren können.
- Erstellung von Test-Konfigurationen für die IT-Sicherheit auf der Basis von Referenz-Architekturen.

Die Arbeiten dazu haben im Jahr 2014 begonnen, es liegen jedoch derzeit noch keine Ergebnisse vor.

Im Unterschied zur bisherigen deutschen Plattform Industrie 4.0 umfasst die Aufgabenstellung des IIC auch die Aspekte von Automotive und Gesundheitswesen.

Stand Mai 2015 bestand das IIC aus über 160 Mitgliedern aus 53 Ländern.

3.1.3.8 Smart Factory 1.0

Smart Factory 1.0[54] ist ein Projekt der Volksrepublik China, in dem ein Modell für die chinesische Industrie entwickelt werden soll, das die Erfordernisse einer vernetzten industriellen Produktion in China adressiert. Initial für das Projekt Smart Factory 1.0 waren nicht zuletzt die Diskussionen über Industrie 4.0 auf der Hannover Messe Industrie 2013.

Der Fokus liegt hier sehr stark auf einer schnellen Umsetzbarkeit mit vorhandenen Technologien und weniger auf noch zu entwickelnden neuen Technologien.

Ein wichtiges Thema ist dabei auch die Interoperabilität der verwendeten Ansätze und Lösungen.

Über Konzepte zur IT-Sicherheit im Kontext von Smart Factory 1.0 liegen derzeit keine Veröffentlichungen vor.

Im Mai 2015 wurde eine enge Kooperation zwischen Deutschland und China bei der Standardsetzung für I4.0 vereinbart.[55]

53 http://iiconsortium.org/wc-security.htm
54 http://www.controleng.com/single-article/smart-factory-10-is-helping-china-s-industry-to-upgrade/99453551b21b649559dad2fe91d68708.html
55 http://www.bmwi.de/DE/Themen/technologie,did=708634.html

3.1.3.9 NIST

Das US-amerikanische National Institute of Standards and Technology (NIST) spielt in den USA sowohl eine dem deutschen DKE (nationale Standardisierung) als auch dem deutschen BSI (Mindestanforderungen an die Informationssicherheit von IT-Systemen der US-Regierung) vergleichbare Rolle. Im Mai 2015 wurde der „Guide to Industrial Control Systems (ICS) Security" in einer überarbeiteten Version[56] veröffentlicht. Diese Neuausgabe der 2013 erstmals publizierten Leitlinie zur IT-Sicherheit für IACS enthält insbesondere Anleitungen wie die in der SP 800-53[57] detaillierten Maßnahmen zur Sicherung von IT-Systemen der Regierung auch für IACS adaptiert und angewendet werden können.

3.1.4 IT-Security-bezogene Förderprojekte/ Förderprogramme zu I4.0

3.1.4.1 Bundesministerium für Wirtschaft und Energie

Das Programm „Autonomik für Industrie 4.0" wurde vom Bundeswirtschaftsministerium im Jahr 2014 aufgesetzt.

„Mit dem Technologieprogramm „AUTONOMIK für Industrie 4.0" sollen modernste I&K-Technologien mit der industriellen Produktion unter Nutzung von Innovationspotenzialen verzahnt und die Entwicklung innovativer Produkte beschleunigt werden. Ziel ist es, Deutschlands Spitzenstellung als hochwertiger Produktionsstandort und als Anbieter für modernste Produktionstechnologien zu stärken."[58]

Für die Projekte dieses Programmes besteht im Rahmen der Begleitforschung eine Arbeitsgruppe, die sich mit dem Querschnittsthema IT-Sicherheit befasst.[59]

Ein Übersichtsartikel[60] vom Januar 2015 fasst die bisherigen Ergebnisse und Erkenntnisse zusammen.

3.1.4.2 Bundesministerium für Bildung und Forschung

Das Bundesministerium für Bildung und Forschung (BMBF) fördert im Rahmenprogramm „Forschung für die zivile Sicherheit" im Zeitraum 2012–2017 auch Projekte mit dem Fokus auf IT-Sicherheit. Einer der Förderschwerpunkte ist hierbei „Sicherheit von Infrastruktur und Wirtschaft". Im Hinblick auf die IT-Sicherheit in der Industrie sind dabei Projekte zu Querschnittsthemen wie „Sicheres Cloud-Computing" von Relevanz. Insgesamt liegt bei diesem Programm der Fokus jedoch sehr stark auf der Sicherheit kritischer Infrastrukturen und weniger auf der IT-Sicherheit der Industrieproduktion.

Daneben betreibt das BMBF gemeinsam mit dem Bundesinnenministerium (BMI) ein „Arbeitsprogramm IT-Sicherheitsforschung"[61], das diverse Projekte fördert, deren Ergebnisse auch im Bereich der Industrieautomatisierung anwendbar sind, die sich jedoch nicht explizit mit deren spezifischen Problemen beschäftigen. Bei der Übertragung dieser Ergebnisse auf industrielle Steuerungsanlagen müssen jedoch die dort herrschenden besonderen Randbedingungen immer noch einmal speziell bewertet werden. Ein Beispiel dafür ist etwa Projekt DynFire, bei dem es um „Erforschung und Entwicklung sicherer Fernwartung über das Internet" geht.

Im März 2015 beschloss die Bundesregierung das neue Forschungsprogramm zur IT-Sicherheit „Sicher und selbstbestimmt in der digitalen Welt". Bis 2020 will das BMBF Fördermittel in Höhe von rund 180 Millionen Euro für dieses Programm ausgeben. Das Forschungsrahmenprogramm konzentriert sich dabei auf die vier Schwerpunkte: Neue Technologien, sichere und vertrauenswürdige Informations- und Kommunikationssysteme, Anwendungsfelder der IT-Sicherheit und Privatheit und Schutz von Daten. Die IT-Sicherheit für die Industrie der Zukunft wird hierbei besonders hervorgehoben.

Im Juni 2015 gab das BMBF bekannt[62], dass im Sommer 2015 ein Nationales Referenzprojekt für IT-Sicherheit in der Industrie 4.0 mit einem Fördervolumen von 20 Millionen Euro starten wird. In diesem Projekt sollen IT-Sicher-

56 NIST SP 800-82 Revison 2, http://dx.doi.org/10.6028/NIST.SP.800-82r2
57 Security and Privacy Controls for Federal Information Systems and Organizations NIST SP 800-53, revision 4, http://dx.doi.org/10.6028/NIST.SP.800-53r4
58 http://www.autonomik40.de/
59 http://www.digitale-technologien.de/DT/Navigation/DE/Foerderprogramme/Autonomik_fuer_Industrie/Querschnittsthemen/IT-Sicherheit/it-sicherheit.html
60 I. Seifert, „Mehr Sicherheit für die Produktion von morgen", Digital Engineering Magazin 01/2015, S.57
61 http://www.bmbf.de/press/3749.php
62 BMBF-Pressemitteilung Nr. 077/2015.

heitslösungen für 4 konkrete Fallbeispiele demonstriert werden („verlässliche Lösungen, die zeigen, wie Industrie 4.0 auch für kleine und mittlere Unternehmen funktionieren kann“):

- Kundenindividuelle Produktion (Losgröße 1)
- Technologiedaten Marktplatz (wie kann man Daten aus den I4.0 Prozessen vermarkten)
- Sichere Dienste (z. B. für Fernwartung)
- Visueller IT-Security Leitstand (Entwicklung von Metriken, mit deren Hilfe der Zustand der IT-Sicherheit einer Anlage für Nichtexperten verständlich visuell dargestellt werden kann)

An diesem Projekt werden mehrere Industriekonzerne (u. a. Siemens, Bosch, VW, Trumpf und Infineon), mittelständische Firmen und Forschungsinstitutionen (u. a. Fraunhofer, TU Darmstadt, TU München) beteiligt sein.

3.1.4.3 Europäische Kommission

Die europäische Kommission fördert in ihren Forschungsrahmenprogrammen FP7 (2007–2013) und Horizon 2020 (2014–20) ebenfalls Forschungsprojekte im Zusammenhang mit dem „Internet of Things“.

Von den bereits abgeschlossenen Projekten ist hier vor allem das Projekt „Internet-of-Things Architecture“[63] zu nennen, das einen Vorschlag für ein Referenz-Architekturmodell generiert hat, in dem auch den Aspekten von Vertrauensbeziehungen, Datenschutz und IT Sicherheit große Aufmerksamkeit gewidmet wird.[64] Dieses Forschungsprojekt beschäftigte sich jedoch wie viele andere mit einer IoT-Architektur auf einer hohen Abstraktionsebene und betrachtete nicht spezifische Aspekte industrieller Produktionsnetze.

3.1.5 IT-Security-bezogene Forschung im akademischen Bereich zu I4.0

IT-Sicherheitsforschung mit den unterschiedlichsten Schwerpunkten wird weltweit an einer Vielzahl von Universitäten, Hochschulen und außeruniversitären Forschungseinrichtungen betrieben. Dieses Kapitel soll einen Überblick darüber geben, ob und wo in Deutschland und im Ausland Forschung zur IT-Sicherheit explizit mit dem Schwerpunkt I4.0/„Internet of Things“ stattfindet.

Ein Beispiel ist das vom BMBF geförderte I4.0-Projekt Secure Plug-and-Work[65], das eine Art „Universalschnittstelle für Anlagenkomponenten“ definiert und implementiert. Ähnlich zum USB-Standard bei PCs werden Mechanismen der Selbstbeschreibung in Bezug auf Funktionalität, Identifizierung, Selbstaufbau der Kommunikation und geregeltem Datenaustausch genutzt, um neue Komponenten, Maschinen oder Anlagen in ein Produktionssystem effizient und sicher einbringen zu können. Diese Mechanismen sollen von vornherein mit integrierter Sicherheitstechnologie arbeiten und zwar auf Basis von marktgängigen und frei verfügbaren Standards wie z. B. OPC UA und AutomationML.

Aus dem akademischen Bereich gibt es erste wissenschaftliche Untersuchungen zum Gesamtzustand der IT-Sicherheit in der industriellen Produktion, einzelne Schwachstellenanalysen für spezielle Protokolle und erste Ideen zur Einführung von Verbesserungen z. B. in Form von Angriffserkennungssystemen (Intrusion Detection System, IDS) in SCADA Netzen.

Sowohl im Inland als auch im Ausland konzentriert sich die Aktivität im akademischen Bereich in Richtung IT-Sicherheit in der Industrieproduktion vor allem auf die wissenschaftliche Begleitung von „Industrie 4.0“-Projekten.

3.1.5.1 Forschungsgebiete

Die Fraunhofer-Verbünde für IuK-Technologie und für Verteidigung und Sicherheit veröffentlichten im Januar 2014 eine Strategie- und Positionspapier „Cybersicherheit 2020“[66]. In diesem Memorandum werden 18 Forschungsfelder für die IT-Sicherheitsforschung identifiziert:

63 http://www.iot-a.eu/public
64 The Internet-of-Things Architecture, Concepts and Solutions for Privacy and Security in the Resolution Infrastructure, http://www.iot-a.eu/public/public-documents/d4.2/at_download/file
65 Verbundprojekt im Rahmen der Bekanntmachung „Intelligente Vernetzung in der Produktion – Ein Beitrag zum Zukunftsprojekt ‚Industrie 4.0‘„ http://www.secureplugandwork.de
66 http://www.iese.fraunhofer.de/content/dam/iese/de/dokumente/Fraunhofer-Strategie-und_Positionspapier_Cyber-Sicherheit2020.pdf

1. Cloud-Sicherheit
2. Cyber-Physical Systems
3. Datenschutz und Privacy Management
4. Energieerzeugung und Energieversorgung
5. Frühwarnsysteme
6. Industrielle Produktion und Automatisierung
7. IT-Forensik
8. IT-Sicherheit für Mobilität
9. Mediensicherheit
10. Netzsicherheit
11. Physically Embedded Cyber Security
12. Piraterieschutz
13. Secure Engineering
14. Secure Mobile Systems
15. Sicherheit gegen Seitenkanal- und Fehlerangriffe
16. Sicherheitsmanagement
17. Vertrauenswürdige Systeme
18. Zusammenspiel Safety und Security

Die jeweiligen Forschungsfragen zu den genannten Gebieten werden in dem Strategie- und Positionspapier im Einzelnen weiter detailliert. Die IT-Sicherheit bei I4.0 ist von fast allen diesen Forschungsgebieten berührt, besonders naturgemäß bei den Punkten „Cyber-Physical Systems“, „Industrielle Produktion und Automatisierung“, „Physically Embedded Cyber Security“, „Piraterieschutz“ sowie „Zusammenspiel Safety und Security“.

Die nachfolgende Tabelle 3–2 listet einzelne Fachgebiete der IT-Sicherheitsforschung und ihren Bezug zu I4.0 auf:

Wenige dieser Fachgebiete stehen isoliert für sich allein. Sie überschneiden sich zum Teil, bedingen oder beinhalten sich.

An den Universitäten und Hochschulen in Deutschland wird das Thema der IT-Sicherheit des sich entwickelnden „Internet of Things“ mit dem Schwerpunkt auf der industriellen Produktion in jüngster Zeit verstärkt wahrgenommen. Die wissenschaftliche Literatur dazu besteht bisher jedoch im Wesentlichen aus vereinzelten Konferenzbeiträgen, Fachzeitschriften-Artikeln und Whitepapers.

Tabelle 3–2: Fachgebiete der IT-Sicherheitsforschung und ihr Bezug zu I4.0

Fachgebiet	I4.0 Relevanz (z. T. Beispiele, unvollständig)
Architektur, Vernetzung, Design, Schutz- und Abwehrtechnologien	
Sicherheitsarchitekturen	Einbindung/Kapselung von Legacy-Komponenten
Netzwerksicherheit	Netzwerksegmentierung (IEC 62443), Herausforderungen bei ad-hoc Vernetzungen
Sichere Kommunikations-protokolle	OPC UA, Einbindung von proprietären sowie von Legacy-Protokollen ohne interne Security-Features, SSL/TLS, SSH, IPSec
Lightweight Cryptography	Berücksichtigung von zeitkritischen Anforderungen und von begrenzten Ressourcen (Prozessor-Kapazität, Energie)
AAA (Authentication, Authorization, Accounting)	unternehmensübergreifende AAA-Verfahren, Berücksichtigung von zeitkritischen Anforderungen
Identitäts-Management	sicherer Identitätsnachweis von Maschinen und Komponenten
Sicherheit von (Web-) Anwendungen	Designvorgaben in Industrieumgebungen, Verfahren zum Schließen von Sicherheitslücken
Sichere Firmware	bei Industrie-spezifischen Komponenten
Produktschutz, Enterprise Rights Management	genuin Industrie-relevant
Verfügbarkeit	Implikationen von Sicherheitsmaßnahmen angesichts unterschiedlicher Schutzzielpriorisierung im Vergleich zur Office-IT

→

Tabelle 3–2: Fachgebiete der IT-Sicherheitsforschung und ihr Bezug zu I4.0 (Fortsetzung)

Fachgebiet	I4.0 Relevanz (z. T. Beispiele, unvollständig)
Robustheit, Widerstandsfähigkeit (Resilience)	Redundanzschemata, Isolation/Bypass befallener Komponenten, Robustheit drahtloser Kommunikation in Industrieumgebungen
Erkennung von Sicherheitsvorfällen	
Intrusion Detection, Mustererkennung	Anpassung auf das spezifische industrielle Umfeld
Penetration Testing	Autorisierte Tests der Systeme auf bekannte Schwachstellen
Monitoring	
Organisatorische Prozesse, Verfahren, Nachsorge, Messbarkeit	
IT-Sicherheitsmanagement	Implementierbarkeit bei KMU, Internationalisierungs-Aspekte (organisatorisch, rechtlich)
Schadensbegrenzung nach Sicherheitsvorfällen	bei höchster Priorität der Aufrechterhaltung der Produktion
Forensik	bei Industrie-spezifischen Komponenten
Zurechenbarkeit	Unabstreitbarkeit/juristische Haftbarkeit; auch unter dem Gesichtspunkt autonomen Handelns von Maschinen
Analyse von Sicherheitsvorfällen	Aufbau einer umfassenden Datenbasis von industrierelevanten Vorkommnissen; Forensische Überprüfung der Vorfälle
Malware Analyse	bei Industrie-spezifischen Komponenten
Metriken	Wirtschaftlichkeit von IT-Sicherheitsmaßnahmen in industriellen Produktionsnetzen
Schwachstellenanalyse	Checklisten, Sicherheitstestverfahren für SCADA-/ICS-/CPS-Systeme, Schwachstellen in Wertschöpfungsketten
Interdependenzen	
Wechselwirkungen von IT-Sicherheit und funktionaler Sicherheit (Security/Safety)	bei I4.0 von besonderer Bedeutung, da in Produktionsumgebungen in keinem Fall die Arbeitssicherheit beeinträchtigt werden darf
Schwachstellen bei Feature Interaktionen	Entwicklung von spezifischen IT-Sicherheits-Testverfahren für Industriekomponenten und -systeme
Datenschutz	
Datenschutz	Technisch-organisatorische Maßnahmen und rechtliche Implikationen, die bei I4.0 aus dem vermehrten Weiterreichen von datenschutzrechtlich sensiblen Daten an unterschiedlichste Partner der Wertschöpfungskette und an Maschinen entstehen, Datenschutzaspekte bei grenzüberschreitendem Austausch von Daten

Es existieren an verschiedenen Universitäten und Hochschulen Lehrstühle in den Fachbereichen Informatik oder Recht, die auf die Themen IT-Sicherheit, Netzsicherheit, Datenschutz oder IT-Recht spezialisiert sind. Bisher hat sich aber noch keiner hauptsächlich auf die Thematik der IT-Sicherheit von Industrieanlagen und Wertschöpfungsketten in vernetzten industriellen Systemen fokussiert. Da das gesamte Thema der IT-Sicherheit an den Universitäten und Hochschulen meist von nur einem oder zwei Lehrstühlen abgedeckt werden muss, ist auch aktuell nicht zu erwarten, dass hier eine Spezialisierung auf IT-Sicherheit bei I4.0 erfolgen wird.

Zum einen existieren Lehrstühle und Institute, die dezidiert dem Thema IT-Sicherheit gewidmet sind, sich dabei besonders mit Basistechnologien beschäftigen, deren Bedeutung zunächst unabhängig von einem konkreten Anwendungsumfeld wie industriellen Produktionsnetzen zu sehen ist. Sie sind jedenfalls bisher selten schwerpunktmäßig auf die besonderen Erfordernisse der IT-Sicherheit in der Industrie fokussiert.

Zum anderen ist für Lehrstühle und Institute im Bereich von Elektrotechnik und Maschinenbau (Steuerungssysteme, Produktions- und Anlagentechnik etc.) die IT-Sicherheit zunehmend eine wichtige Querschnittskompetenz, die in deren Forschungsprojekten adressiert werden muss.

Daraus ergibt sich zwangsläufig, dass die IT-Sicherheitsforschung sehr stark auf interdisziplinäre Zusammenarbeit angewiesen ist, in der das Domänenwissen der Produktions- und Automatisierungstechnik mit dem Spezialwissen der IT-Sicherheitsspezialisten aus der Informatik, der entsprechenden Fachleute aus den Fachbereichen betriebswirtschaftlicher Organisation und nicht zuletzt der Rechtswissenschaft zusammengebracht wird.

Infolge dessen bilden sich an verschiedenen Orten Cluster heraus, in denen vielfältige Kompetenzen aus Informatik, Elektrotechnik, Maschinenbau, Betriebswirtschaft und Rechtswissenschaft gebündelt werden.

3.1.5.2 Forschungszentren in Deutschland

Kompetenzzentren für IT-Sicherheit: EC-SPRIDE, KASTEL, CISPA

Seit 2011 fördert das BMBF drei Kompetenzzentren für IT-Sicherheit in Darmstadt (EC-SPRIDE), Karlsruhe (KASTEL), und Saarbrücken (CISPA) an denen sowohl Hochschulen als auch außeruniversitäre Forschungseinrichtungen beteiligt sind. Ihre Aufgabe besteht in der Entwicklung langfristiger Strategien zur Cyber-Security im Allgemeinen. Der Zeithorizont der dort betriebenen Forschung ist somit nicht darauf angelegt, zu einer unmittelbaren und praktischen Umsetzung von Verbesserungen der heutigen IT Sicherheitssituation bei industriellen Automatisierungs- und Steuerungsanlagen beizutragen.

Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI)

Die Forschungsprojekte des Deutschen Forschungszentrums für Künstliche Intelligenz GmbH (DFKI) berühren in großer Zahl I4.0-Themen (insbesondere die Bereiche Innovative Fabriksysteme, Cyber-Physical Systems, Planbasierte Robotersteuerung, Robotics Innovation Center, Intelligente Analytik für Massendaten). Zur IT-Sicherheit forscht dort der Bereich „Sichere Systeme“ an Methoden zur Verifikation und Evaluation von Sicherheitseigenschaften.

Fraunhofer Gesellschaft

In den Instituten der Fraunhofer-Gesellschaft werden Projekte der angewandten Forschung in enger Kooperation mit Industrieunternehmen betrieben.

Fraunhofer AISEC und Fraunhofer SIT haben als Institute, die explizit auf die IT Sicherheitsforschung ausgerichtet sind, jeweils Arbeitsgruppen eingerichtet, die sich speziell mit der IT-Sicherheit in der Industrie befassen. Andere Institute, wie Fraunhofer ESK, Fraunhofer IOSB, Fraunhofer IPA oder Fraunhofer IML, die einen Schwerpunkt auf der Anwenderseite von I4.0 haben (Industriekommunikation, Industrieautomatisierung, Produktionsleittechnik, Fertigungsplanung, Logistik) haben in ihren Projekten den Aspekt der IT-Sicherheit natürlicherweise ebenfalls als Thema.

Horst Görtz Institut für IT-Sicherheit (HGI)

Das HGI ist mit 10 Professuren im Bereich IT-Sicherheit (Kryptographie, Technik, Wirtschaft, Recht) eines der größten akademischen Institute auf diesem Gebiet weltweit. Die Forscher des HGI sind international gut vernetzt, sowohl im Bereich Kryptographie als auch im Bereich angewandte IT-Sicherheit. Für den Bereich I4.0 besonders relevant sind die Forschungen zur eingebetteten Sicherheit. Das HGI betreibt mehrere Studiengänge im Bereich IT-Sicherheit.

FORSEC

Der bayerische Forschungsverband FORSEC umfasst alle bayerischen Hochschulen, die sich mit IT-Sicherheit befassen, und besitzt einen Forschungsschwerpunkt zum Thema IoT. Eines der Teilprojekte (TP2)[67] befasst sich dabei mit dem Thema „Internet of Things Security“.

3.1.5.3 Außerhalb Deutschlands

Auch im Ausland befasst man sich zwar schon seit Mitte der 2000er Jahre tiefer mit dem Problem der vernachlässigten IT Sicherheit im IACS-Bereich. Auf einschlägigen Kongressen kommen Beiträge zu diesem Thema aus unterschiedlichsten Ländern und Forschungsinstitutionen, z. B. auch von britischen, spanischen oder italienischen Universitäten. Papiere, die sich speziell mit der IT-Sicherheit in der industriellen Produktion befassen, kommen jedoch meist von den Praktikern, d. h. von Industriefirmen.

Hervorstechende „Zentren“ für die Thematik IT-Sicherheit bei I4.0 im engeren Sinne haben sich jedoch noch nicht herausgebildet. Einrichtungen wie z. B. das Center for Control System Security am Sandia National Laboratory oder das Critical Infrastructure Protection Program am Idaho

67 FORSEC Teilprojekte Internet of Things (IoT) Security, https://www.bayforsec.de/de/teilprojekte/teilprojektseiten/internet-of-things-iot-security/, zuletzt abgerufen am 14.07.2015.

National Laboratory in den USA[68] sind auf die Sicherheit kritischer Infrastrukturen ausgerichtet (insbesondere die Energieversorgung betreffend) und nicht auf die spezifischen Aspekte von I4.0. Von den in solchen Einrichtungen erarbeiteten Forschungsergebnissen kann selbstverständlich viel auf den Bereich der Industrieproduktion übertragen werden.

3.1.6 IEEE Smart Cities Initiative

Das Institute of Electrical and Electronics Engineers (IEEE) koordiniert die Initiative IEEE Smart Cities, die sich zum Ziel gesetzt hat in mehreren Städten die „Stadt der Zukunft" modellhaft zu realisieren. Hierfür wurden bis jetzt 3 Städte ausgewählt: Guadalajara in Mexiko, Trient in Italien und Wuxi in China. Beteiligt sind sowohl die staatliche Verwaltung, Hochschulen und Forschungsinstitute als auch Industriefirmen. Die Initiative befindet sich derzeit noch in einem frühen Konzeptstadium und klammert die Thematik von Industrieproduktion und Wertschöpfungsketten noch aus. Diese Aktivitäten werden daher im Rahmen dieser Studie nicht weiter betrachtet.

3.1.7 Die Lage der deutschen IT-Sicherheitsindustrie

Eine Übersicht über die deutsche Sicherheitsindustrie[69], die 2014 aktualisiert vom Bundesministerium für Wirtschaft und Energie (BMWi) veröffentlicht wurde, beziffert den Produktionswert der deutschen Sicherheitswirtschaft im Jahr 2013 auf über zehn Milliarden Euro, von denen vier Prozent auf Hardware, 44 Prozent auf Software und 52 Prozent auf Dienstleistungen entfielen. Der Anteil der Hardware ist dabei von 13 Prozent im Jahre 2005 über die letzten Jahre kontinuierlich gesunken. Die durchschnittlichen Zuwachsraten bei Umsatz und Bruttowertschöpfung insgesamt betrugen über die letzten zehn Jahre über sieben Prozent. Die Zahl der Erwerbstätigen als Selbständige und bei den ca. 7.500 Unternehmen der Branche betrug im selben Jahr über 65.000 (bei denen es sich allerdings nur zum Teil um eigentliche IT Sicherheitsexperten handelt), davon ca. 57.000 als sozialversicherungspflichtig Beschäftigte. Diese Studie schlüsselt allerdings nicht nach Unternehmensgrößen oder Schwerpunktgebieten auf.

An der gesamten IKT-Industrie haben Unternehmen, die sich auf dem Feld der IT-Sicherheit betätigen, mit ca. zehn Prozent einen signifikanten Anteil. Der Exportanteil liegt über dem Durchschnitt der übrigen IKT-Industrie, wenn auch deutlich unter dem Exportanteil von Branchen wie Maschinen- und Anlagenbau, der Automobil- oder Chemieindustrie.

Insgesamt bestand zuletzt immer noch ein Außenhandelsdefizit bei IT Sicherheitsprodukten und Dienstleistungen, das jedoch ausschließlich auf den Hardware-Sektor zurückzuführen ist.

Keine großen deutschen Unternehmen als Weltmarktführer

Bei der globalen Betrachtung der IT-Sicherheitsindustrie stellt man fest, dass die Branche von nichtdeutschen und nichteuropäischen Firmen dominiert wird.

Im Bereich der Internettechnik, die naturgemäß auch immer auch einen hohen Anteil IT-Security beinhaltet, werden die Maßstäbe von amerikanischen (Cisco, Juniper) und chinesischen (Huawei, ZTE) Firmen gesetzt. Die übriggebliebenen europäischen Telekommunikationshersteller wie Ericsson oder Nokia Networks konzentrieren sich vornehmlich auf den Bereich des Mobilfunks.

Unter den großen Anbietern dezidierter IT-Sicherheitstechnik wie Verschlüsselungstechnik, Zertifikats-Management / Trust Center, Firewalls, Malware-Abwehr etc. sind ebenfalls kaum deutsche Schwergewichte in Form von Weltmarktführern zu finden. Lediglich im Bereich der Sicherheits-Mikrocontroller beansprucht die Firma Infineon eine Weltmarktführerrolle.

Diese Entwicklung hat nicht nur, aber sicher auch damit zu tun, dass in Deutschland die Nachfrage nach solchen Technologien aus den Militär- und Geheimdienstbudgets, wo auf nationale Hersteller naturgemäß ein besonderer Wert gelegt wird, um Größenordnungen niedriger ist, als insbesondere in den USA.[70]

68 Eine kompakte Übersicht über die US-Programme bietet der Artikel „Cyberphysical Security for Industrial Control Systems Based on Wireless Sensor Networks „(Tianbo Lu et al., International Journal of Distributed Sensor Networks 2014), http://downloads.hindawi.com/journals/ijdsn/2014/438350.pdf

69 IT-Sicherheitsmarkt in Deutschland, http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/it-sicherheitsmarkt-in-deutschland-studie-2014, zuletzt abgerufen am 06.05.2015

70 Laut einem Report von Cybersecurity Ventures (http://cybersecurityventures.com/cybersecurity-market-report/), betrug das Volumen der Ausgaben der US-Regierung für IT-Sicherheitsprodukte und IT-Sicherheitsdienstleistungen im Jahr 2014 7,8 Milliarden US-Dollar.

Gleichwohl hat sich in Deutschland eine zum Teil hochinnovative Szene von IT-Sicherheitsfirmen herausgebildet, die in ihren jeweiligen Spezialbereichen auch international einen guten Ruf genießen. Diese Firmen sind jedoch meist klassische KMUs vom Startup mit einstelligen Mitarbeiterzahlen bis zu gut etablierten Mittelständlern mit bis zu 300 Mitarbeitern und einem Umsatz in der Größenordnung von 50 Millionen Euro. IT-Sicherheitsfirmen sind auch als teils 100-prozentige Tochterunternehmen von Großunternehmen wie Bosch (z. B. die escrypt) oder von großen Mittelständlern wie Giesecke & Devrient (z. B. die Secunet (79 Prozent) oder Rohde & Schwarz (z. B. die Sirrix und gateprotect) zu finden.

IT-Sicherheits-Anbieter im Umfeld I4.0

Im Anbieterverzeichnis des Branchenverbands der deutschen IT-Sicherheitsindustrie (TeleTrusT) haben sich etwa 25 Firmen unterschiedlicher Größe unter den Stichworten „Industrial Security (Industrie 4.0)“ bzw. „Produktionsanlagen/Leittechnik/SCADA (IT-Sicherheitslösungen)“ eingetragen.

Neben diesen spezialisierten IT-Sicherheitsfirmen sind im Umfeld I4.0 auch Anwender und Anlagenhersteller (Siemens, Bosch, ZF u. a.) auf dem Gebiet der IT-Sicherheit tätig. Diese Tätigkeit erfolgt jedoch in der Regel für interne Zwecke bzw. in Form von proprietären Lösungen für die eigenen Produkte bei den Kunden. Ähnliches gilt für die Hersteller von Automatisierungstechnik wie Phoenix Contact, Festo oder Beckhoff Automation.

Der Aufwand, der bei allen diesen Teilnehmern für Forschung und Entwicklung von IT-Sicherheit in industriellen Produktionsnetzen betrieben wird, lässt sich nicht beziffern, da KMUs ihren F&E-Aufwand größtenteils nicht veröffentlichen und von größeren Firmen das F&E-Budget nicht auf die Entwicklung von IT-Sicherheitstechnik und -lösungen heruntergebrochen wird.

3.2 Wesentliche IT-Sicherheitsnormen, Standards und Richtlinien

Eine umfängliche Nennung aller im Kontext relevanten IT-Sicherheitsnormen, Standards und Richtlinien würde den Rahmen dieser Studie sprengen. Zahlreiche nationale und internationale Standardisierungseinrichtungen und Verbände haben in den letzten Jahrzehnten Arbeitsgruppen dazu eingerichtet und Ergebnisse veröffentlicht, die als konsensbasierte de facto und/oder de jure Standards anerkannt sind.

Gemäß ihrer Domänenzugehörigkeit und gebietlicher Zuständigkeit sind hier im Wesentlichen folgende Organisationen zu nennen:

Tabelle 3–3: Wichtige Organisationen und deren wesentliche IT-Sicherheitsnormen, Standards und Richtlinien

Name	Langname	Gebiet	Domäne	Beitrag IT-Sicherheit
BSI	Bundesamt für Sicherheit in der Informationstechnik	Deutschland	IT-Sicherheit	*ICS (Industrial Control Systems) Security Kompendium* Diverse Technische Richtlinien, u. a. zu kryptographischen Verfahren, für sicheres WLAN, technische Vorgaben für SmartMeter-Komponenten, den Beweiswerterhalt kryptographisch signierter Daten und den sicheren Betrieb von Zertifizierungsinstanzen.
CEN	Europäisches Komitee für Normung (franz. Comité Européen de Normalisation)	Europa	alle Domänen mit Ausnahme der Elektrotechnik (→ CENELEC) und Telekommunikation (→ ETSI)	
CENELEC	Europäisches Komitee für elektrotechnische Normung	Europa	Elektrotechnik	
DIN	Deutsches Institut für Normung	Deutschland	alle Domänen	
ETSI	Europäisches Institut für Telekommunikationsnormen	Europa	Telekommunikation	
IEC	International Electrotechnical Commission	global	Elektrotechnik	IEC 62446 (industrielle Leitsysteme – Netz- und Systemschutz) vgl. ISO

→

Tabelle 3–3: Wichtige Organisationen und deren wesentliche IT-Sicherheitsnormen, Standards und Richtlinien

Name	Langname	Gebiet	Domäne	Beitrag IT-Sicherheit
IETF	Internet Engineering Task Force	global	Internet	– Glossar – Verschlüsselung (SSL/TLS) – IPSec – Privatheit – Public Key Infrastructure (PKI) (→ Internet-Profil von ITU X.509)
ISA	International Society of Automation	USA	Automatisierungstechnik	– ISO/IEC 62443 (ISA99) – Allgemeines – Policies – Komponenten- und Systemebene
ISO	Internationale Organisation für Normung (englisch: International Organization for Standardization)	global	alle Domänen mit Ausnahme der Elektrotechnik (→ IEC) und Telekommunikation (→ ITU)	– Anforderungen, Leitfaden, Governance, Rahmenwerke und Management (ISO/IEC 270xy) – Privatheit – Identitätsmanagement – Authentifizierung – Evaluierung – Verschlüsselung – Schlüsselmanagement – Nicht-Abstreitbarkeit – Monitoring – Erkennen von Eindringlingen – Hilfsfunktionen (hash, Zufallszahlen ...)
ITU	International Telecommunications Unit	global	Telekommunikation	– X.509 Public Key Certificate Infrastructure
NAMUR	Interessengemeinschaft Automatisierungstechnik der Prozessindustrie	international	Chemie- und Pharmaindustrie	– Randbedingungen – Schutzziele
NIST	National Institute of Standards and Technology	USA	alle Domänen	– Übersichten – Verschlüsselung (DES – Data Encryption Standard und Nachfolger AES – Advanced Encryption Standard) – Schlüsselmanagement
OASIS	Organization for the Advancement of Structured Information Standards	global	Informationstechnologie	– Web Services (WS-*, insb. WS-Security) – Security Assertion Markup Language (SAML) – eXtensible Access Control Markup Language (XACML)
VDI/VDE GMA	Verein Deutscher Ingenieure/ Verein Deutscher Elektrotechniker	Deutschland	Mess- und Automatisierungstechnik	– allgemeines Vorgehensmodell für industrielle Anwendungen (VDI/VDE 8182)
W3C	World Wide Web Consortium	global	World Wide Web	– Verschlüsselung (XML) Signaturen (XML)

Eine erste Analyse zeigt, dass die Standards und Richtlinien im Wesentlichen in sich branchenspezifisch aufgestellt und wenig untereinander vernetzt sind. Die ISO/IEC Standards betrachten vornehmlich die organisatorischen Aspekte der IT-Sicherheit. Die technischen Empfehlungen aus dem Internet und World Wide Web werden von den branchenspezifischen Standards noch kaum verwendet und referenziert, was im Zuge der Anwendung des Internet der Dinge und Dienste auf die industrielle Produktion eine Lücke darstellt.

Eine detailliertere Bewertung der Standards und Normen für I4.0 folgt in Kapitel 6.4.

3.3 Rechtliche Stellungnahmen und neue rechtliche Anforderungen

Als Ausgangspunkt für die Entwicklung von Handlungsempfehlungen zur Minimierung der mit I4.0 verbundenen rechtlichen Risiken und insbesondere der im Rahmen

dieser Studie zu entwickelnden technischen Referenzmodelle, haben wir zunächst bereits vorhandene Stellungnahmen zu I4.0 und verwandten Themen im Hinblick auf wesentliche rechtliche Fragestellungen ausgewertet. Dabei haben wir insbesondere die Feststellungen in dem von dem BMWi zur Autonomik publizierten Band 2 „Recht und funktionale Sicherheit in der Autonomik“[71] sowie den Abschlussbericht des Arbeitskreises zur Industrie 4.0[72], „Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0“ von April 2013 als Ausgangspunkt herangezogen.

Überdies haben wir weitere gängige rechtliche Kommentierungen sowie sonstige (rechtliche) Literatur im Hinblick auf rechtliche Implikationen von I4.0 ausgewertet. Zugrunde gelegt haben wir dabei, dass die wesentliche Neuerung von I4.0 gegenüber herkömmlicher Industrie darin besteht, dass Produktionsmaschinen so miteinander vernetzt werden, dass sie mit den Werkstücken sowie mit anderen Maschinen und Unternehmensteilen kommunizieren können und dies bis hin zur Unternehmensplanung und dem Controlling.[73] Diese Kommunikation beinhaltet insbesondere auch den Austausch sensibler (personenbezogener) Daten über Unternehmens- und Ländergrenzen hinaus.

Einen kurzen Überblick über die so eruierten rechtlichen Themenfelder, im Hinblick auf I4.0 und insbesondere die noch zu spezifizierenden Fallbeispiele, sowie die zentralen damit einhergehenden Fragestellungen für die Schaffung eines wirksamen Rechtsrahmens haben wir nachfolgend dargestellt:

3.3.1 Vertragsrechtliche Aspekte

Die Zusammenarbeit in der I4.0 wird regelmäßig durch Verträge zwischen den Beteiligten geregelt. Es wird untersucht, welchem Recht diese Verträge unterliegen und welche spezifischen vertragsrechtlichen Herausforderungen sich nach deutschem Recht ergeben. Die Erörterung erfolgt auf der Grundlage deutschen Rechts. Anwendbare internationale Abkommen werden berücksichtigt.

3.3.1.1 Typ der vertraglichen Zusammenarbeit

Die Zusammenarbeit in der I4.0 kann sehr unterschiedlich vertraglich gestaltet werden. Ein vorherrschender Gestaltungstyp hat sich bisher nicht herausgebildet. Die Studie von Forschungsunion/acatech fordert die Entwicklung neuer Vertragsmodelle, um die Kooperation effizient vertraglich zu regeln.[74] Diese liegen bisher jedoch nicht vor.

Für die weitere Erörterung in dieser Studie wird die Annahme zugrunde gelegt, dass die Zusammenarbeit häufig in Form eines Kooperationsvertrags erfolgt, in dem sich die Beteiligten verpflichten, über die im Vertrag festgelegten elektronischen Kanäle zusammenzuwirken, etwa um Entwicklung oder Herstellung von Produkten zu koordinieren. Ein solcher Vertrag kann auch als Rahmen- oder Nebenvereinbarung zu anderen Verträgen geschlossen werden. Denkbar ist auch, dass die Einbeziehung von Partnern, etwa Lieferanten, oder Abnehmern von Produkten, über Kaufverträge erfolgt, die dann die Einbeziehung in die Kooperation regeln oder auf einen bestehenden Kooperationsvertrag oder vom Vertragspartner gesetzte Bedingungen verweisen.

3.3.1.2 Das auf den Kooperationsvertrag anwendbare Vertragsrecht (Rom I–VO)

Wenn bei der Zusammenarbeit in der I4.0 so genannte Auslandselemente vorliegen, insbesondere Partner mit Sitz oder beteiligter Niederlassung in verschiedenen Staaten beteiligt sind oder Teile der Tätigkeit in anderen Staaten erfolgen, muss das auf den Kooperationsvertrag anwendbare Recht ermittelt werden. Maßgebliche Rechtsgrundlage ist insoweit die so genannte Rom I-Verordnung (Rom I–VO)[75], die in allen EU-Mitgliedstaaten gilt. Die Rom I–VO ist nach ihrem Art. 1 Abs. 1 auf alle zivilrechtlichen Schuldverhältnisse und damit auch auf Kooperationsverträge in der I4.0 anwendbar. Eine Ausnahme gilt nach Art. 1 Abs. 2 lit. f) Rom I–VO für gesellschaftsrechtliche Fragen. Dies kann Relevanz haben, wenn die Kooperation in Form einer eigenen Gesellschaft geführt wird. Eine Gesellschaft in Form einer BGB-Gesellschaft kann auch dann angenommen werden, wenn keine juristische Person entstehen soll und

71 BMWi, AUTONOMIK, Band 2, Recht und funktionale Sicherheit in der Autonomik, Leitfaden für Hersteller und Anwender, Stand Januar 2013.
72 Forschungsunion/Acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, April 2013.
73 Geis, ZD 2013, 591 (591).
74 Forschungsunion/acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, April 2013, Ziff. 5.7.1 (S. 63).
75 Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates vom 17. Juni 2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I–VO).

kein Vermögen der Gesellschaft gebildet werden soll. Im Folgenden geht die Studie von einem schuldrechtlichen Kooperationsvertrag aus.

Die Rom I–VO bietet in ihrem Art. 3 Abs. 1 Rom I– VO die Möglichkeit der freien Rechtswahl des Vertrags, von der die Parteien bei Kooperationsverträgen in der I4.0 in aller Regel Gebrauch machen werden. Die Rechtswahl ist auch schon aus Gründen der Rechtsklarheit zu empfehlen. Die Parteien können dabei ein beliebiges Recht wählen, also etwa auch ein Recht eines Staates, mit dem der Vertrag keine Berührung hat („neutrales Recht"). Der Vertrag unterliegt dann dem gewählten Recht.

Der Grundsatz der freien Rechtswahl gilt jedoch nicht uneingeschränkt. Nach Art. 3 Abs. 3 Rom I–VO kann bei reinen Binnensachverhalten nicht vom zwingenden inländischen Recht abgewichen werden.[76] Gleiches gilt nach Art. 3 Abs. 4 Rom I–VO für die Anwendung des Gemeinschaftsrechts, sofern alle anderen Sachverhaltselemente in einem oder mehreren Mitgliedsstaaten belegen sind und ein Drittstaat gewählt wurde. Eine weitere Einschränkung der freien Rechtswahl findet sich in Art. 9 Abs. 2 Rom I–VO, nach dem die Anwendbarkeit sog. Eingriffsnormen des Rechts des anzurufenden Gerichts nicht abbedungen werden kann.[77] Ebenso können nach Art. 9 Abs. 3 Rom I–VO Eingriffsnormen des Erfüllungsortes zur Anwendung gelangen. Derartige Eingriffsnormen enthalten in Deutschland z. B. Teile des Urheberrechts sowie das Datenschutzrecht.[78]

Haben die Beteiligten keine Rechtswahl getroffen, kommt es zu einer objektiven Anknüpfung nach Art. 4 Rom I–VO. Art. 4 Abs. 1 Rom I–VO bestimmt das anwendbare Recht, sollte der Vertrag einem der dort bezeichneten Verträge zuzuordnen sein. Ist eine eindeutige Zuordnung nicht möglich, so ist nach Art. 4 Abs. 2 Rom I–VO das Recht desjenigen Staates anwendbar, in dem die Partei, die die charakteristische Leistung erbringt, ihren gewöhnlichen Aufenthalt hat.

Beide Kriterien bereiten bei Verträgen über Kooperation in der I4.0 Schwierigkeiten. Der Kooperationsvertrag (dazu oben 1.2.1.1) lässt sich in die in Art. 4 Abs. 1 Rom I–VO genannten Vertragstypen nicht einordnen. Nach Art. 2 Abs. 2 Rom I–VO kommt es darauf an, welche Partei die charakteristische Leistung erbringt. Bei einem Kooperationsvertrag im engeren Sinne, bei dem alle Beteiligten jeweils nicht nur ein Entgelt bezahlen, sondern ihrerseits Sachleistungen erbringen, wird sich eine charakteristische Leistung, die nur einer Partei zuzuordnen ist, regelmäßig nicht ermitteln lassen, so dass Art. 4 Abs. 2 Rom I–VO nicht anwendbar ist. Sofern aufgrund der Gestaltung des Vertrags die charakteristische Leistung ausnahmsweise einer einzelnen Partei zugeordnet werden kann, gilt gemäß Art. 4 Abs. 2 Rom I–VO das Recht des Staates, in dem diese Partei ihren gewöhnlichen Aufenthalt hat (sofern nicht gleichwohl eine offensichtlich engere Verbindung zu einem anderen Staat besteht, Art. 4 Abs. 3 Rom I–VO).

Im Regelfall wird das anwendbare Recht bei fehlender Rechtswahl gemäß Art. 4 Abs. 4 Rom I–VO zu bestimmen sein. Maßgeblich ist dann das Recht des Staates, mit dem die engste Verbindung besteht.

Als Ergebnis zum anwendbaren Recht bei Kooperationsverträgen in der I4.0 lässt sich damit festhalten, dass die Rom I–VO mit der Möglichkeit der Rechtswahl ein geeignetes Instrument bietet, um ein angemessenes Ergebnis zu erzielen.

3.3.1.3 Vertragsrechtliche Regelungen

Die vertragliche Gestaltung der Kooperation unterliegt den allgemeinen Regeln des Vertragsrechts im Bürgerlichen Gesetzbuch (BGB). Spezifische gesetzliche Regeln für eine derartige Kooperation enthält das BGB nicht. Die Parteien können die Zusammenarbeit weitgehend frei regeln. Soweit die Bedingungen des Kooperationsvertrags von einem Beteiligten gestellt und nicht ausgehandelt sind, handelt es sich allerdings um Allgemeine Geschäftsbedingungen (AGB), die auch bei Verträgen zwischen Unternehmern der AGB-Kontrolle des BGB, nicht zuletzt der Inhaltskontrolle nach § 307 BGB unterliegen. Die Voraussetzungen des Aushandelns sind de lege ferenda Gegenstand intensiver Diskussion. Nach geltendem Recht nimmt die Rechtsprechung ein Aushandeln nur an, wenn die Klausel vom Verwender ernsthaft zur Disposition gestellt wird. Dies wird nicht immer der Fall sein. Insgesamt besteht bei mehrseitigen Kooperationsverträgen erhebliche Rechtsunsicherheit über die Anwendbarkeit und Auswirkungen der AGB-Kontrolle.

Die Kooperation in der I4.0 wirft aufgrund der Beteiligung mehrerer Partner etliche Fragen auf, die bisher nicht gelöst sind. Die Studie von Forschungsunion und Acatech fordert

76 MüKo/Martiny, Rom I-VO, Art. 3 Rn. 87.
77 Becks'sches Mandatshandbuch IT-Recht/Auer/Reinsdorff, § 32 Rn. 82.
78 Becks'sches Mandatshandbuch IT-Recht/Auer/Reinsdorff, § 32 Rn. 82.

daher die Entwicklung praxisorientierter Leitfäden, Checklisten sowie Mustervertragsklauseln.[79] Daneben besteht Forschungsbedarf zu den rechtlichen Grundlagen, deren Klärung für die Formulierung von Musterverträgen erforderlich ist.

Die allgemeinen vertragsrechtlichen Aspekte sind teilweise auch für die IT-Sicherheit in der I4.0 von Bedeutung und werden insoweit im Rahmen dieser Studie näher untersucht (dazu unten).

3.3.2 Aspekte des Haftungsrechts

Bei der netzgestützten internationalen Zusammenarbeit kann es zu Störungen kommen. Als spezifischer Aspekt der I4.0 werden Störungen in Bezug auf Daten, insb. Verlust oder Veränderung von Daten untersucht. Insoweit werden das anwendbare Recht und die Haftung nach deutschem Recht untersucht.

3.3.2.1 Anwendbares Haftungsrecht

Für die rechtlichen Folgen in Schadensfällen ist das Haftungsrecht (Deliktsrecht) maßgeblich. Bei der internationalen Zusammenarbeit im Rahmen von I4.0 ist, genauso wie beim Vertragsrecht, das maßgebliche nationale Recht zu ermitteln. Insoweit ist nach den Rechtsgrundlagen der Haftung zu unterscheiden.

Im Rahmen der vertraglichen Haftung (s. u. 1.2.1.2.1) ist Rechtsgrundlage die Rom I–VO. Das auf den Vertrag anwendbare Recht gilt gemäß Art. 12 Abs. 1 lit. c) Rom I–VO auch für die vertragliche Haftung der Beteiligten. Insoweit kann auf die Ausführungen unter 1.2.1.2 verwiesen werden.

Daneben kann eine Haftung aus Deliktsrecht (Recht der unerlaubten Handlung) in Betracht kommen. Insoweit ist das anwendbare Deliktsrecht nach den Regeln der so genannten Rom II-Verordnung (Rom II–VO)[80] zu bestimmen, die in allen EU-Mitgliedstaaten gilt. Die Rom II–VO ist nach ihrem Art. 1 Abs. 1 auf alle außervertraglichen zivilrechtlichen Schuldverhältnisse anwendbar. Soweit also im Rahmen der Kooperation Rechtsgüter verletzt werden, die der außervertraglichen Haftung (etwa nach den §§ 823 ff. BGB, dazu unten 1.2.2.2.) unterliegen, ist die Rom II–VO maßgeblich.

Wie im Vertragsrecht ist auch für das Deliktsrecht eine Rechtswahl denkbar. Neben der nachträglichen Rechtswahl nach Art. 14 Abs. 1 lit. a Rom II–VO ist gemäß Art. 14 Abs. 1 lit. b Rom II–VO im Verhältnis von Unternehmern untereinander eine vorherige Rechtswahl möglich. Art. 14 Abs. 2 und Abs. 3 Rom II–VO enthalten Einschränkungen der freien Rechtswahl, die weitgehend Art. 3 Abs. 3 Rom I–VO,[81] bzw. Art. 3 Abs. 4 Rom I–VO nachgebildet sind (siehe dazu oben 1.2.1.2.).[82] Diese Rechtswahl ist für Kooperationsverhältnisse sehr interessant, da sie für Haftungsfälle zwischen Kooperationspartnern Rechtssicherheit in Bezug auf das maßgebliche Haftungsrecht erzeugen kann.

Wurde keine Rechtswahl getroffen, richtet sich das anwendbare Recht nach den Art. 4 ff. Rom II–VO. Gemäß Art. 4 Abs. 1 Rom II–VO ist auf ein außervertragliches Schuldverhältnis aus unerlaubter Handlung das Recht des Staates anzuwenden, in dem der Schaden eingetreten ist. Soweit die Rechtsgutverletzung in der Zerstörung oder Manipulation von Datenbeständen besteht, was einen hohen Risikofaktor im Bereich I4.0 darstellt, kommt es somit nach traditioneller Ansicht auf den Lageort des Zielrechners[83] bzw. der datenverarbeitenden Anlage an. Ähnlich wie im Cloud Computing kann sich jedoch das Problem stellen, dass die Daten auf verschiedensten Servern bzw. Anlagen gespeichert sind. Insoweit ist das anwendbare Recht gegebenenfalls nach Art. 4 Abs. 2 oder Abs. 3 Rom II–VO[84] zu bestimmen. Diese sehen Ausnahmen von der Anknüpfung an den Ort des Schadenseintritts vor.

Wenn Schädiger und Geschädigter zum Zeitpunkt des Schadenseintritts ihren Aufenthaltsort in demselben Staat haben, so ist gem. Art. 4 Abs. 2 Rom II–VO das Recht dieses Staates anwendbar. Art. 4 Abs. 3 S. 1 Rom II–VO sieht vor, dass bei einer offensichtlich engeren Verbindung zu einem anderen Staat das Recht dieses Staates anwendbar ist. Eine solche Verbindung kann sich nach Art. 4 Abs. 3 S. 2 Rom II–VO

79 Forschungsunion/Acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0 April 2013, Ziff. 5.7. – Handlungsempfehlungen (S. 65).
80 Verordnung (EG) Nr. 864/2007 des Europäischen Parlaments und des Rates vom 11. Juli 2007 über das auf außervertragliche Schuldverhältnisse anzuwendende Recht (Rom II–VO).
81 MüKo/Junker, BGB, Art. 14 Rom II–VO, Rn. 39.
82 Spindler/Schuster/Pfeiffer/Weller/Nordmeier, Recht der elektronischen Medien, Art. 4 Rom II–VO, Rn. 6.
83 Nordmeier, MMR 2010, 151, 153.
84 So für das Cloud Computing: Nordmeier, MMR 2010, 151, 155.

insbesondere aus einem zwischen den Parteien bestehenden Vertrag ergeben, welcher mit der unerlaubten Handlung in enger Verbindung steht. Dies wird bei Kooperationsverträgen für die Haftung zwischen den Partnern häufig der Fall sein, so dass auch dann, wenn eine Rechtswahl fehlt, für die deliktische Haftung meist das Recht anwendbar sein wird, dem der Kooperationsvertrag unterliegt.

3.3.2.2 Relevante Haftungsfragen und Rechtsgrundlagen

Im Bereich von I4.0 stellen sich verschiedenste Haftungsfragen. Dabei ist aus rechtlicher Sicht etwa zwischen Haftungsfällen zwischen den Kooperationspartnern und Haftungsfällen im Verhältnis zu Dritten zu unterscheiden. Weiterhin ist nach der Art von Haftungsereignissen und Schäden zu differenzieren. Neben einer zivilrechtlichen Haftung sind Sanktionen nach Straf- oder Ordnungswidrigkeitenrecht von Bedeutung. Die für die Studie relevanten Haftungsszenarien werden in späteren Abschnitten (unten) dargestellt.

Voraussetzungen einer Haftung auf Schadensersatz
Eine zentrale Frage ist, unter welchen Voraussetzungen ein Kooperationspartner bei einer Störung zum Schadensersatz verpflichtet ist, insbesondere, ob ein Verschulden erforderlich ist. Weiter ist von Bedeutung, welche Sorgfaltspflichten bestehen, deren Verletzung ein Verschulden auslöst. Rechtsgrundlage sind insoweit die allgemeinen Regeln der vertraglichen (§§ 280 ff. BGB) oder deliktischen Haftung (§§ 823 ff. BGB), ggf. auch Sonderregeln, etwa nach Produkthaftungsgesetz (ProdHaftG).

Umfang der ersatzfähigen Schäden
Bei Störungen in vernetzter Entwicklung oder Produktion können sich bei den Kooperationspartnern sehr unterschiedliche Schäden einstellen, etwa Schäden von Anlagen oder anderen Sachgütern (Waren, Material) oder von Personen. Sehr wichtig sind Schäden durch Verzögerung im Kooperationsgegenstand, etwa einer Entwicklungsarbeit, oder der Produktion. Es ist daher von Bedeutung, welche Schäden ersatzfähig sind und damit Gegenstand eines Schadensersatzanspruchs sein können. Maßgeblich sind im deutschen Recht insoweit die allgemeinen Regeln des Deliktsrechts (§§ 823 ff. BGB, §§ 249 ff. BGB) sowie ggf. Sonderregeln, etwa nach ProdHaftG.

Möglichkeiten der Haftungsbeschränkung
In Kooperationsverhältnissen ist von Bedeutung, ob die Haftung der Beteiligten begrenzt werden kann. Da denkbare Schäden schwer eingrenzbar sind, drohen ohne Haftungsbeschränkung erhebliche Haftungsrisiken, die einer Kooperation entgegenstehen können.

Eine Haftungsbegrenzung kann gesetzlich geregelt sein oder vertraglich vereinbart werden. Eine allgemeine gesetzliche Haftungsbegrenzung für Kooperationsverhältnisse besteht nicht.

Im Innenverhältniszwischen den Kooperationsbeteiligten wird häufig eine Haftungsbegrenzung vereinbart. Diese unterliegt nach deutschem Recht dem Vertragsrecht des BGB. Grenzen ergeben sich insbesondere aus dem Recht der allgemeinen Geschäftsbedingungen, §§ 305ff. BGB sowie aus vertragsrechtlichen Grundsätzen (§§ 1248, 138, 276 Abs. 3 BGB).

Eine Haftungsbeschränkung gegenüber Dritten kann vertraglich nicht innerhalb des Kooperationsverhältnisses geregelt werden. Soweit zu dem geschädigten Dritten keine Vertragsbeziehung besteht, scheidet eine Haftungsbeschränkung von vornherein aus.

Nachweis von Verursachung von Schäden und Pflichtverletzung
Die Grundsätze zum Nachweis ergeben sich, soweit es um Schadensersatz geht, aus dem Prozessrecht des angerufenen Gerichts, bei deutschen Gerichten folglich aus dem Beweisrecht der Zivilprozessordnung (ZPO).

Haftung für Verhalten Dritter
Ein spezifischer Aspekt der Kooperation in der I4.0 betrifft die Haftung für Verursachungseiträge anderer Kooperationspartner oder Dritter, etwa von Angreifern. Diese Frage erreicht in der I4.0 wegen der Komplexität der einbezogenen Akteure und der Abläufe eine neue Qualität und bedarf daher besonderer Beachtung. Spezifische rechtliche Regelungen hierfür existieren bisher nicht. Maßgeblich sind die allgemeinen Grundsätze der vertraglichen (§§ 280 ff. BGB) oder deliktischen Haftung (§§ 823 ff. BGB), auf die auch in Sonderregeln regelmäßig verwiesen wird.

3.3.3 Aspekte des Datenschutzes

Aufgrund des erheblichen Datenaufkommens durch die Vernetzung im Rahmen von Industrie 4.0, spielen datenschutzrechtliche Aspekte bei der Bestimmung des Rechtsrahmens eine wesentliche Rolle.

3.3.3.1 Bundesdatenschutzgesetz (BDSG)

Bei der Anwendung der datenschutzrechtlichen Normen ist zu beachten, dass das Datenschutzrecht in Deutschland nur personenbezogene und nicht rein unternehmensbezogene Daten schützt.[85] Es ist mithin auch bei Vorgängen im Rahmen von I4.0 stets in einem ersten Schritt zu prüfen, ob bspw. innerhalb eines Prozessschrittes bei der automatisierten Maschinenkommunikation personenbezogene Daten, dies meint Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person, verwendet werden, d. h. solche Daten, die einen Rückschluss auf die Identität eines Menschen zulassen.[86]

Ist dies der Fall, ist weiter festzustellen, ob diese Daten im deutschen Inland erhoben, verarbeitet und/oder genutzt werden, wobei hierunter auch die Weitergabe der Daten an einen Dritten im In- oder Ausland fällt.[87] Denn dann gilt nach dem in § 4 Abs. 1 BDSG geregelten sog. Verbot mit Erlaubnisvorbehalt ein grundsätzliches Verbot der Erhebung, Verarbeitung oder Nutzung solcher personenbezogenen Daten. Dieses Verbot kann seinerseits nur durch Rechtsvorschrift oder Einwilligung des Betroffenen durchbrochen werden.[88]

Einwilligung des Betroffenen
Ob die Einholung von Einwilligungen der Betroffenen bei Vorgängen im Rahmen von I4.0 praktikabel und rechtssicher ausgestaltet werden kann, muss jeweils im einzelnen Anwendungsfall geprüft werden. Hierbei ist zu beachten, dass eine Einwilligung des Betroffenen nur dann wirksam erteilt werden kann, wenn der Betroffene über sämtliche Schritte der Datenverarbeitung genau informiert ist. Insoweit wird von der sog. informierten Einwilligung gesprochen.[89] Dies umfasst auch hinreichende Informationen bezüglich potenzieller Übermittlungsempfänger der Daten[90], was aufgrund der Komplexität der technischen Vorgänge im Rahmen von I4.0 voraussichtlich mit nicht unerheblichen Herausforderungen verbunden sein wird.

Soweit Beschäftigtendaten von den verschiedenen Datenerhebungen, -verarbeitungen oder -nutzungen betroffen sind, stellt sich überdies die Frage nach der von § 4a Abs. 1 Satz 1 BDSG geforderten Freiwilligkeit der Einwilligungserklärung. So ist umstritten, ob aufgrund des insoweit bestehenden „faktischen Zwangs“ im Beschäftigungsverhältnis eine wirksame Einwilligung seitens des Arbeitgebers eingeholt werden kann.[91] Das Bundesarbeitsgericht (BAG) hat zuletzt in seinem Urteil vom 11. Dezember 2014 (AZ: 8 AZR 1010/13) für – die situativ vergleichbare – Freiwilligkeit der Einwilligung eines Beschäftigten nach § 22 KUG hinsichtlich Bildveröffentlichungen zu seiner Person durch seinen Arbeitgeber die Auffassung vertreten, dass diese als freiwillig anzusehen ist, wenn keine konkreten Anhaltspunkte für die Ausübung von Druck oder Zwang bestehen (BAG, Urteil vom 11. Dezember 2014, AZ: 8 AZR 1010/13, Rn. 32 und 33). Das BAG verneint damit die Gegenauffassung, die in einem Beschäftigungsverhältnis generell einen „faktischen Zwang“ unterstellt.

Die Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten spielt bei der Anwendung von I4.0 eine erhebliche Rolle, so etwa im Rahmen von Produktionsprozessen wie dem Einsatz von Assistenzsystemen, wenn diese bspw. den Standort, die Vitalfunktionen oder die Qualität der Aufgabenerfüllung durch einen Mitarbeiter aufzeichnen.[92] Entsprechend dürfte die Verarbeitung von Beschäftigtendaten im Kontext von I4.0 oftmals als unumgänglich zu qualifizieren sein, wobei die zuvor erwähnten Verarbeitungsbeispiele zeigen, dass auch sensitive Daten (§ 3 Abs. 9 BDSG) oder Daten, die der Leistungs- und Verhaltenskontrolle der Beschäftigten dienen, betroffen sein können.

Das BDSG sieht mit solchen Verarbeitungen *„besondere Risiken für die Rechte und Freiheiten der Betroffenen“* verbunden, weshalb es entsprechende Verarbeitungsarten unter die Vorabkontrolle des § 4d Abs. 5 BDSG durch den betrieblichen Datenschutzbeauftragten stellt. An die datenschutzrechtliche Legitimation werden mitunter daher erhöhte Anforderungen zu stellen sein, wobei letztlich zu klären sein wird, ob deshalb die Einwilligungseinholung zwingend notwendig für die Rechtmäßigkeit der entspre-

85 Simitis/Dammann, BDSG, 8. Aufl. 2014, § 3 Rn. 17.
86 Vgl. Simitis/Dammann, BDSG, 8. Aufl. 2014, § 3 Rn. 7.
87 Vgl. § 3 Abs. 4 Nr. 3 BDSG.
88 Gola/Schomerus, BDSG, 11. Aufl. 2012, § 4 Rn. 3.
89 Behling/Abel/Ringel, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 10 Rn. 118.
90 Simitis/Dammann, BDSG, 8. Aufl. 2014, § 4a, Rn. 72.
91 Behling/Abel/Gola, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 8 Rn. 10; Däubler/Hjort/Schubert/Wolmerath/Hilbrans, Arbeitsrecht, 3. Aufl. 2013, BDSG § 4a, Rn. 3.
92 Forschungsunion/Acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0 April 2013, S. 64.

chenden Verarbeitungsarten ist. Denn ist dies festzustellen, dürfte als anerkannt gelten, dass eine Einwilligungseinholung auch im Beschäftigungsverhältnis in jedem Falle möglich sein muss.[93] Insoweit dürften die zuvor erläuterten Erwägungen des BAG zu übertragen sein.

Betriebsvereinbarungen und Tarifverträge
Wo rechtliche Unsicherheiten bezüglich der Möglichkeit zur wirksamen Einwilligungseinholung verbleiben oder insoweit praktische Herausforderungen entgegenstehen, wird zu klären sein, ob der Abschluss von Betriebsvereinbarungen oder der Rückgriff auf Tarifverträge in Betracht kommt, um die fraglichen Verarbeitungen von Beschäftigtendaten zu legitimieren. So ist jedenfalls für Betriebsvereinbarungen anerkannt, dass auch diese Erlaubnisnormen i. S. v. § 4 Abs. 1 BDSG darstellen können, wenn die Betriebsparteien darin die Verarbeitung von Beschäftigtendaten regeln.[94] Andererseits spricht Vieles dafür, dass auch Betriebsvereinbarungen keine Datenverarbeitungen legitimieren können, die das BDSG selbst nicht zuließe.[95] Entsprechend wird zu analysieren sein, ob und inwieweit gerade sensible Verarbeitungen von Beschäftigtendaten im Kontext von I4.0 über den Abschluss von Betriebsvereinbarungen abgedeckt werden können. Im Hinblick auf Tarifverträge wird insbesondere zu klären sein, ob solche betrieblichen Einzelfragen, wie eine konkrete Datenverarbeitung, überhaupt hierin geregelt werden können.

Legitimationsnorm des § 32 Abs. 1 S. 1 BDSG
Sollten Einwilligungen oder Betriebsvereinbarungen letztlich ausscheiden, um die entsprechenden Verarbeitungen von Beschäftigtendaten im Kontext von I4.0 umfassend zu legitimieren, stellt sich die Frage, ob diese nach § 32 Abs. 1 Satz 1 BDSG erlaubt sind. Danach dürfen *„[p]ersonenbezogene Daten eines Beschäftigten [...] für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.“*

Gerade der der Vorschrift innewohnende Grundsatz der Erforderlichkeit kann im Zusammenhang mit I4.0 mit Herausforderungen verbunden sein. So ist nach überwiegender Meinung im Schrifttum eine Erforderlichkeit im vorgenannten Sinne nur gegeben, wenn die Datenverarbeitung jeweils geeignet und gegenüber dem Beschäftigten das relativ mildeste Mittel ist, um den unternehmerischen Interessen bei der Begründung, der Durchführung oder Beendigung von Beschäftigungsverhältnissen Rechnung zu tragen.[96] Letztlich dürfte die Nutzung von I4.0 aber vor allem der Modernisierung und Effizienzsteigerung dienen, weshalb sich die Frage stellt, ob bzw. inwieweit eine Erforderlichkeit der damit einhergehenden Verarbeitungen von Beschäftigtendaten zur Durchführung des jeweiligen Beschäftigungsverhältnisses tatsächlich bejaht werden kann.

Legitimationsnorm des § 28 BDSG
Sollten sich vor dem erläuterten Hintergrund die entsprechenden Verarbeitungen von Beschäftigtendaten nicht auf § 32 Abs. 1 Satz 1 BDSG stützen lassen, stellt sich die Frage, ob § 28 Abs. 1 Satz 1 Nr. 2 BDSG als Erlaubnisnorm herangezogen werden kann. Dies ist umstritten und wird entsprechend nicht einheitlich beurteilt.[97] Sollten sich Verarbeitungen von Beschäftigtendaten im Zusammenhang mit I4.0 nicht auf § 32 Abs. 1 Satz 1 BDSG stützen lassen, wird deshalb zu klären sein, ob § 28 Abs. 1 Satz 1 Nr. 2 BDSG insoweit als Auffangnorm herangezogen werden kann.

Werden andere personenbezogene Daten als Beschäftigtendaten im Rahmen von I4.0 verarbeitet, wird eine Anwendbarkeit von § 28 Abs. 1 Satz 1 BDSG häufig gegeben sein. Vor dem Hintergrund, dass I4.0 ferner dazu dienen dürfte, Betreiber entsprechender Anlagen in die Lage zu versetzen, auf individuelle Kundenwünsche unmittelbar eingehen zu können, liegt es nahe, dass auch personenbezogene Kundendaten Gegenstand der Verarbeitung sein können. Entscheidet sich etwa der Käufer eines PKW für eine Individuallackierung und wird die individuelle Farbcodierung deshalb zwischen den beteiligten Rechnern und intelligenten Lackierrobotern im Industrie 4.0-Umfeld des Automobilherstellers ausgetauscht, dürfte der spezielle Farbcode – da dieser dem fraglichen Kunden zugeordnet werden kann – als personenbezogenes Datum zu qualifizieren sein.

Eine Anonymisierung im datenschutzrechtlichen Sinne, die den Personenbezug und damit die datenschutzrechtliche Problematik entfallen lassen würde, dürfte hier demgegen-

93 Behling/Abel/Gola, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 8 Rn. 10.
94 Behling/Abel/Gola, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 8 Rn. 17.
95 Behling/Abel/Gola, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 8 Rn. 17.
96 Simitis/Seifert, BDSG, 8. Aufl. 2014, § 32 Rn. 11.
97 Behling/Abel/Gola, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 8 Rn. 6; Gola/Schomerus/Gola/Schomerus, BDSG, § 32 Rn. 31 ff.

über nur schwerlich zu erreichen sein. Denn damit das Fahrzeug mit dem individuellen Farbcode mit dem Abschluss der Lackierung dem richtigen Kunden zugeordnet werden kann, müssen Farbcode und Kunde mit einem Zuordnungsmerkmal verknüpft werden, sodass regelmäßig eine Personenbeziehbarkeit gegeben sein wird. So meint Anonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (§ 3 Abs. 6 BDSG).[98] Hier ist jedoch gerade die spätere Zuordnung zum Kunden beabsichtigt und notwendig. Dies wird auf die meisten Verarbeitungsverfahren zutreffen, die im I4.0-Umfeld erfolgen, um individualisierte Produktionsschritte für menschliche Endkunden durchzuführen.

Die Verarbeitung des personenbezogenen Datums ist an § 28 Abs. 1 Satz 1 BDSG zu messen, falls keine legitimierende Einwilligung des Betroffenen hierfür vorliegt. Insoweit einschlägig sein können die Nummern 1 und 2 dieser Vorschrift, die das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke erlauben,

- „wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist“ (Nr. 1) oder

- „soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt“ (Nr. 2).

Wie bei § 32 Abs. 1 Satz 1 BDSG steht also auch bei diesen Erlaubnistatbeständen der Grundsatz der Erforderlichkeit im Vordergrund, weshalb es in Bezug auf die Verarbeitung von personenbezogenen Kundendaten ebenfalls zu klären gilt, ob diese allein auf die gesetzlichen Erlaubnistatbestände des § 28 Abs. 1 Satz 1 Nr. 1 und 2 BDSG gestützt werden können.

Auftragsdatenverarbeitungen § 11 BDSG
Soweit Produktion und Datenverarbeitungen im Rahmen von I4.0 ausschließlich im Europäischen Wirtschaftsraum (EWR) stattfinden, können zumindest die Datenübermittlungen möglicherweise auch durch die Vereinbarung einer Auftragsdatenverarbeitung nach § 11 BDSG legitimiert werden. Denn sind deren Voraussetzungen erfüllt, ist der Transfer von personenbezogenen Daten zwischen zwei verschiedenen Stellen selbst dann erlaubt, wenn sich dieser nicht über die gesetzlichen Erlaubnistatbestände der §§ 28, 32 BDSG legitimieren lässt, § 3 Abs. 7 und 8 Satz 2 BDSG. Allerdings ist die Konstruktion der Auftragsdatenverarbeitung an verschiedene Voraussetzungen geknüpft, deren Umsetzbarkeit im Zusammenhang mit I4.0 zu prüfen ist. So kommt eine Auftragsdatenverarbeitung etwa nur in Betracht, wenn der Datenempfänger streng nach den Weisungen der übermittelnden Stelle agiert, was immer dann problematisch ist, wenn letztere ein Eigeninteresse an den fraglichen Daten hat. Entsprechend wird zu prüfen sein, ob eine Auftragsdatenverarbeitung im Industrie 4.0-Umfeld überhaupt in Betracht kommt und, falls ja, ob es Besonderheiten bei der Vertragsgestaltung zu beachten gilt. Sie kann insbesondere bei der Beteiligung von Dienstleistern relevant sein, auf die zur Unterstützung bei der Erhebung, Verarbeitung und Nutzung der Daten zurückgegriffen wird.

§§ 4b, 4c BDSG
Sofern personenbezogene Daten (auch) außerhalb des EWR (in sog. Drittländern) im Rahmen von I4.0 verarbeitet werden, setzt dies voraus, dass ein angemessenes Datenschutzniveau bei der empfangenden Stelle außerhalb des EWR gewährleistet ist. Hierzu kommen grundsätzlich verschiedene Instrumente in Betracht, bspw. der Abschluss von sog. EU-Standardverträgen oder auch die Implementierung von Binding Corporate Rules.[99] Ob diese im Einzelfall geeignet sind, ein angemessenes Datenschutzniveau herzustellen, ist – nicht zuletzt vor dem Hintergrund, dass zumindest bestehende Verarbeitungsbezüge zu den USA wegen des NSA-Skandals seitens der Datenschutzaufsichtsbehörden stets kritisch gesehen werden[100] – zu eruieren.

98 Zu den Anforderungen an eine Anonymisierung vgl. etwa Simitis/Dammann, BDSG, 8. Aufl. 2014, § 3 Rn. 196ff.
99 So auch Forschungsunion/Acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0 April 2013, S. 64.
100 Vgl. Pressemitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Datenschutzkonferenz: Geheimdienste gefährden massiv den Datenverkehr zwischen Deutschland und außereuropäischen Staaten“ v. 24.7.2013, abrufbar unter http://www.datenschutz-bremen.de/sixcms/detail.php?gsid=bremen236.c.9283.de

Verstoß gegen das Zweckbindungsgebot
Im Übrigen sind auch Verstöße gegen das datenschutzrechtlich geltende Zweckbindungsgebot[101] möglich, wenn bspw. für kundenorientierte Produkteigenschaften datenverarbeitende Komponenten am Endprodukt verbleiben und dadurch bei dem Besteller des Produkts zweckändernd genutzt werden können.[102] So ist spezifisch relevant für Industrie 4.0, dass solche Komponenten im Produktionsprozess verwendet werden[103], wobei es nahe liegt, dass diese beispielweise Beschäftigtendaten aufnehmen, die dann, wenn das Endprodukt den Besteller erreicht, ggf. durch diesen für eigene Zwecke ausgelesen und verwendet werden können.

3.3.3.2 Entwurf Beschäftigtendatenschutzgesetz

In Bezug auf Beschäftigtendaten sei weiterhin erwähnt, dass im Jahre 2010 der Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes (BDSG-E) auf Grundlage eines Referentenentwurfs des Bundesinnenministeriums durch die Bundesregierung verabschiedet wurde.[104] Der Entwurf wurde aufgrund von erheblichen Unstimmigkeiten innerhalb der 17. Legislaturperiode nicht mehr verabschiedet und verfiel wegen des Grundsatzes der sachlichen Diskontinuität nach Ablauf dieser Legislaturperiode im September 2013.[105] Derzeit ist eine Verabschiedung des Entwurfs nicht absehbar; dies insbesondere vor dem Hintergrund des aktuellen Entwurfs der EU-Datenschutz-Grundverordnung (DS-GVO), bei welchem noch nicht feststeht, ob bei dessen Inkrafttreten nationale Abweichungen noch zulässig bleiben.[106] Allenfalls, wenn eine Regelung des Beschäftigtendatenschutzes auf europäischer Ebene – wie derzeit vorgesehen[107] – sicher nicht erfolgen wird, soll der Entwurf zum Beschäftigtendatenschutz neu aufgerollt werden.[108]

Sofern der BDSG-E hiernach doch noch in Kraft treten sollte, ist von einem gegenüber dem geltenden § 32 BDSG strengeren Erforderlichkeits- und Zweckbindungsmaßstab auszugehen, der durch § 32c und § 32d BDSG-E statuiert würde und an dem sich entsprechend auch die Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten im Rahmen von I4.0 messen lassen müssten. Im Falle seines Inkrafttretens würde der BDSG-E daher einen wesentlichen datenschutzrechtlichen Compliance-Rahmen vorgeben, den es entsprechend umzusetzen gilt. Aufgrund des Umstandes allerdings, dass der BDSG-E zum derzeitigen Stand als verfallen anzusehen ist, wird dieser bei der nachfolgenden Betrachtung außen vor bleiben.

3.3.3.3 EU-Datenschutzgrundverordnung

Die EU-Kommission hat im Januar 2012 einen Entwurf der DS-GVO zur Harmonisierung des Datenschutzrechts in der EU vorgelegt, welcher stark kritisiert wurde.[109] Im März 2014 wurde hieraus seitens des Europäischen Parlaments eine Verhandlungsposition entwickelt und auch verabschiedet; der Rat der Europäischen Union einigte sich sodann im Juni 2014 über bestimmte Aspekte des Entwurfs der DS-GVO[110] und beschloss schließlich im Juni 2015 eine allgemeine Ausrichtung.[111] Zum Zeitpunkt der Anfertigung dieser Studie dauern die Beratungen zwischen Kommission, Parlament und Rat im sog. Trilog noch an. Ob und wann ein Inkrafttreten des Entwurfs der DS-GVO zu erwarten steht, ist zurzeit jedoch noch nicht absehbar; jedenfalls ist aber ein klarer Wille erkennbar, die Verabschiedung der DS-GVO voranzutreiben.[112]

Im Falle ihres Inkrafttretens wird die DS-GVO das geltende Datenschutzrecht grundlegend umgestalten. Dabei wird es eines Umsetzungsaktes auf nationaler Ebene dann nicht

101 Danach dürfen personenbezogene Daten grundsätzlich nur zu dem Zweck verarbeitet werden, zu dem sie auch erhoben worden sind, vgl. z. B. § 28 Abs. 2 BDSG.
102 Forschungsunion/Acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0 April 2013, S. 64, vgl. auch BMWi, Band 2 zur AUTONOMIK, Stand Januar 2013, S. 12.
103 Forschungsunion/Acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0 April 2013, S. 64, vgl. auch BMWi, Band 2 zur AUTONOMIK, Stand Januar 2013, S. 12.
104 BT-Drs. 17/4230.
105 Behling/Abel/Behling, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 14 Rn. 7; Simitis/Seifert, BDSG, 8. Aufl. 2014, § 32 Rn. 3.
106 Simitis/Seifert, BDSG, 8. Aufl. 2014, § 32 Rn. 3.
107 Behling/Abel/Behling, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 14 Rn. 7.
108 Simitis/Seifert, BDSG, 8. Aufl. 2014, § 32 Rn. 3.
109 Roßnagel/Kroschwald, ZD 2014, 495, 495.
110 Behling/Abel/Behling, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 14 Rn. 17.
111 Interinstitutionelles Dossier: 2012/0011 (COD) des Rates der Europäischen Union, abrufbar unter: http://data.consilium.europa.eu/doc/document/ST-13772-2014-INIT/de/pdf
112 Behling/Abel/Behling, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 14 Rn. 17.

mehr bedürfen, da sie – verordnungstypisch – in allen Mitgliedsstaaten unmittelbar gelten wird.[113] Das laufende Verfahren zielt jedenfalls nach derzeitigem Stand auf eine Gesamtharmonisierung ab[114] und wird in diesem Zuge Unternehmen u.a. auch dazu anhalten, die Grundsätze von „privacy by design“ und „privacy by default“ umzusetzen.

„Privacy by design“

Dabei meint „privacy by design“, dass unter Berücksichtigung neuester technischer Errungenschaften, des Stands der Technik, bewährter internationaler Verfahren und den von der Datenverarbeitung ausgehenden Risiken sowohl zum Zeitpunkt der Festlegung der Verarbeitungszwecke und -mittel als auch zum Zeitpunkt der Datenverarbeitung selbst geeignete und verhältnismäßige technisch-organisatorische Maßnahmen sowie Verfahren zu implementieren sind, durch die sichergestellt wird, dass die Verarbeitung den Anforderungen der DS-GVO genügt und die Betroffenenrechte gewahrt werden.[115] Dies dürfte für I4.0 mit nachhaltigen Herausforderungen verbunden sein, da im Falle personenbezogener Datenverarbeitungen in diesem Kontext die Datenverarbeitungen sowohl in rechtlicher als auch in technisch-organisatorischer Hinsicht voraussichtlich „Best Practice“-Standards genügen müssten.

„Privacy by default“

„Privacy by default“ meint dagegen, dass Verarbeitungsverfahren – per Voreinstellung – sicherstellen müssen, dass sowohl in zeitlicher als auch in quantitativer Hinsicht nur so viele personenbezogene Daten erhoben, behalten und verbreitet werden, wie dies gemessen am jeweiligen Verarbeitungszweck unbedingt erforderlich ist.[116] Sowohl Entwickler als auch Betreiber von Anlagen im Umfeld von I4.0 werden mit Inkrafttreten der DS-GVO daher sicherstellen müssen, dass trotz der voraussichtlich großen Datenmenge, die in diesem Zusammenhang verarbeitet wird, das Maß an personenbezogenen Daten so gering zu halten ist, wie es eben möglich ist. Auch dies stellt sich möglicherweise als eine Herausforderung für die Umsetzung dar. Sollen (personenbezogene) Daten, die im I4.0 Kontext erhoben worden sind, etwa zu statistischen Zwecken auch für Big Data-Analysen weiterverwendet werden, sollten diese zur Vermeidung datenschutzrechtlicher Komplikationen daher möglichst vollanonymisiert werden. Dies gilt vor dem Hintergrund der nach BDSG zu beachtenden Grundsätze der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) sowie der Erforderlichkeit (§§ 28 Abs. 1 S. 1 Nr. 2; § 32 Abs. 1 S. 1 BDSG) im Übrigen auch heute schon.

Weitere Herausforderungen

Weitere Herausforderungen können daraus erwachsen, dass durch die DS-GVO voraussichtlich sowohl die Anforderungen an eine Einwilligung des Betroffenen als auch die Tatbestandsmerkmale von gesetzlichen Erlaubnissen verändert werden, wenngleich diese mitunter auch weniger streng gehalten sind als die des BDSG.[117]

Ein weitaus wesentlicherer Unterschied zum rechtlichen Status quo in Deutschland besteht allerdings bei der Auftragsdatenverarbeitung, da diese die Übermittlung von personenbezogenen Daten – auch wenn sie im Inland verbleiben – nicht mehr privilegieren würde.[118]

Die Datenübermittlung an Stellen außerhalb des EWR bleibt an ähnliche Voraussetzungen wie im Regelungsregime des BDSG geknüpft, wobei Angemessenheitsentscheidungen der EU-Kommission in Bezug auf das jeweilige Land ggfs. eine höhere Bedeutung eingeräumt wird. So wird im aktuellen Gesetzgebungsverfahren bezüglich der Zulässigkeit der Übermittlung von personenbezogenen Daten in einen sog. Drittstaat diskutiert, ob diese von einer Angemessenheitsentscheidung durch die EU-Kommission abhängig gemacht werden soll, wobei diese auch negativ ausfallen können soll.[119] Würde die EU-Kommission also zu dem Ergebnis kommen, dass gewisse Länder nicht sicher sind, bedürfe es ergänzender Maßnahmen, um diese bei I4.0 mit einbinden zu können.

Insoweit wird es – wie im heutigen System der §§ 4b, 4c BDSG – weiterhin Ausnahmetatbestände wie bspw. abgeschlossene EU-Standardvertragsklauseln geben, die notwendige Garantien gewährleisten können und zwar auch dann, wenn die Angemessenheitsentscheidung negativ ausgefallen ist.[120]

113 Behling/Abel/Behling, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 1 Rn. 5.
114 Beck OK Datenschutzrecht/Spoerr, 9. Ed., Stand 01.08.2014, § 11 BDSG Rn. 141.
115 Behling/Abel/Behling, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 1 Rn. 43.
116 Behling/Abel/Behling, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 1 Rn. 45.
117 Roßnagel/Kroschwald, ZD 2014, 495, 497.
118 Roßnagel/Kroschwald, ZD 2014, 495, 497.
119 Roßnagel/Kroschwald, ZD 2014, 495, 498.

Insgesamt ist daher im Rahmen einer kursorischen Betrachtung zu überprüfen, inwiefern die Anforderungen des aktuell gültigen Entwurfs der DS-GVO von den Anforderungen des BDSG abweichen, um festzustellen zu können, ob sich daraus mögliche Umsetzungshindernisse ergeben.

3.3.4 Welthandelsrecht (WTO-Recht)

Neben dem Datenschutzrecht hat möglicherweise auch das WTO-Recht Auswirkungen auf Industrie 4.0. Über das WTO-Recht sind alle Mitglieder der Welthandelsorganisation (WTO)[121], zu denen auch Deutschland zählt, zur Einhaltung von Standards bei der Ausgestaltung ihrer Außenhandelsbeziehungen verpflichtet. Diese Pflicht umfasst auch die Einhaltung des "General Agreement on Tariffs and Trade" (GATT), des "General Agreement on Trade in Services" (GATS) sowie der „Trade Related Aspects of Intellectual Property Rights" (TRIPS). Insofern wird im Kontext von I4.0 zu eruieren sein, ob diese völkerrechtlichen Normen in Deutschland unmittelbar Anwendung finden[122] und, falls ja, ob sich hieraus Restriktionen ergeben.

3.3.4.1 GATT

Das GATT soll zur Liberalisierung des grenzüberschreitenden Handels mit Waren in der Weise beitragen, dass Vereinbarungen getroffen werden, die auf der Grundlage der Gegenseitigkeit und zum gemeinsamen Nutzen auf einen wesentlichen Abbau der Zölle und anderer Handelsschranken sowie auf die Beseitigung der Diskriminierung im internationalen Handel abzielen.[123] Als Waren in diesem Sinne werden körperliche, greifbare Gegenstände verstanden.[124]

Fraglich ist, ob dieser Warenbegriff bei I4.0 tatsächlich gesondert zum Tragen kommen kann. Zwar werden im Zuge von I4.0 auch Maschinen eingesetzt, mit denen Waren automatisiert produziert werden können, sodass sowohl auf Maschinenseite als auch auf Produktseite Waren im Sinne des GATT in Frage stehen können. Dies ist aber keine Eigenheit von Industrie 4.0, sondern gilt bereits heute für jede maschinelle Warenproduktion.

Wie einleitend ausgeführt, unterscheidet sich I4.0 vom industriellen Status quo vielmehr durch die umfassende Maschinenvernetzung und den intelligenten Informationsaustausch über das Internet. Es steht also nicht der Waren-, sondern der intelligente Informationsaustausch bei I4.0 im Vordergrund, der aber – da sich dieser über das Internet unkörperlich vollzieht – nicht in den Anwendungsbereich des GATT fallen dürfte. Entsprechend soll das GATT bei der nachfolgenden Betrachtung außen vor bleiben.

3.3.4.2 GATS

Das GATS als Gegenstück zum GATT regelt den Abbau von Hemmnissen im grenzüberschreitenden Handel mit Dienstleistungen.[125] Der Begriff der Dienstleistung selbst wird im GATS nicht definiert. Die Erbringung einer Dienstleistung wird aber als die Erzeugung, der Vertrieb, die Vermarktung, der Verkauf oder die Bereitstellung einer Dienstleistung durch einen Akteur aus einem anderen Mitgliedsstaat der WTO-Abkommen definiert.[126] In der Literatur heißt es hierzu, eine Dienstleistung sei „die zu einem bestimmten Zeitpunkt erbrachte Leistung, zur Befriedigung eines Bedürfnisses".[127] Mithin kommt eine Anwendbarkeit des GATS im Zusammenhang mit I4.0 zumindest in Betracht; etwa unter dem Aspekt der Erbringung von (Fern-) Wartungsdienstleistungen, die bspw. vorstellbar sind, wenn Systeme oder Applikationen von I4.0–Maschinen nicht mehr einwandfrei arbeiten und deshalb Instandsetzungsarbeiten per Fernzugriff durch den Hersteller erfolgen.

120 Roßnagel/Kroschwald, ZD 2014, 495, 498.
121 Zurzeit zählt die WTO 160 Mitgliedsstaaten. Eine jeweils aktuelle Liste der Mitglieder einschließlich deren Beitrittsdatum ist abrufbar unter: http://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm
122 Sehr strittig. Hierzu insgesamt: Ohler, WuR-Bei 2012, 137; dagegen EuGH, Rs. C-149/96, Portugal/Rat, Urteil vom 23.11.1999, Slg. 1999, I-8395.
123 Art. 1 Abs. 2 GATT.
124 Sucker, ZUM 2009, 30, 31.
125 Sucker, ZUM 2009, 30, 30.
126 Vgl. Art. XXVIII Abs. 2 GATS.
127 Sucker, ZUM 2009, 30, 31.

3.3.4.3 TRIPS

Damit stellt sich schließlich die Frage, ob etwas Anderes zumindest in Bezug auf das TRIPS gelten kann.

Das TRIPS betrifft die handelsbezogenen Aspekte des geistigen Eigentums und kann deshalb bei der Umsetzung von I4.0 anwendbar sein, wenn die ausgetauschten Informationen in der Produktionskette als „geistiges Eigentum" i. S. d. TRIPS zu qualifizieren sind. Dies liegt insofern nahe, als der Industrie 4.0-typische Informationsaustausch möglicherweise in den Anwendungsbereich von Art. 39 Abs. 2 TRIPS fällt. Danach muss natürlichen und juristischen Personen die Möglichkeit eingeräumt werden, zu verhindern, „dass Informationen, die rechtmäßig unter ihrer Kontrolle stehen, ohne ihre Zustimmung auf eine Weise, die den anständigen Gepflogenheiten in Gewerbe und Handel zuwiderläuft, Dritten offenbart, von diesen erworben oder benutzt werden, solange diese Informationen

a) in dem Sinne geheim sind, dass sie entweder in ihrer Gesamtheit oder in der genauen Anordnung und Zusammenstellung ihrer Bestandteile Personen in den Kreisen, die üblicherweise mit den fraglichen Informationen zu tun haben, nicht allgemein bekannt oder leicht zugänglich sind,

b) wirtschaftlichen Wert haben, weil sie geheim sind, und

c) Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen seitens der Person waren, unter deren Kontrolle sie rechtmäßig stehen."

Entsprechend wird zu eruieren sein, ob in den betrachteten Fallkonstellationen Art. 39 Abs. 2 TRIPS zum Tragen kommt und ob hieraus spezielle Anforderungen für I4.0 resultieren.

3.3.5 Geheimnisschutz

Weiter stellt sich die Frage, ob die im Zuge von I4.0 ausgetauschten, ggf. vertraulichen Informationen, in Deutschland ausreichend rechtlich geschützt sind.[128] Denn nur wenn ein hinreichender rechtlicher Geheimnisschutz sichergestellt ist, ist zu erwarten, dass die verschiedenen Akteure im Rahmen von I4.0 auch bereit sein werden, sensible Informationen über das Internet auszutauschen. Dabei ist zu beachten, dass Informationen insoweit grundsätzlich nur als sog. Betriebs- und Geschäftsgeheimnisse (im Folgenden zusammen „Unternehmensgeheimnisse") geschützt sind, vgl. §§ 17, 18 Gesetz gegen den unlauteren Wettbewerb (UWG). Ein Unternehmensgeheimnis in diesem Sinne ist „jede im Zusammenhang mit einem Unternehmen stehende Information, die nicht offenkundig, sondern nur einem eng begrenzten Personenkreis bekannt ist und nach dem bekundeten Willen des Unternehmensinhabers, der auf einem ausreichenden wirtschaftlichen Interesse beruht, geheim gehalten werden soll".[129] Ob die vertraulichen Informationen jeweils als Unternehmensgeheimnis zu qualifizieren sind und, falls ja, ob die in §§ 17, 18 UWG statuierten Regelungen zu ihrem Schutz genügen, wird gleichfalls Gegenstand der rechtlichen Untersuchung sein. Daneben wird zu untersuchen sein, ob weitere Normen und Gesetze existieren, die den Geheimnisschutz nach UWG in Deutschland flankieren. Zu denken ist dabei etwa an das aus § 3 UWG folgende allgemeine Verbot unlauterer geschäftlicher Handlungen sowie an das deliktsrechtliche Haftungsregimes der §§ 823, 826 BGB.[130]

3.3.6 Exportkontrolle

Schließlich kann die Nutzung von I4.0 exportkontrollrechtlichen Beschränkungen unterliegen. Zwar gilt zunächst der Grundsatz des freien Warenverkehrs. Dieser gilt jedoch nicht absolut, sondern unterliegt aufgrund der Kollision mit höherrangigen Schutzgütern notwendigen Beschränkungen. Der Regelungsgegenstand des Exportkontrollrechts umfasst nicht nur die Kontrolle und Einschränkung des Exports und der Verwendung von Gütern, die aufgrund ihrer technischen Eigenschaften ein Risiko für die nationale Sicherheit darstellen können.[131] Vielmehr kann auch die den Gütern zugrundeliegende Technik, also auch diesbezügliche Informationen unter die Vorschriften des Exportkontrollrechts fallen[132], sodass auch technologische Daten, die im Wege von I4.0 transferiert werden, den Anforderungen des Exportkontrollrecht unterliegen können.

128 Forschungsunion/Acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0 April 2013, S. 63.
129 Ohly, GRUR 2014, 1, 4.
130 So jedenfalls Ohly, GRUR 2014, 1, 4, für den Fall, dass die §§ 17, 18 UWG hinter den Anforderungen des Art. 39 TRIPS zurückblieben, so dass das UWG völkerrechtskonform auszulegen sei.
131 Hilber/Müller, Handbuch Cloud Computing, 2014, S. 761.
132 Hilber/Müller, Handbuch Cloud Computing, 2014, S. 762.

Dies gilt sowohl im Hinblick auf exportkontrollrechtliche Anforderungen des nationalen Rechts, also des Außenwirtschaftsgesetzes (AWH) in Verbindung mit der Außenwirtschaftsverordnung (AWV), als auch im Hinblick auf die insofern ggf. anwendbare europäische Dual-Use-Verordnung (VO EU 428/2009).[133] Während das deutsche Außenwirtschaftsrecht sich primär auf die Exportkontrolle von Waffen und Rüstungsgütern – also von Gütern, die ihrer Natur nach militärischen Zwecken dienen – bezieht, regelt die Dual-Use-Verordnung die Ausfuhr von Gütern, die sowohl für zivile Zwecke als auch potentiell zu militärischen Zwecken Verwendung finden könnten.

So wird jedenfalls vertreten, dass das Bereitstellen oder auch Abrufen von Daten im Rahmen des Cloud Computings unter die jeweiligen exportkontrollrechtlichen Vorschriften fallen kann, sofern der Abruf oder die Bereitstellung zu einem grenzüberschreitendem Datentransfer führt.[134]

Überdies können auch Verschlüsselungstechnologien Exportbeschränkungen unterliegen, namentlich wenn diese unter die EG Dual-Use Verordnung fallen.[135] Da eine Verschlüsselung bei der Übermittlung von vertraulichen Informationen über das Internet im Rahmen von I4.0 regelmäßig anzuraten sein dürfte oder datenschutzrechtlich sogar geboten ist, kann auch diese Exportbeschränkung im Rahmen von I4.0 virulent werden.[136]

Insgesamt wird deshalb auch das Exportkontrollrecht in die rechtliche Betrachtung mit einbezogen werden.

133 Verordnung (EG) Nr. 428/2009 des Rates vom 5. Mai 2009 über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung und der Durchfuhr von Gütern mit doppeltem Verwendungszweck (Dual-Use-VO).
134 Hilber/Müller, Handbuch Cloud Computing, 2014, S. 771.
135 Hoeren/Sieber/Holznagel/Kuner/Hladjk, Multimedia-Recht, 39. Erg.Lfg. 2014, Teil 17 Rechtsprobleme der Kryptographie, Rn. 26 ff.
136 Forschungsunion/Acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0 April 2013, S. 64.

4. Herausforderungen, Bedrohungen & Risiken

4.1 Darstellung und Analyse von konkreten Fallbeispielen

Um bei der weiteren Analyse von neuen Bedrohungen und Risiken möglichst konkrete wirklichkeitsnahe Szenarien zugrunde legen zu können, wurden für die Studie in enger Abstimmung mit betroffenen Unternehmen vier Fallbeispiele skizziert, die nachfolgend dargestellt werden.

Drei Vorbemerkungen müssen dabei vorausgeschickt werden:

1. Wie in der Einleitung bereits beschrieben ist Industrie 4.0 (I4.0) entsprechend der Vision der acatech-Studie[137] heute noch in keinem Unternehmen annähernd voll verwirklicht. Die Fallbeispiele beschreiben daher Vorgänge, die in der derzeitigen Situation von vernetzten industriellen Prozessen tatsächlich stattfinden. Diese werden zum Zweck der Betrachtung neuer IT-Sicherheitsbedrohungen in der Welt von I4.0 in Richtung weiter zunehmender Vernetzung über Länder-, Standort-, und Unternehmensgrenzen, in Richtung zunehmender autonomer Abläufe in Produktion und Logistik und in Richtung zunehmender Verfügbarkeit von großen und teils sensitiven Datenbeständen extrapoliert.

2. Die Unternehmen, die bei der Darstellung der Fallbeispiele mit den Autoren der Studie sehr offen kooperiert haben, haben diesen viele Informationen unter der Bedingung zur Verfügung gestellt, dass in einer zur Veröffentlichung bestimmten Studie ihre Geschäftsgeheimnisse gewahrt bleiben sowie bestimmte Teilnehmer und Vorgänge anonymisiert werden. Solche Vorgänge mussten für die Beschreibung der Fallbeispiele daher entsprechend verallgemeinert werden.

3. Die Fallbeispiele haben ihre Schwerpunkte auf Problemstellungen unterschiedlicher Art. Dementsprechend variieren die Art der Darstellung und die Beschreibungstiefe. So legt das Fallbeispiel aus dem Automobilbau („Inbetriebnahme“) seinen Fokus auf organisatorische Abläufe und rechtliche Aspekte, das Fallbeispiel aus der Chemieindustrie („Netzwerksegmentierung“) ganz spezifisch auf die Vernetzung, das Fallbeispiel aus der Logistik auf die Wertschöpfungsketten („Produktionsoptimierung“), das Fallbeispiel aus dem Maschinenbau („Fernwartung“) auf das Zusammenspiel sehr vieler unterschiedlicher Teilnehmer in einem Gesamtszenario.

4.1.1 Fallbeispiel Automobilbau

4.1.1.1 Kurzbeschreibung

Inbetriebnahmen einzelner Anlagen oder produktionsrelevanter Systeme (Echtzeitsysteme) unter Zeitdruck gefährden die Sicherheit kompletter Produktionsnetze. Bei steigendem Zeitdruck sind Produktionsverantwortliche eher bereit, Sicherheitsrichtlinien zu vernachlässigen als eine Verzögerung des Produktionsanlaufs – und damit Einbußen in produzierten Stückzahlen – in Kauf zu nehmen.

Diese „lokalen“ Verletzungen der Sicherheitsrichtlinien führen typischerweise zu „global“ unsicheren Situationen, weil die Ausnutzung lokaler Sicherheitslücken üblicherweise die gesamte Sicherheitsinfrastruktur kompromittiert.

4.1.1.2 Ausführliche Beschreibung

Die Produktion in der Automobilindustrie zeichnet sich durch einen hohen Automatisierungsgrad aus. Im Allgemeinen erfolgt die Fertigung nach dem Perlenketten-Prinzip [1]. Durch die Nutzung mehrerer hundert Anlagen pro Gewerk mit einem sehr hohen Datenaufkommen kann die Produktion sinnvollerweise nur automatisiert mittels Software betrieben werden, welche die Produktion und die Produktionsanlagen ständig online steuert und überwacht. Daraus resultiert ein Problem, wenn die zugrundeliegende Automatisierungslösung verändert oder aber ein neues Produktionsleitsystem installiert werden soll. Dies kann im Allgemeinen nicht während der laufenden Produktion vorgenommen werden.

Typischerweise werden Veränderungen der Automatisierungssysteme lange vorab geplant und ein Zeitfenster sowie ein Ablaufplan für die zu erledigenden Aufgaben festgelegt. Dabei werden zunächst die Hard- und Software der Automatisierungssysteme an sich (also alle Systeme die sich innerhalb des Produktionsnetzes befinden) fertiggestellt und anschließend die übergeordneten Systeme (Leittechnik, Manufacturing Execution Systems (MES) etc.) installiert. Des Öfteren kommt es dabei zu Verzögerungen beim ersten Teil der Aufgabe, so dass für die Installation der überlagerten Ebene weniger Zeit verbleibt als vorab geplant.

137 Forschungsunion/acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, April 2013.

Im Sinne von I4.0 werden Produktionsnetze eines Unternehmens über mehrere Standorte hinweg zusammengeschaltet. Dies bietet einerseits Vorteile für die Koordination der Gewerke und den Betrieb der Netze, eröffnet aber vom Standpunkt der IT-Sicherheit neue Gefahren und Angriffsziele. Insbesondere bei einer Software-Inbetriebnahme innerhalb des Produktionsnetzes, bleiben die entstehenden Risiken damit nicht (wie bisher) auf ein einzelnes Gewerk beschränkt, sondern können sich sowohl in andere Gewerke, als auch auf andere Produktionsstandorte des Unternehmens fortpflanzen.

Folgendes fiktives Beispielszenario soll die Problematik verdeutlichen: Die komplette Automatisierung eines ganzen Gewerks in der Automobilindustrie soll modernisiert und gleichzeitig ein neues Leitsystem implementiert werden. Die Arbeiten an der Implementierung und Konfiguration der Leitsystem-Software wurden im Vorfeld vorgenommen und im Sinne einer virtuellen Inbetriebnahme vorab auf den benötigten Stand gebracht. Für die eigentliche Inbetriebsetzung der Software waren planmäßig 36 Stunden vorgesehen. Am Abend des zweiten Tages (21 Uhr) war der Produktionsanlauf vorgesehen.

Durch Verzögerungen bei den Vorarbeiten standen aber nur 14 Stunden für die Inbetriebsetzung der Leitsystem-Software zur Verfügung. Zusätzlich hatten sich bei Installation der Automatisierungshardware kleine Abweichungen zur ursprünglichen Spezifikation ergeben, die noch in die Konfiguration des Leitsystems eingearbeitet werden mussten und die folglich nicht vorab getestet werden konnten.

Der Projektleiter seitens des Kunden bestand darauf, dass trotzdem der Produktionsanlauf zum vorab geplanten Termin (21 Uhr) stattfinden müsse.

Da sich das übergeordnete Produktionsleitsystem nicht innerhalb des Produktionsnetzes sondern im Unternehmensnetz befindet, musste die Firewall zwischen diesen Netzen so konfiguriert werden, dass ein performanter und zugleich sicherer Betrieb des Gesamtsystems erfolgen konnte. Genau die Konfiguration der Firewall machte aber Schwierigkeiten, so dass bis 14 Uhr noch kein einziges Signal der Produktionsanlagen – bzw. der datentragenden OPC Data Access (OPC DA)-Server – im Leitsystem sichtbar war.

Bei einer Krisensitzung mit allen Beteiligten beschloss der Produktionsleiter, dass alle Sicherheitseinstellungen der Firewall ausgeschaltet werden sollten, um die Chance zu wahren, den Produktionsanlauf um 21 Uhr zu gewährleisten. Nach Durchführung dieser Maßnahme konnte die Inbetriebsetzung erfolgreich bis zum Produktionsstart durchgeführt werden.

Eigentlich wurde bei der Krisensitzung gleich mitbeschlossen, dass die korrekte Konfiguration der Firewall „in den nächsten Tagen“ nachgeholt werden sollte. Dies geschah aber über einen längeren Zeitraum nicht, da die Angst dadurch einen Produktionsausfall zu erleiden größer war, als die Sicherheitsbedenken.

Durch die unzureichende Konfiguration der Firewall gab es faktisch keine Trennung von Produktions- und Unternehmensnetz. Dies führte zu einer Schwachstelle im Produktionsnetz. Für jeden Angreifer, der in das Unternehmensnetzwerk eindringen konnte, waren die OPC-DA-Server der Produktionsanlagen sichtbar. Damit waren ebenfalls alle Produktionsdaten der Anlagen sichtbar und teilweise die Parameter der Anlagen manipulierbar.

Durch das Zusammenschalten der Produktionsnetze des Unternehmens über mehrere Standorte hatte diese Sicherheitslücke nicht nur lokale Auswirkungen. Vielmehr waren davon drei weitere Werke des Unternehmens betroffen: Ein Werk innerhalb Europas (EU), ein Werk in den USA und ein weiteres Werk in Südamerika.

4.1.1.3 Assets

Zu schützende Assets (Wertgegenstände, zu schützende Vermögenswerte) im Sinne dieses Fallbeispiels sind sämtliche Produktionsanlagen des betroffenen Gewerks, der Nachbargewerke am selben Standort und aller Gewerke, welche sich im gleichen Produktionsnetz an anderen Produktionsstandorten des Unternehmens befinden.

Schäden, die für das Unternehmen entstehen können sind:

- Auspionieren der Produktionsanlagen (Typ, Funktionsweise, Parametrierung etc.).
- Manipulation der Funktionsweise einzelner Anlagen oder mehrerer verketteter Anlagen.

  Dies kann u. U. zu Schäden an der Anlage führen.

  Weit bedeutender ist allerdings, dass nach einer Manipulation einzelne Produktionsschritte evtl. nicht korrekt ausgeführt werden, was zu Mängeln am Produkt führen kann.

Ebenfalls kann die Betriebssicherheit (Safety) der Anlagen durch eine Manipulation beeinträchtigt werden, was unter Umständen Personenschäden beim Bedienpersonal zur Folge haben kann

- Manipulation der Arbeitszeitmodelle verketteter Anlagen.

  Da verkettete Anlagen nicht über Produktionspuffer entkoppelt sind, führt eine Manipulation der Arbeitszeitmodelle fast zwingend zu Produktionsstillständen, da ein einzelnes unpassendes Arbeitszeitmodell in einer Kette zwangsläufig zu Stillstand der gesamten Kette führt.

- Ausspionieren des Produktionsprozesses.

  Plan-, Soll- und Ist-Stückzahlen sowie aktuelle und vergangene Störungen und Stillstände lassen sich typischerweise aus den OPC-DA-Servern der Produktionsanlagen auslesen. Dies lässt Rückschlüsse auf die aktuellen Produktionszahlen und die aktuelle Produktionsqualität zu.

4.1.1.4 Geschäftsprozesse

Da es sich bei diesem Fallbeispiel nicht um einen regulären Geschäftsprozess handelt, können hier nicht (wie sonst üblich) geplante Datenflüsse mit Quellen und Senken angegeben werden. Vielmehr sind zum Zeitpunkt der Inbetriebsetzung alle „normalen“ Geschäftsprozesse außer Kraft gesetzt. Diese werden erst mit Anlauf der Produktion (also nach der Inbetriebsetzung) wieder aktiviert.

4.1.2 Fallbeispiel Anlagen-/Maschinenbau

Dieses Beispiel betrifft den Anwendungsfall der Fernwartung im Anlagen- und Maschinenbau unter dem Gesichtspunkt der IT-Sicherheit. Derzeit existiert hier keine durchgängige oder standardisierte Lösung, was insbesondere kleinen und mittleren Unternehmen zunehmend Probleme bereitet, hinsichtlich derer erwartet wird, dass sie sich mit der zunehmenden Komplexität im Rahmen der Entwicklungen Richtung I4.0 drastisch verschärfen werden.

Der Anwendungsfall verdient in Rahmen dieser Studie vor allem deshalb besondere Beachtung, weil hier typischerweise viele kleine und mittlere Unternehmen oft mit Großunternehmen zu einer für beide Seiten zufriedenstellenden und auch praktikablen Lösung finden müssen. Große Unternehmen müssen heute viele Lösungen akzeptieren, da sonst die Produkte teurer werden, (wenn diese nicht ihre Standard-Sicherheitslösung einsetzen dürfen). KMU müssen dagegen oft auch Szenarien akzeptieren, die große Unternehmen vorgeben.

Des Weiteren spielt bei diesem Anwendungsfall auch das Schutzziel der Unabstreibarkeit eine wichtige Rolle, da hier zeitweilig die faktische Kontrolle und damit die Verantwortung für schützenswerte Daten von einem Akteur auf einen anderen übergehen. Die hierfür erforderliche Vertrauensbasis ist, da mit verfügbaren Methoden nicht quantifizierbar, heute nicht gegeben.

I4.0-Komponenten zeichnen sich unter anderem dadurch aus, dass große Datenmengen gesammelt und über Netzwerke (in Gegensatz zu heute auch dauerhaft) ausgetauscht und ausgewertet werden. Die Fernwartung von Maschinen, die zwar bereits heute vielfach praktiziert wird, wird damit aus Sicht der IT-Sicherheit vielschichtiger und kritischer.

4.1.2.1 Beschreibung

Bei der Fernwartung sind unterschiedliche Fälle zu unterscheiden:

- Die routinemäßige Pflege von Hardware, Firmware und Software (temporär geplante Routine-Wartung)

- Vorausschauende Instandhaltung, basierend auf dauerhaften Zustandsinformationen aus den betroffenen Komponenten

- Online-Hilfestellung durch Spezialisten des Herstellers oder von Service-Unternehmen bei der Analyse und Behebung von Fehlerfällen oder bei der Konfiguration der Komponenten, die adhoc und schnell realisiert werden muss.

Im Falle einer geplanten Routine-Wartung ist der Datenumfang, den der Hersteller für die Durchführung benötigt, in aller Regel vordefiniert und aus Sicht der IT-Sicherheit verhältnismäßig gut beherrschbar. Hier ist vor allem auf das Schutzziel der Verfügbarkeit zu achten, damit beispielsweise ein fehlerhaftes Update nicht zu längeren Produktionsausfällen oder zu Seiteneffekten auf andere Komponenten der Produktionsanlage führt. Die Gefahr wird bei I4.0 freilich zunehmen, dass auch bei solchen Vorgängen sensible Informationen für Außenstehende zugänglich werden. Eingeschliffene Vorgehensweisen bergen stets die Gefahr, Änderungen der Gesamtkonstellation nicht rechtzeitig ausreichend zu berücksichtigen.

Anders verhält es sich schon, wenn die Maschine autonom Daten über ihren Zustand an Dritte (außerhalb des Anwender-Unternehmens) abgibt, z. B. um diesem fortlaufend Informationen zu liefern, wann welche Maßnahmen zur Wartung eingeleitet werden sollten (Anwendung „Condition Monitoring"). Hier besteht bereits ein erhöhtes Interesse des Anwenders, eine Kontrolle darüber zu haben, welche Daten dem Hersteller hier zur Verfügung gestellt werden. Daher wird der Betreiber immer versuchen, dem Hersteller die Daten nicht direkt zur Verfügung zu stellen, sondern über ein Repository, um somit selbst definieren zu können welche Daten dieser erhält.

Im Falle der Online-Unterstützung bei der Analyse von Fehlfunktionen schließlich benötigt der durchführende oder assistierende Spezialist meist einen wesentlich umfangreicheren Zugriff auf die Daten der Maschine beim Anwender und gegebenenfalls sogar darüber hinaus auf Daten aus deren Umgebung. Hier tritt das Schutzziel der Verfügbarkeit zurück, da die Produktion durch die Fehlfunktion ohnehin beeinträchtigt ist, das Schutzziel der Vertraulichkeit erhält eine höhere Bedeutung.

Verschärft wird das Problem in komplex vernetzten Szenarien dadurch, dass bei der Fernwartung nicht nur ein Anwender und ein Hersteller beteiligt sein können, sondern weitere Zulieferer des Herstellers, externe Dienstleister und die Hersteller der Fernwartungs-Lösung selbst. Zudem können sich die genannten Beteiligten in unterschiedlichen Rechtsräumen befinden.

Heutige Fernwartungs-Lösungen basieren meist auf einer bislang hohen – aber zunehmend schwindenden – Vertrauensbeziehung zwischen Hersteller und Anwender. Meist wird dann vom Anwender ein Ende zu Ende VPN Tunnel zu einem Diagnose-Server beim Hersteller aufgebaut, über den der Service-Techniker dann einen Remote-Zugriff auf die Maschine erhält. Diese recht einfachen Szenarien lassen sich bei I4.0 so nicht mehr aufrechterhalten,

- weil der Maschinenhersteller seinerseits die Service-Techniker von Zulieferern von I4.0-Komponenten seiner Maschine in den Wartungsvorgang einbinden muss, um ein Problem zu analysieren und zu beheben,
- weil das dort verfügbare Datenvolumen Unbefugten möglicherweise zu viele Einblicke in die Produktionsprozesse und andere Geschäftsgeheimnisse des Anwenders gewähren würde.

Der konkrete Fall eines Werkzeugmaschinenherstellers ist für I4.0 auch deshalb relevant, weil es sich bei dessen Produkten in der Regel um Unikate handelt, die nach Kundenspezifikationen für ganz bestimmte Zwecke gebaut werden. Ein Einsatz derartiger Maschinen in einem standort- oder firmenübergreifenden Produktionsprozess ist also für I4.0 typisch.

4.1.2.2 Ablauf eines Fernwartungsvorgangs:

Die folgende Beschreibung gilt für ein Szenario, bei dem eine Fernwartungslösung zum Einsatz kommt, in der von virtuellen Maschinen (VM), auf denen die Entwicklungsumgebung läuft, auf die Maschinen beim Anwender/Betreiber zugegriffen wird. Typischerweise werden die Infrastruktur für diese VMs vom Maschinenhersteller oder einem Dienstleister zur Verfügung gestellt.

Ausgangsvoraussetzungen:

1. Es existiert ein Fernwartungsvertrag zwischen einem Hersteller und einem Anwender, in dem die Modalitäten für die Fernwartung geregelt sind.

Fernwartungsvorgang:

1. Der Anwender gibt die Maschine vor Ort zur Fernwartung frei.
2. Es wird ein gesicherter Kommunikationskanal zwischen der Maschine und einer VM auf einem Server in einer Demilitarisierten Zone (DMZ) erzeugt wird, auf der sich die Entwicklungsumgebung für die Maschinen-Software befindet.
3. Der Service-Techniker beim Hersteller kann von seinem Arbeitsplatz aus ebenfalls über einen gesicherten Kanal auf die VM zugreifen. Über die VM hat der Service-Techniker heute in der Regel vollen Zugriff auf die Maschine.

4.1.2.3 Kontrolle und Verantwortung

4.1.2.3.1 Betreiber-zentrierte Lösung

Der Anwender stellt eine zentrale Plattform zur Verfügung, von der aus zu den Maschinenherstellern zum Zweck der Fernwartung Verbindungen hergestellt werden können. Die Hersteller müssen sich auf die jeweiligen Sicherheitsvorgaben jedes einzelnen Anwenders anpassen.

Diese Plattform kann entweder zentral für alle Standorte betrieben werden oder einzeln pro Standort/Produktionsanlage. Die Standorte des Anwenders können in unterschiedlichen Rechtsräumen liegen. Die Hersteller können ebenfalls aus einer Vielzahl unterschiedlicher Länder kommen. Bei Großunternehmen kann es sich dabei leicht um eine vier- bis fünfstellige Zahl von Lieferanten handeln.

Die Plattform selbst befindet sich in einer Demilitarisierten Zone (DMZ) unter Kontrolle des Anwenders. In der DMZ wird auf Servern für jede Maschine oder Komponente, die gewartet werden soll, für die Dauer der Wartung eine virtuelle Maschine (VM) mit der Entwicklungsumgebung eingerichtet.

4.1.2.3.2 Hersteller-zentrierte Lösung

Der Hersteller betreibt eine zentrale Plattform, zu der von den Anwendern zum Zweck der Fernwartung Verbindungen hergestellt werden können. Anwender müssen die jeweiligen Standard-Schnittstellen der Hersteller benutzen, sofern der Hersteller nicht auf Grund gesonderter Vereinbarungen Anwender-spezifische Adaptoren bereitstellt.

Die Plattform befindet sich hier in einer Demilitarisierten Zone (DMZ) unter der Kontrolle des Herstellers. Typischerweise ist in jeder Maschine beim Anwender ein VPN-Modul integriert, das einen Ende-zu-Ende VPN-Tunnel zur DMZ beim Hersteller aufbaut, wo dieser Tunnel in einem VPN-Konzentrator terminiert wird.

Im Übrigen entspricht das Szenario der Lösung 4.1.2.3.1.

Auch hier besteht grundsätzlich die Möglichkeit für den Anwender, Daten aus seinen Maschinen in den VM in der DMZ des Herstellers gefiltert zur Verfügung zu stellen.

4.1.2.3.3 Dienstleister-basierte Lösung

Die DMZ mit den VMs kann auch von einem Dienstleister betrieben werden, der mehreren Herstellern und mehreren Anwendern diese Funktionalität als Service – auch grenzübergreifend – zentral zur Verfügung stellt.

Diese Lösung dürfte aus rechtlicher Sicht wegen der hier zusätzlich zu berücksichtigenden Verantwortlichkeiten für die Informationssicherheit besonders interessant sein. Andererseits kann diese Lösung das Dilemma auflösen, dass sich ein Hersteller auf viele unterschiedliche Arten (Schnittstellen, Sicherheitsrichtlinien, Verfahren) an seine Anwender anpassen muss oder umgekehrt.

4.1.2.3.4 Spezifische IT-Sicherheitsprobleme

Problem (technisch/organisatorisch): Im konkreten Fall betrachtet der Maschinenhersteller das maschinen-interne Netz als seine Domäne, auf die der Anwender keinen Zugriff haben soll. Praktisch ist dieses Paradigma jedoch technisch nicht abgesichert, da sich der Anwender trotzdem Zugriff auf dieses Netz verschaffen kann (z. B. über die USB-Schnittstelle).

Problem (organisatorisch/rechtlich): Manche Anwender fordern, dass der Fernwartungszugriff durch den Hersteller ihnen gegenüber personalisiert wird. An den Hersteller werden Security-Dongles ausgegeben, die dort nur von einer bestimmten Person benutzt werden dürfen und in der Firma sicher verwahrt werden müssen. Dies macht einen 24/7-Support durch den Hersteller teuer und dadurch schwierig bis unmöglich, bei dem z. B. am Wochenende ein Service-Techniker in Rufbereitschaft von zu Hause aus die VPN-Verbindung aufbauen können soll.

4.1.3 Fallbeispiel aus der chemischen Industrie

Das folgende Fallbeispiel umfasst die Netzwerksegmentierung von Produktionsnetzwerken in der chemischen Industrie.

4.1.3.1 Kurzbeschreibung

In den Produktionsprozessen der chemischen Industrie sind heute schon häufig Anlagen über verschiedene Ebenen der Wertschöpfungskette miteinander verbunden und die Steuerung dieser Anlagen miteinander vernetzt. Als Schutzmechanismus ist das Netzwerk, über welches die Anlagen miteinander kommunizieren, in verschiedene Sicherheitszellen unterteilt mit Regeln, welche Komponenten aus welchem Netzsegment mit welchen anderen Komponenten in einem anderen Netzsegment kommunizieren dürfen.

Die Regelung der Netzwerksegmentierung erfordert neue Technologien, wenn im Rahmen von I4.0 die Systeme unternehmensübergreifend und über alle Schritte der Produktion hinweg miteinander vernetzt werden sollen. Zudem wird der „Defense In Depth“-Ansatz, also, dass Schutzmechanismen auf verschiedenen Ebenen, rund um die Pro-

duktionssysteme diese absichern, vermutlich nicht mehr ausreichen, sondern werden neue Sicherheitsmechanismen und -konzepte direkt in den Produktions-/Automatisierungssystemen notwendig.

4.1.3.2 Ausführliche Beschreibung

In der chemischen Produktion sind in einem Bereich oft verschiedene Produktionsanlagen miteinander verbunden und zur Steuerung werden verschiedene Systeme eingesetzt, die miteinander vernetzt sind. Da die eigentlichen Produktionsanlagen oft über unzureichende Schutzmechanismen verfügen, wird durch den Einsatz verschiedener Technologien, z. B. Firewalls, Virtual LANs, Authentisierung, Autorisierung, Anti-Virus, Intrusion-Detection, Sandboxing usw., die Kommunikation zwischen den Systemen kontrolliert. Mittels Netzwerksegmentierung, also virtuellen LANs und auch physisch voneinander getrennten LANs, wird ein wesentlicher Aspekt der Sicherheit abgedeckt.

Netzwerksegmentierung innerhalb eines Produktionsbereichs/ einer Firma

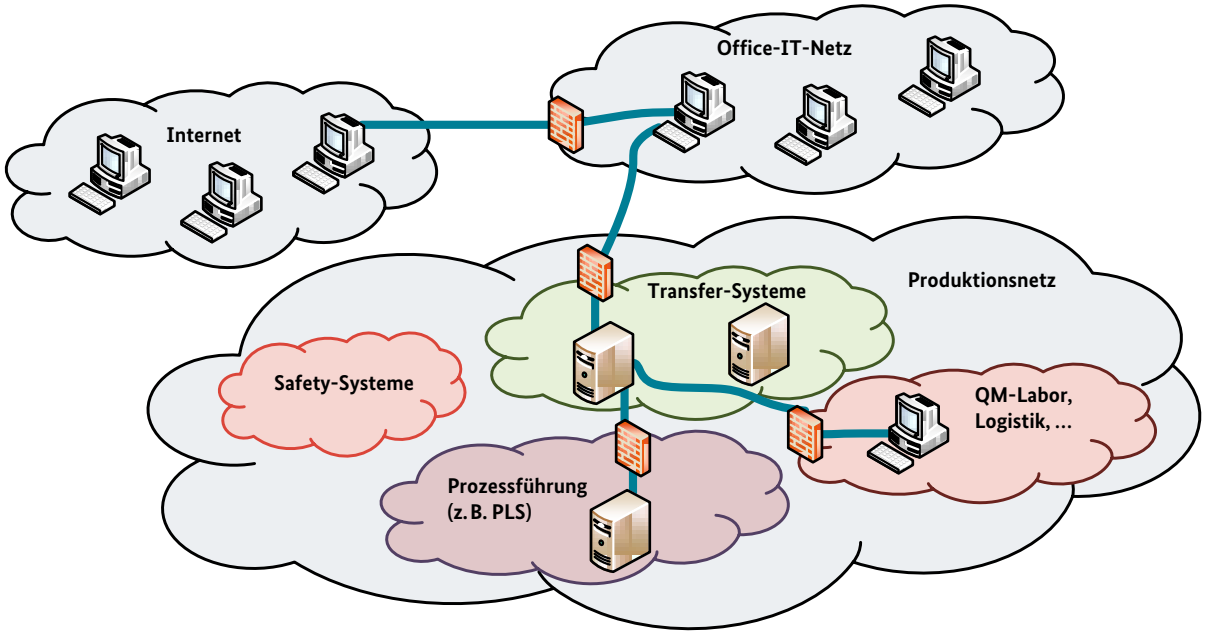
Ein Schutzmechanismus der heute schon in Chemie-Standorten zum Einsatz kommt, ist die Netzwerksegmentierung. Das Firmennetzwerk, wird in verschiedene Bereiche unterteilt, z. B. einem Office-IT-Netz, in dem die Arbeitsplatzrechner vernetzt sind und einem Produktionsnetz, in welchem die Produktionssysteme vernetzt sind. Zudem wird das Produktionsnetz noch weiter in verschiedene Security-Zellen unterteilt, die welches Systeme für spezielle Aufgabenbereiche der Produktion zusammengefasst werden und durch verschiedene Schutzmechanismen, z. B. dem Einsatz von Firewalls, wird über Zugriffslisten gesteuert, welche Systeme über die Security-Zellen hinaus miteinander kommunizieren können.

In Abbildung 4–1 wird in einem Beispiel dargestellt, wie verschiedene Security-Zellen in einem Produktionsnetz mit dem Einsatz von Firewalls den Zugriff nur für speziell definierte Kommunikationswege erlauben. Dabei kann es auch isolierte Security-Zellen geben, z. B. für Safety-relevante Systeme, die überhaupt keinen Zugriff aus anderen Netzwerksegmenten erlauben.

Vernetzung über mehrere Produktionsbereiche/ Firmen hinweg

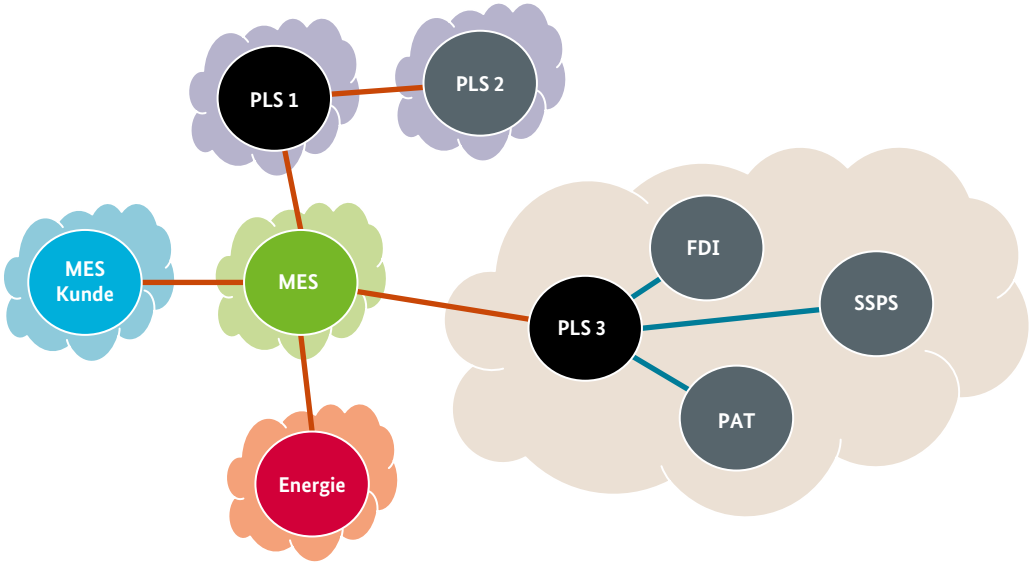
Im Rahmen von I4.0 ist es das Ziel, dass die Produktionssysteme über die komplette Wertschöpfungskette hinweg mit den weiteren Systemen der Auftraggeber, Abnehmer

Abbildung 4–1: Netzwerksegmentierung durch die Definition von Security-Zellen innerhalb eines Netzwerks



Quelle: Software AG

Abbildung 4–2: Vernetzung über mehrere Produktionsbereiche/Firmen hinweg (Manufacturing Execution System (MES), Prozessleitsystem (PLS), Field Device Integration (FDI), Process Analytical Technology (PAT), Soft-SPS (Speicherprogrammierbare Steuerung in Software, kurz SSPS))



Quelle: Software AG

usw. vernetzt werden – teilweise adhoc bei Bedarf, teilweise für kurze Zeiten während eines Auftrags, teilweise längerfristig.

Um einem Auftraggeber zu erlauben, dass die produzierten Produkte dynamisch den aktuellen Anforderungen entsprechen, ist eine Vernetzung des Manufacturing Execution Systems (MES) des Auftraggebers mit dem MES in dem Produktionsstandort erforderlich. Dieser ist wiederum mit einem oder mehreren Prozessleitsystemen (PLS) am Produktionsstandort vernetzt, die wiederum mit weiteren Systemen im Produktionsnetz kommunizieren müssen. In Abbildung 4–2 ist eine einfache Darstellung einer solchen Vernetzung zu sehen.

Bei einer Vielzahl an Auftraggebern und mit der Anforderung, dass natürlich jeder Auftraggeber nur genau die Systeme erreichen darf und nur für genau die Zwecke, die für ihn erlaubt sind, wird leicht ersichtlich, dass die Komplexität des Systems schnell ein Ausmaß annimmt, welches mit heutigen, relativ statischen und hierarchisch strukturierten Schutzsystemen, nur schwer zu bewältigen ist.

Herausforderungen

Damit die oben beschriebenen Security-Zellen weiterhin funktionieren, aber die Netzwerke zudem den dynamischen Anforderungen der I4.0-Szenarien gerecht werden, bedarf es neuer Sicherheitssysteme. Es ist nicht davon auszugehen, dass eine dynamische Konfiguration über große Netzwerke mit ausreichender Zuverlässigkeit realisierbar sein wird, also gibt es einen Bedarf an neuen Schutzmechanismen, die direkt in den Automatisierungssystemen enthalten sind. Der „Defense in Depth“-Ansatz wird in sehr komplexen Systemen nicht mehr den notwendigen Schutz bieten können, und somit ergeben sich neue Sicherheitsanforderungen im Rahmen von I4.0, die gezielt in die Automatisierungssysteme eingebaut werden müssen.

4.1.4 Fallbeispiel grenzüberschreitende Logistik-Prozesse

Das folgende Fallbeispiel umfasst grenzüberschreitende Logistik-Prozesse in der Verpackungsindustrie.

4.1.4.1 Kurzbeschreibung

In der Verpackungsindustrie (hier konkret: Wellpappenherstellung und -verarbeitung) herrscht ein extrem hoher Kostendruck, der dazu führt, dass Produktion und Logistik in hohem Maße durchautomatisiert sind.

Diese Querschnittsindustrie nimmt für Unternehmen von der Lebensmittelindustrie bis zum Maschinenbau eine wichtige Rolle bei der Optimierung von deren Logistikprozessen ein.

4.1.4.2 Ausführliche Beschreibung

WITRON, ein Spezialist und Weltmarktführer für hochdynamische Logistik Systeme bietet hierfür unter dem Namen CPMS (Corrugated Packaging Management System) eine umfassende IT-Lösung an. Diese Lösung bildet die gesamte Wertschöpfungskette in einem „360°-View“ (Logistik, Produktion, Vertrieb) ab.

Die einzelnen Komponenten aus Logistik (Lagerhaltung, Lagerauffüllung, Transport, drahtloses Tracking), den verschiedenen Stufen des Planungs-, Herstellungs- Vertriebsprozesses (u. a. Forecast, Einkauf, Zeiten für Rüsten und Produktion, Geschwindigkeiten, Gut-Stückzahl, Abfall), müssen dabei unter den Beteiligten flexibel und minutiös aufeinander abgestimmt werden. Bereits in der Kalkulation muss auch eine Optimierung hinsichtlich der Fertigungswege erfolgen, da die Produktionsanlagen unterschiedliche Aufträge parallel ausführen können, dabei aber auf bestimmte Randbedingungen geachtet werden muss (z. B. notwendige Druckfarben für das Verpackungsmaterial).

Dies geschieht auf Grund des hohen Automatisierungsgrades in der Branche zum großen Teil autonom durch die untereinander vernetzten Systeme anhand der Analyse der von den beteiligten Komponenten gelieferten Daten.

Unternehmensintern verfügt der Hersteller dabei oft über viele über unterschiedliche Länder verteilte Standorte. Extern sind neben den Kunden auch Zulieferer, Transportbörsen (Fourth-Party-Logistics, 4PL), und gegebenenfalls die Telematiksysteme von Spediteuren in die IT-Prozesse eingebunden.

Zulieferer und Dienstleister können bei Bedarf auf Zeit in das System integriert werden, wozu dann ad-hoc Partnernetzwerke mit diesen eingerichtet werden.

Die erforderliche IT-Infrastruktur für dieses Logistik-System kann durch einen externen Dienstleister zur Verfügung gestellt werden oder komplett in der Hoheit des Produzenten liegen.

4.1.4.3 Datenflüsse

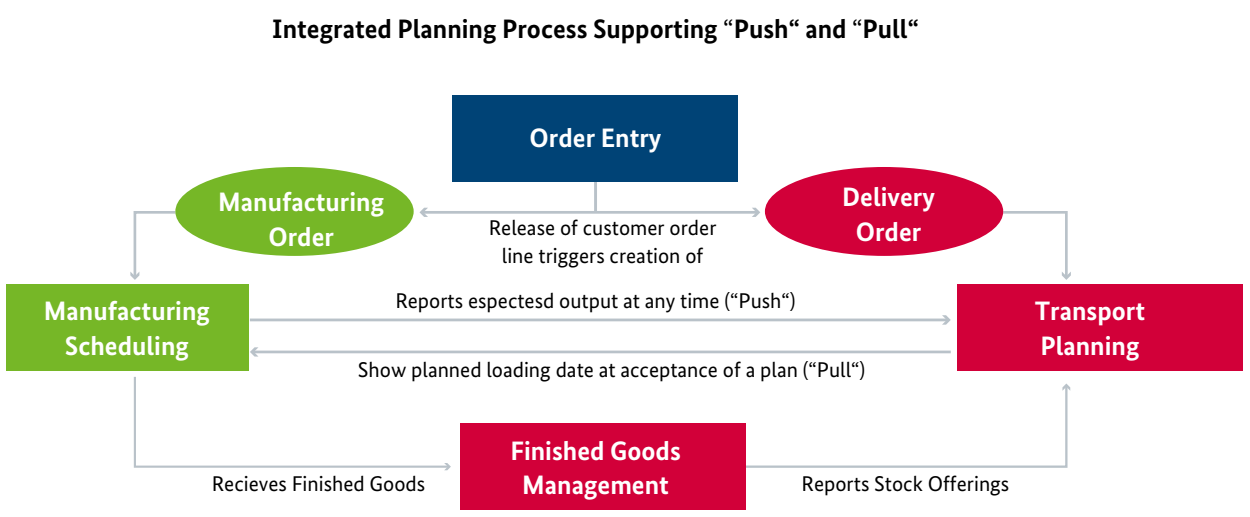
Die Abbildung 4–3 zeigt eine Übersicht des Datenflusses in CPMS.

4.1.4.4 IT-Sicherheit

Bei den hierbei zwischen Unternehmen (auch grenzüberschreitend) ausgetauschten Daten

- lassen sich bei Verletzung der Vertraulichkeit sensitive Informationen z. B. über die geschäftliche Situation der Kunden (Auslastung), Kostenstrukturen, geplante Marketing-Kampagnen oder wiederum deren Kunden gewinnen,
- kann bei Verletzung der Datenintegrität ein hoher Schaden beim Hersteller oder beim Kunden z. B. durch verfälschte Stückzahlen oder verfälschtes Timing (Folgen wären z. B. Blockierungen des Produktionsprozesses durch leere Verpackungsmateriallager bzw. Vergeudung von Ressourcen durch Überproduktion), irreführende Auszeichnung beim Bedrucken der Verpackungen oder unnötige Transportkosten entstehen.

Abbildung 4–3: Übersicht Datenfluss in CPMS



Quelle: WITRON Logistik + Informatik GmbH, 2014

4.2 Referenzmodell

Nach der Betrachtung konkreter Fallbeispiele im vorherigen Abschnitt werden diese nun im Hinblick auf ihre Teilnehmer und deren Beziehungen zueinander (innere und äußere Systemgrenzen, Kommunikationsprozesse und Datenflüsse) untersucht. Diese Erkenntnisse werden herangezogen, um ein möglichst allgemeingültiges Referenzmodell für I4.0-Szenarien zu formulieren, welches ermöglicht, allgemeine IT-Sicherheitsimplikationen, sowie konkrete Bedrohungs- und Risikoeinschätzungen abzuleiten.

Ein solches umfassendes Referenzmodell von IT-Sicherheitsszenarien von I4.0-Systemen setzt sich aus einem Teilnehmer- und Kommunikationsmodell sowie einem passenden Bedrohungs- und Risikomodell zusammen. Ziel ist es, relevante I4.0-Szenarien auf das erstellte Modell abbilden zu können, um diese bezüglich existierender Bedrohungen und Risiken zu untersuchen. Das Modell soll sowohl dazu geeignet sein, konkrete Fallbeispiele (wie z. B. in Kapitel 4.1 dargestellt) als auch abstraktere Szenarien (wie beispielsweise die im Abschlussbericht des Arbeitskreises Industrie 4.0 genannten Szenarien[138] der vernetzten Produktion, des intelligenten Instandhaltungsmanagements und weitere Szenarien) zu evaluieren.

4.2.1 Teilnehmer- und Kommunikationsmodell

Im Folgenden wird das Teilnehmer- und Kommunikationsmodell beschrieben. Dieses Modell stellt eine Abstraktion aus den Fallbeispielen dar. Auf Referenzarchitekturen, z. B. das Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0) (VDI/VDE GMA und ZVEI)[139] und IIRA (IIC), wird dabei kein Bezug genommen, da diese erst spät während der Erstellung dieser Studie veröffentlicht wurden und die Sicherheitsarchitekturen dazu noch in Arbeit sind, so dass sie nicht als Grundlage für die Analyse in dieser Studie einbezogen werden konnten. Zudem wird es nach Ansicht maßgeblicher Experten (z. B. Richard Soley, Executive Director des IIC[140]) auch bei I4.0 stets mehrere Referenzarchitekturen geben. Es handelt sich bei dem in dieser Studie benutzten Teilnehmer- und Kommunikationsmodell daher um eine speziell für diese Studie entwickelte Hilfskons-

138 Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0 - Abschlussbericht des Arbeitskreises Industrie 4.0, Seite 107f, http://www.plattform-i40.de/sites/default/files/Abschlussbericht_Industrie4%200_barrierefrei.pdf, zuletzt abgerufen am 16.07.2015.
139 Statusreport Referenzarchitekturmodell Industrie 4.0 (RAMI4.0), VDI/VDE GMA und ZVEI, April 2015.
140 http://www.produktion.de/aktuell/top-story/iic-chef-soley-rami-4-0-ist-unzulaenglich/

truktion, um eine höhere Abstraktionsebene zur Analyse der in den Fallbeispielen dargestellten Szenarien zu erreichen.

4.2.1.1 Beschreibung des Modells

In den Fallbeispielen wird bereits die Komplexität der Szenarien für eine Beschreibung der IT-Sicherheitsaspekte deutlich. Die Vision von I4.0 erhöht diese Komplexität durch das Hinzutreten von zusätzlichen Teilnehmern und Kommunikationsbeziehungen noch weiter.

Um eine Analyse zu ermöglichen, bei welcher die Herausforderungen, Bedrohungen und Risiken systematisch erfasst werden können, ist es in der Technik eine übliche Herangehensweise, zu versuchen diese Komplexität aufzubrechen und durch Abstraktion in übersichtliche und für sich handhabbare Teile zu zerlegen. Gesucht wird der „kleinste gemeinsame Nenner", in dem alle wesentlichen Eigenschaften der Teilnehmer und der Kommunikationsbeziehungen enthalten sind, so dass sich jede in den Fallbeispielen aufscheinende Kommunikationsbeziehung und jeder Teilnehmer durch Zuordnung von spezifischen Eigenschaften abbilden lässt.

Ein solches generisches Modell beinhaltet im vorliegenden Fall Teilnehmer, Kommunikationsbeziehungen sowie Daten.

Diese drei Komponenten haben jede für sich viele Eigenschaften, durch die sie vollständig beschrieben sind. Für den vorliegenden Zweck einer Betrachtung zur IT-Sicherheit müssen von allen Eigenschaften eines Teilnehmers oder einer Kommunikationsbeziehung jedoch nur diejenigen einbezogen werden, die für die Analyse von IT-Sicherheitsfragen aus technischer, organisatorischer und rechtlicher Sicht erheblich sind.

<u>Teilnehmer</u>

Teilnehmer erhalten eine Information als Input oder Anreiz, verarbeiten diese Information und geben ein Ergebnis weiter. Kommunikationstechnisch gesehen stellt jeder Teilnehmer für sich somit ein Gateway dar.

Auf das Wesentliche reduziert sind seine relevanten Eigenschaften:

- Typ *{Person, Organisation, Maschine}*
- Rolle *{Auftraggeber, Auftragnehmer}*
- Berechtigungen
  - *{Zugriffsberechtigungen {Identifikation von Datenspeichern und Netzzugängen},*
  - *Dateninhalte {lesen, verändern, löschen, weitergeben},*
  - *nicht relevant}*

Der Typ des Teilnehmers ist für die rechtlichen Betrachtungen von Bedeutung, da z. B. autonom entscheidende Maschinen für die Folgen dieser Entscheidungen nicht in Haftung genommen werden können. Für die technischen und organisatorischen Betrachtungen ist sie bei der Wahl der Mittel wesentlich, die zur Erhöhung der IT-Sicherheit angewendet werden können. Bei Personen und Organisationen werden dies organisatorische Prozeduren (IT-Sicherheitsmanagement, Schulung) – unterstützt durch technische Mittel – sein, bei Maschinen liegt der Schwerpunkt naturgemäß auf technischen Vorkehrungen.

Die Rolle des Teilnehmers ist für die Betrachtung von bestimmten, einzelnen Vorgängen innerhalb eines Gesamtszenarios relevant. Grundsätzlich kann in I4.0-Szenarien jeder Teilnehmer sowohl als Auftraggeber als auch als Auftragnehmer auftreten.

Ein weiteres Merkmal eines Teilnehmers sind seine Zugriffsberechtigungen auf Systeme und Datenspeicher eines Kommunikationspartners, sowie die Regeln (engl. „Policies"), die für den Umgang mit von einem anderen Teilnehmer erhaltenen Daten einzuhalten sind.

<u>Kommunikationsbeziehungen</u>

Kommunikationsbeziehungen entstehen dadurch, dass sich zwei oder mehr Teilnehmer miteinander mittels Kommunikationstechnologien (z. B. über TCP/IP) vernetzen.

In den Fallbeispielen hat sich gezeigt, welche Vielfalt von Kommunikationsbeziehungen auftreten kann:

- Beziehungen zwischen unterschiedlichen Sicherheitszonen innerhalb einer Organisation
- direkte Beziehungen zwischen unterschiedlichen Organisationen, die entweder permanent bestehen oder nur bei Bedarf zeitweise aufgebaut werden

- indirekte Beziehungen zwischen unterschiedlichen Organisationen, die über („via“) einen anderen Teilnehmer entstehen können oder durch die gemeinsame Nutzung von zentralen Ressourcen durch unterschiedliche Teilnehmer. Diese Teilnehmer wiederum können untereinander alle gegenseitig bekannt sein oder aber durch eine von einem der Teilnehmer vorgenommene dynamische Auswahl in die Kommunikation einbezogen werden, ohne dass diese den anderen Teilnehmern von vorneherein bekannt sind oder sogar ohne dass diese den anderen Teilnehmern jemals bekannt werden.

- Beziehungen innerhalb derselben Organisation, aber unter unterschiedlichen rechtlichen Rahmenbedingungen (Standorte in unterschiedlichen Rechtsräumen)

- Beziehungen zwischen unterschiedlichen Organisationen unter unterschiedlichen rechtlichen Rahmenbedingungen.

Somit ergeben sich für eine Kommunikationsbeziehung folgende relevante Eigenschaften:

- Art der Vernetzung {permanent, ad hoc {vorhersehbar, unvorhersehbar}}

- Teilnehmerbeziehung

  - *{technisch {sicherheitszonenintern, sicherheitszonenüberschreitend}*
  - *organisatorisch {organisationsintern, organisationsüberschreitend}*
    {– Vertrauensbeziehung {vertraglich definiert, nur durch den allgemeinen Rechtsrahmen}}
  - *rechtlich {jurisdiktionsintern, jurisdiktionsüberschreitend}}*

- Identifizierbarkeit der Kommunikationspartner *{Authentifizierung sicher {einseitig, gegenseitig}, unsicher}*

- Verschlüsselung *{Ende zu Ende, abschnittsweise, keine}*

- Vertrauensstatus

Die Art der Vernetzung kann

- eine ständige Verbindung sein

- eine temporäre Verbindung sein

  - als Verbindung, die nur bei Bedarf hergestellt wird, wobei die Teilnehmer fix vordefiniert sind
  - als Verbindung, die nur bei Bedarf hergestellt wird, wobei die Teilnehmer ad hoc festgelegt werden

Unter einer Sicherheitszone wird ein Netzsegment verstanden an dessen Grenzen alle Datenflüsse durch eine IT-Sicherheitseinrichtung (Firewall, Datendioden etc.) kontrolliert werden.

Bei organisationsüberschreitender Kommunikation ist die Herstellung einer Vertrauensbeziehung erforderlich. Diese wird in der Regel durch entsprechende Verträge zwischen den beteiligten Organisationen gewährleistet, die auch die verpflichtende Zertifizierungen der Partner (z. B. nach ISO 27001) beinhalten können. Hier ist zu berücksichtigen, dass die bisher übliche Zertifizierungen gerade für KMU problematisch sind, da sie mit dem Aufwand für die Realisierung und Aufrechterhaltung von organisatorischen Prozessen, die für eine erfolgreiche Zertifizierung erforderlich sind, überfordert sind. In einfachen Fällen kann auch der allgemeine Rechtsrahmen mit seinen Haftungsregelungen hinreichend sein (vgl. Abschnitt 4.4.3).

Für die rechtliche Teilnehmerbeziehung ist im Falle grenzüberschreitender Kommunikation relevant, ob nur nationales Recht eines Landes, internationales Recht, oder auch nationales Recht beider Länder angewendet werden muss.

Die beiden letzten Eigenschaften, Authentifizierung und Verschlüsselung, sind spezifisch für eine IT-Sicherheitsbetrachtung relevant.

Eine Authentifizierung, mit der die Teilnehmer verlässlich identifiziert werden können, ist für sichere Kommunikation unerlässlich, sobald die lokale Sicherheitszone überschritten wird, in der diese Identität implizit als zutreffend angenommen werden kann.

Verschlüsselung schließlich sichert zunächst die Vertraulichkeit und in Kombination mit kryptographischen Hash-Funktionen auch die Integrität der Inhalte, die bei der Kommunikationsbeziehung übermittelt werden. Für die Sicherheitsbetrachtung ist es wichtig, ob eine solche Verschlüsselung Ende zu Ende auf der Anwendungsebene sichergestellt wird, oder – wie häufig der Fall – nur abschnittsweise auf der Transportebene.

Inhalte und Datenflüsse

Die Teilnehmer tauschen über ihre Kommunikationsbeziehungen Daten aus. Für die Analyse eines Szenarios unter IT-Sicherheitsaspekten muss für die dabei übergebenen Daten definiert und geregelt sein:

- welche Daten personendatenschutzrelevant oder für den Sender geschäftsdatensicherheitsrelevant sind und daher vom Empfänger mit entsprechenden Sicherheitsmaßnahmen zu behandeln sind
- ob und an wen welche Daten vom Empfänger an Dritte weitergegeben werden dürfen oder müssen
- welche Daten gelesen, modifiziert oder gelöscht werden dürfen
- ob die Daten beim Empfänger gespeichert werden dürfen und wann sie gelöscht werden müssen
- wie die Daten gespeichert werden (verschlüsselt oder unverschlüsselt)

Im Modell übermittelt ein Auftraggeber Daten an einen Auftragnehmer. Der Auftragnehmer führt aufgrund dieser Daten einen Auftrag aus.

Der Auftragnehmer liefert entweder ein Ergebnis direkt an den Auftraggeber zurück, z. B. ein Protokoll oder ein Produkt und möglicherweise auch produktbegleitende Daten (Qualitätssicherungsnachweise, Produktbeschreibungen etc.). Oder aber der Auftragnehmer wird seinerseits zum Auftraggeber und übermittelt das Ergebnis seinerseits an einen Unterauftragnehmer weiter. Die vom ursprünglichen Auftraggeber erhaltenen Daten können dabei verändert oder unverändert Bestandteil der an den Unterauftragnehmer übermittelten Daten sein.

Für die IT-Sicherheitsbetrachtung wesentlich ist hierbei die Art der Übermittlung der Daten. Diese können zwischen Auftraggeber und Auftragnehmer direkt übermittelt werden (Peer-to-Peer), sie können auf einem Datenspeicher liegen, auf den beide Partner Zugriff haben, oder sie können – dies ist bei „Smart Products“ eines der Konzepte[141] von I4.0 – auf einem physikalischen Produkt selbst gespeichert sein, z. B. auf einem RFID-Transponder.

4.2.1.2 Instanziierungsbeispiel

Im Folgenden wird anhand des Fallbeispiels Fernwartung exemplarisch dargestellt, wie ein konkreter Fall im Modell abgebildet wird

Das Objekt der Fernwartung wird als Maschine M bezeichnet. Die virtuelle Maschine mit den Wartungswerkzeugen, von der aus auf die Maschine M zugegriffen wird als VM bezeichnet.

Auf der obersten organisatorischen Ebene bezeichnen wir die Teilnehmer folgendermaßen:

- Firma A: Hersteller der Maschine M
- Firma B: Betreiber (oder Anwender) der Maschine M

Optional können im Szenario noch eine Rolle spielen:

- Firma C: ein Zulieferer der Firma A (einer Komponente für die Maschine M)
- Firma D: ein Kunde der Firma B, falls es sich z. B. bei B um einen Systemhersteller von Produktionsanlagen handelt, der die Maschine M seinen Anlagen verbaut hat.

Fernwartung findet durch Teilnehmer in folgenden Ausprägungen statt:

1. Der Service-Techniker T(A) der Firma A, der über Fernwartung auf die Maschine bei der Firma B zugreift,
2. Der Techniker T(B1) der Firma B, der für die Instandhaltung der Maschine bei der Firma B zuständig ist,
3. Der Techniker T(B2) der Firma B, der die Maschine M als Teil einer Anlage der Firma B bei der Firma D wartet,
4. Der Service-Techniker T(C) der Firma C, der vom Service-Techniker der Firma A in einem Support-Fall bei der Wartung einer Maschine der Firma B hinzugezogen wird,
5. Die Maschine M, die für den Zweck der vorbeugenden Wartung Daten an die Firma A liefert.

141 Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0 – Abschlussbericht des Arbeitskreises Industrie 4.0, Seite 25, http://www.plattform-i40.de/sites/default/files/Abschlussbericht_Industrie4%200_barrierefrei.pdf, zuletzt abgerufen am 16.07.2015.

Jeder der Teilnehmer 1-4 kann von seinem Typ her als eine Person, eine Organisation oder eine Maschine auftreten (letzteres ist heute eher eine I4.0-Vision), Teilnehmer 5 ist immer eine Maschine.

Die jeweiligen Eigenschaften der Teilnehmer und der Kommunikationsbeziehungen sind für jede dieser fünf Ausprägungen in den nachfolgenden Tabellen[142] dargestellt:

Ausprägung 1:

Tabelle 4–1: Eigenschaften der Teilnehmer im Fernwartungsszenario (1)

Teilnehmer	Typ	Rolle	Berechtigungen (Beispiele!)
Firma A	Organisation	Auftragnehmer	nicht relevant
Firma B	Organisation	Auftraggeber	nicht relevant
T(A)	Person Maschine (I4.0)	Auftragnehmer	VPN-Verbindung anfordern Zugriff auf die VM
T(B1)	Person	Auftraggeber	Wartung anfordern
M	Maschine	–	VPN-Verbindung aufbauen
VM (in der DMZ bei Firma A)	Maschine	–	Zugriff auf das maschinen-interne Netz Zugriff auf Konfigurationsdaten Zugriff auf Basis-SW Zugriff auf Log-Dateien

Tabelle 4–2: Eigenschaften der Kommunikationsbeziehungen im Fernwartungsszenario (1)

Verbindung	Eigenschaften
M <-> VM	ad hoc, vorhersehbar sicherheitszonenüberschreitend organisationsüberschreitend jurisdiktionsintern oder jurisdiktionsüberschreitend Authentifizierung sicher Ende-zu-Ende-verschlüsselt
T(A) <-> VM	ad hoc, vorhersehbar sicherheitszonenüberschreitend organisationsintern jurisdiktionsintern Authentifizierung sicher Ende-zu-Ende-verschlüsselt

142 Verwendete Abkürzungen sind im Abkürzungsverzeichnis erläutert.

Ausprägung 2:

Tabelle 4–3: Eigenschaften der Teilnehmer im Fernwartungsszenario (2)

Teilnehmer	Typ	Rolle	Berechtigungen (Beispiele!)
Firma B	Organisation	Auftraggeber	nicht relevant
T(B1)	Person Organisation Maschine (I4.0)	Auftragnehmer	VPN-Verbindung anfordern Zugriff auf das maschinen-interne Netz Voller Zugriff auf alle Maschinendaten
M	Maschine	Auftraggeber	VPN-Verbindung aufbauen

Tabelle 4–4: Eigenschaften der Kommunikationsbeziehungen im Fernwartungsszenario (1)

Verbindung	Eigenschaften
T(B1) <-> M	ad hoc, vorhersehbar sicherheitszonenüberschreitend organisationsintern jurisdiktionsintern Authentifizierung sicher Ende-zu-Ende-verschlüsselt

Ausprägung 3:

Tabelle 4–5: Eigenschaften der Teilnehmer im Fernwartungsszenario (1)

Teilnehmer	Typ	Rolle	Berechtigungen (Beispiele!)
Firma B	Organisation	Auftragnehmer	nicht relevant
Firma D	Organisation	Auftraggeber	nicht relevant
T(B2)	Person Maschine (I4.0)	Auftragnehmer	VPN-Verbindung anfordern Zugriff auf die VM
T(D)	Person	Auftraggeber	Wartung anfordern
M	Maschine	–	VPN-Verbindung aufbauen
VM (in der DMZ bei Firma B)	Maschine	–	Zugriff auf das maschinen-interne Netz Zugriff auf Konfigurationsdaten Zugriff auf Anwender-SW Zugriff auf Log-Dateien

Tabelle 4–6: Eigenschaften der Kommunikationsbeziehungen im Fernwartungsszenario (4)

Verbindung	Eigenschaften
M <-> VM	ad hoc, vorhersehbar sicherheitszonenüberschreitend organisationsüberschreitend jurisdiktionsintern oder jurisdiktionsüberschreitend Authentifizierung sicher Ende-zu-Ende-verschlüsselt
T(B2) <-> VM	ad hoc, vorhersehbar sicherheitszonenüberschreitend organisationsintern jurisdiktionsintern Authentifizierung sicher Ende-zu-Ende-verschlüsselt

Ausprägung 4:

Tabelle 4–7: Eigenschaften der Teilnehmern im Fernwartungsszenario (4)

Teilnehmer	Typ	Rolle	Berechtigungen (Beispiele!)
Firma A	Organisation	Auftragnehmer (der Firma B)	nicht relevant
Firma B	Organisation	Auftraggeber	nicht relevant
Firma C	Organisation	Auftragnehmer (der Firma A)	nicht relevant
T(A)	Person Maschine (I4.0)	Auftragnehmer	Zugriff auf das maschinen-interne Netz Zugriff auf Konfigurationsdaten Zugriff auf Basis-SW Zugriff auf Log-Dateien
T(C)	Person Maschine (I4.0)	Auftragnehmer	VPN-Verbindung zu Firma A Zugriff auf die VM bei Firma A
M	Maschine	–	VPN-Verbindung aufbauen
VM (in der DMZ bei Firma A)	Maschine	–	Zugriff auf das maschinen-interne Netz Zugriff auf Konfigurationsdaten Zugriff auf Basis-SW Zugriff auf Log-Dateien

Tabelle 4–8: Eigenschaften der Kommunikationsbeziehungen im Fernwartungsszenario (4)

Verbindung	Eigenschaften
M <-> VM	ad hoc, vorhersehbar sicherheitszonenüberschreitend organisationsüberschreitend jurisdiktionsintern oder jurisdiktionsüberschreitend Authentifizierung sicher Ende-zu-Ende-verschlüsselt
T(A) <-> VM	ad hoc, vorhersehbar sicherheitszonenüberschreitend organisationsintern jurisdiktionsintern Authentifizierung sicher Ende-zu-Ende- verschlüsselt
T(C) <-> VM	ad hoc, vorhersehbar sicherheitszonenüberschreitend organisationsüberschreitend jurisdiktionsintern oder - überschreitend Authentifizierung sicher Ende-zu-Ende-verschlüsselt

Ausprägung 5:

Tabelle 4–9: Eigenschaften der Teilnehmern im Fernwartungsszenario (5)

Teilnehmer	Typ	Rolle	Berechtigungen (Beispiele!)
Firma A	Organisation	Auftragnehmer	nicht relevant
Firma B	Organisation	Auftraggeber	nicht relevant
M	Maschine	–	VPN-Verbindung aufbauen Zustandsdaten
S	Maschine	–	

Tabelle 4–10: Eigenschaften der Kommunikationsbeziehungen im Fernwartungsszenario (5)

Verbindung	Eigenschaften
M <-> S	ad hoc, vorhersehbar sicherheitszonenüberschreitend organisationsüberschreitend jurisdiktionsintern oder jurisdiktionsüberschreitend Authentifizierung sicher Ende-zu-Ende-verschlüsselt

4.2.2 Bedrohungs- und Risikomodell

In diesem Abschnitt wird das Teilnehmer- und Kommunikationsmodell durch ein Bedrohungs- und Risikomodell ergänzt, mittels dem Bedrohungen und Risiken hinsichtlich der Schutzziele Integrität, Vertraulichkeit, Verfügbarkeit, Authentifizierung und Autorisierung identifiziert und bewertet werden können. Dabei wird zur Analyse, Identifikation und Bewertung von Risiken und neuen Herausforderungen ein Ansatz verfolgt, der sowohl Menschen als auch Prozesse und allen Schichten der IT-Infrastruktur von industriellen Produktionsumgebungen berücksichtigt.

Während das Bedrohungsmodell u.a. Aspekte wie die Gruppe der potentiellen Angreifer (Mitarbeiter, Wettbewerber, Staaten etc.), deren mögliche Angriffsvektoren, sowie schützenswerte Assets erfasst, wird mit dem Risikomodell eine Möglichkeit geschaffen, auf Basis konkreter Parameter eines Szenarios (z.B. Exponiertheit einer Produktionsanlage, Gefahr für Leib- und Leben, rechtliche Rahmenbedingungen aus denen finanzielle Verpflichtungen erwachsen könnten, etc.) ein Gesamtrisiko abzuschätzen.

Die besonderen Eigenschaften industrieller Anlagen erfordern dabei ein Vorgehen, das über eine reine Bedrohungs- und Risikoanalyse hinausgeht und eher als stetig aktualisierte IT-Sicherheitsdokumentation bezeichnet werden kann. Der Hauptgrund hierfür ist der Lebenszyklus industrieller Anlagen, der sich über mehrere Jahrzehnte erstrecken kann. Bedrohungen und Verwundbarkeiten, die in der Planungsphase einer industriellen Anlage erfasst werden, können daher niemals eine finale Bedrohungsanalyse der Anlage darstellen. Es ist vielmehr erforderlich, Entscheidungen von Anlagenbauern, Entwicklern und anderen involvierten Gruppen über den gesamten Lebenszyklus einer Anlage zu dokumentieren. Es ist nicht auszuschließen, dass Personal, welches in der Planungsphase einer Anlage involviert war, Jahre später für eine Erweiterung oder Aktualisierung nicht mehr zur Verfügung steht. In solchen Fällen ist es dann hinsichtlich der Sicherheitseigenschaften einer Anlage von essentieller Wichtigkeit, auch Designentscheidungen nachvollziehen zu können, die während des Lebenszyklus der Anlage getroffen wurden.

Im Folgenden werden die Schritte des Verfahrens zur Bedrohungs- und Risikomodellierung vorgestellt.

4.2.2.1 Beschreiben der Systemarchitektur

Der Zweck dieses ersten Schritts besteht darin, einen Überblick über das zu untersuchende Gesamtsystem zu erhalten. Zudem werden auch die Systemgrenzen definiert, innerhalb derer eine Bedrohungsmodellierung stattfinden soll. So geht bspw. durch Einschränkung der Auswahl auf bestimmte Komponenten und deren Konfiguration auch eine Beschränkung der modellierten Granularität einher. Idealerweise können viele Informationen zur Bearbeitung der nachfolgenden Schritte aus dem bereits im vorigen Kapitel erstellten Teilnehmer- und Kommunikationsmodell herausgelesen werden. Folgende ergänzende Informationen sollten darüber hinaus ebenfalls erfasst sein:

- Falls vorhanden, Name und Planungsstand (Version) des zu untersuchenden Systems.
- Was ist der Anwendungszweck für das System? In welcher Domäne soll es zum Einsatz kommen?
- Was ist der Nutzen des Systems in der jeweiligen Domäne? Für welche Zwecke wurde das System ggf. explizit nicht entworfen?
- Kurze Zusammenfassung der Architektur, bestehend aus einer Auflistung der wesentlichen Komponenten, ggf. Paradigmen, verwendeten Technologien und anderen High-Level-Aspekten abstrakter Art.
- Mindestens ein Datenflussdiagramm (High-Level), das die Datenflüsse innerhalb des Systems darstellt.

Das Erstellen eines Datenflussdiagramms ist der übliche Weg, um die statische Struktur eines Systems mitsamt seinen Komponenten, Schnittstellen zwischen diesen sowie externe Schnittstellen zu beschreiben. Datenflussdiagramme (siehe Abbildung 4–4) bestehen aus den folgenden Elementen:

- **Prozesse** repräsentieren Aufgaben in einem System, die Daten verarbeiten oder Aktionen auf Basis dieser Daten ausführen. Im Rahmen dieser Studie werden insbesondere auch kombinierte Hardware- und Software-Komponenten wie z.B. MES, PLS oder SPS als Prozesse modelliert.
- **Datenspeicher** können beispielsweise Dateien oder Datenbanken innerhalb eines Systems sein, welche die dort gespeicherten Daten mit Prozessen austauschen.

- **Externe Akteure** sind Entitäten außerhalb des modellierten Systems, die damit interagieren. Solche externen Entitäten senden Daten an einen oder mehrere Prozesse oder empfangen Daten von Prozessen. So werden beispielsweise auch Anwender als externe Entitäten modelliert, die typischerweise mit einem Client- oder Graphical User Interface (GUI)-Prozess interagieren.

- **Datenflüsse** repräsentieren die gerichtete Übertragung von Daten zwischen Prozessen, externe Entitäten und Datenspeichern.

Ein weiterer wichtiger Bestandteil bei der Beschreibung der Systemarchitektur ist das Anlegen einer Inventarliste von Komponenten. Um als Basis für spätere Arbeitsschritte zu dienen, sollte diese Liste alle relevanten datenverarbeitenden Komponenten eines Systems auflisten. Diese können sicherlich zum Teil schon aus dem zuvor erwähnten Datenflussdiagramm entnommen werden, sollten aber im Hinblick auf eine möglichst vollständige Erfassung auch um alle physisch abgrenzbaren und begrifflich unterscheidbaren Software-Komponenten ergänzt werden. Beispiele sind etwa: Maschinen, Steuerungen, Komponenten, Rechner, Datenbanken, Softwaresysteme, sowie weitere Ressourcen, die ein System benötigt.

4.2.2.2 Sammeln bereits bekannter Sicherheitsvorfälle

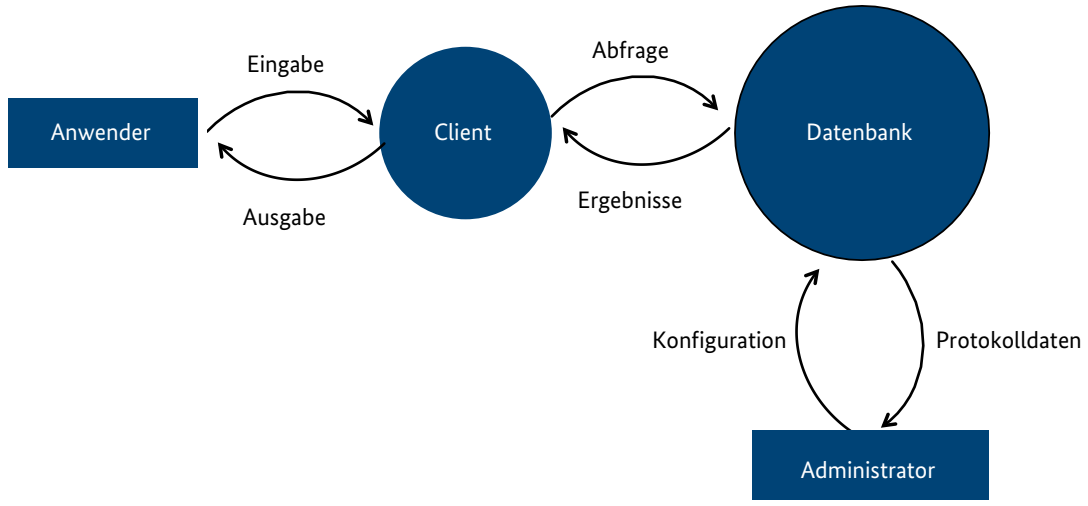
Nach der Erstellung eines Gesamtüberblicks im vorigen Abschnitt sollen nun alle bekannten Sicherheitsvorfälle erfasst werden, die schon aus der Vergangenheit von Vorgängersystemen oder anderen ähnlichen Systemen bekannt sind. Dieses Erfahrungswissen sollte unbedingt bei der Planung neuer Systeme einfließen, nicht zuletzt um auch einen besseren Blick für die Sicherheitsprobleme im jeweiligen Kontext zu entwickeln. Die Erfassung einer solchen Historie von Sicherheitsvorfällen kann in Listenform geschehen, wobei jeweils eine kurze Bewertung des Vorfalls vorgenommen werden sollte. Eine solche Referenzliste kann neben allgemeinen Sicherheitsvorfällen auch konkrete Schwächen oder Verwundbarkeiten des Systems enthalten. Die folgenden Fragen können bei der Erstellung einer solchen Liste hilfreich sein:

- Gibt es allgemein oder auch nur intern bekannte Sicherheits-Verwundbarkeiten?

- Gibt es in der Historie von Sicherheitsvorfällen Besonderheiten, wie bspw. wiederkehrende Verwundbarkeiten oder Schwächen?

- Sind alle relevanten Dokumentationen up-to-date und vollständig?

Abbildung 4–4: Beispiel eines Datenflussdiagramms



Quelle: Fraunhofer SIT

- Gibt es evtl. dokumentierte Vorfälle oder sonstige Notizen, die ggf. weiteren Handlungsbedarf erfordern, wie z. B. besondere Erfordernisse für bestimmte Komponenten bei deren Konfiguration oder Einbringung ins Feld?

Diese Liste sollte möglichst immer aktuell gehalten werden, d. h. bei Veränderungen am System oder bei Bekanntwerden neuer Sicherheitsvorfälle sollten diese Liste entsprechend ergänzt werden.

4.2.2.3 Erstellen von Sicherheitsprofilen

Dieser Schritt adressiert explizit erforderliche Sicherheitsmaßnahmen für einzelne Komponenten, die bei der Planung/Bewertung eines Systems berücksichtigt werden sollten. Auch dieser Schritt kann dabei behilflich sein, einen besseren Blick für die Sicherheitsprobleme im jeweiligen Kontext zu entwickeln. Dazu muss für jede Komponente bestimmt werden, ob diese ohne besondere Berücksichtigung von Sicherheitsanforderungen in das Gesamtsystem integriert werden kann, oder ob dafür erst besondere Maßnahmen/Lösungen implementiert werden müssen. Möglicherweise stellt sich eine bestimmte Komponente unter den gegebenen Sicherheitsanforderungen für das Gesamtsystem auch als überhaupt nicht geeignet oder einsetzbar heraus. Des Weiteren sollten auch andere Systeme betrachtet werden, in denen gleiche Komponenten verwendet werden, und deshalb auch gemeinsame oder vergleichbare Schwachstellen und Verwundbarkeiten aufweisen können.

Zunächst ist eine Liste aller Komponenten notwendig. Dann müssen für jede Komponente individuell organisatorische Maßnahmen, Umgang mit Sicherheitsvorfällen, Erfordernisse bei der Einrichtung und verfügbare Sicherheitsdokumentation bewertet werden. Dazu können folgende Fragen hilfreich sein:

- Organisatorische Maßnahmen:
  - Gibt es Informationen des Herstellers bzgl. der Sicherheit von Komponenten?
  - Gibt es Informationen vom Hersteller bzgl. bekannter Schwachstellen und Verwundbarkeiten?
  - Gibt es Ansprechpartner und ggf. definierte Prozesse für das Melden von Schwachstellen?
- Umgang mit Sicherheitsvorfällen:
  - Gibt es Einträge in offiziellen Datenbanken für Sicherheitsvorfälle (z. B. CVE[143])?
  - Falls ja, welche Auswirkung hatten diese Einträge (z. B. CVSS-Score[144])?
  - Wurden die Schwachstellen von der Komponente selbst oder von anderen integrierten Komponenten verursacht?
  - Gibt es Besonderheiten, z. B. ständig wiederkehrende Verwundbarkeiten oder ähnliche Schwachstellentypen?
  - Wieviel Zeit hat der Hersteller zur Reaktion bei einem Sicherheitsvorfall benötigt?
- Erfordernisse bei der Einrichtung:
  - Ist die Standardkonfiguration einer Komponente sicher?
  - Gibt es Standard-Kennwörter oder Standard-Ports?
  - Welche Benutzerrechte sind für den Betrieb einer Software erforderlich und kann diese ggf. in besonders gehärteten Umgebungen eingesetzt werden?
- Sicherheitsdokumentation:
  - Gibt es eine Sicherheitsdokumentation für die Komponente?
  - Falls ja, ist diese aktuell und verständlich?
  - Bezieht sich die Dokumentation nur auf die Software oder bezieht sie auch die jeweilige Umgebung, in der sie eingesetzt wird, mit ein?
  - Wurde die Komponente bereits sicherheitsgeprüft und sind die Ergebnisse dieser Prüfung ggf. öffentlich verfügbar?
  - Falls die Komponente Sicherheitseigenschaften besitzt:
    - Ist auch dessen Sicherheitsarchitektur dokumentiert?
    - Werden die Sicherheitseigenschaften auf Basis von Best Practice und Standards implementiert, wie z. B. anerkannte kryptographische Algorithmen, Durchsetzung (engl. enforcement) von Passwort-Policies etc.?

143 Common Vulnerability Enumeration
144 Common Vulnerability Scoring System

Die Sicherheitsprofile sollten ebenfalls möglichst immer aktuell gehalten werden, d.h. bei Veränderungen am System oder bei Bekanntwerden neuer Sicherheitsvorfälle sollten auch die Profile entsprechend aktualisiert werden.

4.2.2.4 Identifizieren von Asset Stakeholders

Die Bedeutung von Assets ist typischerweise für unterschiedliche Personen oder Unternehmen die mit einem IT-System befasst sind verschieden. Im nächsten Schritt werden deshalb zunächst alle potentiell relevanten Stakeholder identifiziert, die ein Interesse an den Assets eines Systems haben könnten. Das Ergebnis sollte eine Liste von realen Personen, Gruppen, Organisationen oder Unternehmen sein, für die das jeweilige Asset einen Wert darstellt. Alle Stakeholder zeichnen sich dadurch aus, dass sie ein Interesse daran haben, den Wert bestimmter Assets zu erhalten. Dabei kann ein und dasselbe Asset durchaus verschiedene Werte für verschiedene Stakeholder darstellen. Asset Owner besitzen Assets. Ein Asset kann mehrere Asset Owner haben und auch für diese unterschiedliche Werte darstellen. Beim Bestimmen aller Asset Stakeholder sollten auch Personen oder Unternehmen berücksichtigt werden, die nur indirekt Beziehungen zu einem Asset haben.

4.2.2.5 Identifizieren von relevanten Assets

Ein Asset kann alles sein, dass einen Wert darstellt, wie z.B. Objekte oder Daten. Auch abstrakte Werte, wie z.B. die Reputation eines Unternehmens, können Assets sein. In einigen Fällen können auch Personen oder deren Gesundheit relevante Assets sein, wie bspw. bei einem Safety-System. Relevante Assets lassen sich typischerweise einer der folgenden Kategorien zuordnen:

- Informationen, die von einer Komponente verarbeitet werden
- Die Komponente selbst
- Prozesse, die von der Komponente abhängig sind
- Andere System, Komponenten oder externe Daten, die beeinträchtigt werden können
- Nicht-technische Assets, wie Menschenleben, finanzielle Assets, Besitz
- Geistiges Eigentum
- Abstrakte Werte, wie bspw. Reputation
- Übereinstimmung mit Richtlinien

Als Ergebnis dieses Arbeitsschritts sollte eine Liste mit potentiell relevanten Assets und assoziierten Asset Stakeholders aus dem vorigen Schritt sein. Bei dieser Aufgabe kann es nützlich sein, die wichtigsten Stakeholder bei der Identifizierung der Assets selbst miteinzubeziehen. Dabei kann auch gleich die Bestimmung der Schutzziele für jedes Asset im nächsten Schritt vorgenommen werden.

Als Ausgangsbasis kann die Liste der Asset Stakeholder aus dem vorigen Schritt dienen. Für jeden Stakeholder sollte untersucht werden, in welcher Beziehung er zum System steht und welche Abhängigkeiten bestehen. Um relevante Assets zu identifizieren, sind Use-Case-Diagramme und ähnliche Darstellungen nützlich. Zusätzlich sollten auch unterschiedliche Geschäftsszenarien und der geschäftliche Kontext berücksichtigt werden. Für einen Hersteller ist beispielsweise nicht nur die Sicherheit seiner Systeme von Bedeutung, sondern auch das Vertrauen seiner Kunden, das Schaden erleiden könnte, wenn infolge eines IT-Sicherheitsvorfall auch die Qualität der Produkte beeinträchtigt wurde. Für nicht offensichtliche Assets sollte eine kurze Erläuterung oder Kommentar ergänzt werden.

Generell sollte eine zu technische Sichtweise vermieden werden, d.h. eine ausschließliche Betrachtung der konkreten technischen Systeme und spezifischen Bedrohungen. Assets und Schutzziele sollte idealerweise direkt vom eigentlichen Zweck eines Systems und dessen Kontext abgeleitet werden. IT-Systeme und die darin verarbeiteten Daten stellen typischerweise eine Repräsentation realer Prozesse und Informationen dar. Diese realen Assets sind potentiell gefährdet, nicht die Bits und Bytes. Es kann daher hilfreich sein, zu entscheiden, ob es sich um ein reales Asset handelt, dass geschützt werden muss, oder nur um eine Komponente, die in irgendeiner Weise mit einem realen Asset in Verbindung steht. Beispielsweise sollte ein Verschlüsselungs-Schlüssel immer geschützt werden, aber eigentlich gilt der ganze Aufwand dem Schutz der zu verschlüsselnden Information. Deren Vertraulichkeit wird durch eine Vielzahl anderer Gefährdungen bedroht, als dem Schlüsselverlust allein. Beispielsweise könnte deren Herausgabe auch durch Erpressung erzwungen werden. Durch die Fokussierung auf die realen Assets kann ein zu kurzsichtiger technologiezentrierter Blick auf das System vermieden werden.

4.2.2.6 Identifikation der Schutzziele für relevante Assets

Die Schutzziele entsprechen den sicherzustellenden primären Sicherheitseigenschaften eines jeweiligen Assets. Ein klassisches Beispiel für das primäre Schutzziel einer Rezeptur in der Getränkeherstellung wäre zum Beispiel die Vertraulichkeit des Rezepts. Ein weiteres Schutzziel wäre die Integrität.

Der Verwendungszeck einer Industrieanlage steht in aller Regel fest und ändert sich auch im Verlauf der Zeit nur selten oder gar nicht. Für eine konkrete Anlage ist es daher recht einfach, einmalig zu identifizieren, welche Assets relevant sind und welche Schutzziele ihnen zugeordnet werden müssen. Als Grundlage können existierende Policies, Geschäftsmodelle oder externe regulatorische Gegebenheiten (z. B. rechtliche Vorschriften) herangezogen werden.

Als Ergebnis steht eine Liste mit Schutzzielen, die der Eigentümer des jeweiligen Assets für wichtig erachtet. Da generelle Schutzziele mehrdeutig sein können, sollten sie mit einer eindeutigeren Kurzbeschreibung der erwünschten Systemeigenschaft versehen werden.

Die drei wesentlichen Schutzziele, auch bekannt als CIA-Dreieck, sind: Vertraulichkeit, Integrität und Verfügbarkeit.

Die Begriffe haben dabei folgende Bedeutung:

- **Vertraulichkeit** (englisch: confidentiality): Daten dürfen lediglich von autorisierten Benutzern gelesen werden, dies gilt sowohl beim Zugriff auf gespeicherte Daten, wie auch während der Datenübertragung.
- **Integrität** (englisch: integrity): Daten dürfen nicht unautorisiert bzw. unbemerkt verändert werden. Alle Änderungen müssen nachvollziehbar sein.
- **Verfügbarkeit** (englisch: availability): Verhinderung von Systemausfällen; der Zugriff auf Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet sein.

Während oft weitere Schutzziele genannt werden (z. B. Authentizität, Nicht-Abstreitbarkeit), reichen die drei Schutzziele CIA in den meisten Fällen aus, um die notwendigen Sicherheitseigenschaften zu definieren. Dennoch ist es in der Praxis sinnvoll eine präzisere Beschreibung zu formulieren, was im jeweils konkreten Fall unter Vertraulichkeit, Integrität und Verfügbarkeit verstanden wird.

Beispielsweise kann Integrität streng definiert werden, als das Ziel eine unerlaubte Manipulation unter allen Umständen zu verhindern oder aber weniger Strikt als das Ziel, eine solche unerlaubte Manipulation zeitnah erkennen zu können. Für das Schutzziel Vertraulichkeit kann meist klar definiert werden, wem gegenüber die Daten vertraulich zugänglich gemacht werden sollen. Zur Ableitung der erforderlichen Sicherheitseigenschaften ist es demnach ratsam, das CIA-Dreieck als Einstiegshilfe heranzuziehen aber zusätzlich in eigenen Worten zu beschreiben, was im konkreten Fall erreicht werden soll.

Die folgenden Fragen können bei der Auflistung und Beschreibung von Schutzzielen für Assets helfen:

Vertraulichkeit:

- Welchen Rollen sollten die vertraulichen Informationen zugänglich sein, welchen nicht?
- Gibt es Sonderfälle, in denen die Vertraulichkeit aufgehoben werden darf?

Integrität:

- Sind bestimmte unautorisierte Veränderungen an Daten vernachlässigbar (z. B. Löschung, Duplizierung, Veränderung der Reihenfolge, Verzögerung)?
- Ist das Ausmaß an Modifikation relevant (z. B. einzelne Bits, alle Daten die einer bestimmten Rolle zugeordnet sind, ganzer Datensatz)?
- Reicht es unter Umständen aus, die Veränderung erkennen zu können oder muss sie verhindert werden?
- Wenn Integrität ein erforderliches Ziel ist, muss meist auch die Quelle der Daten sichergestellt werden. Damit wird auch das Schutzziel Authentizität erforderlich.

Verfügbarkeit:

- Welches Maß an Nicht-Verfügbarkeit ist kritisch (z. B. langsame Antwortzeit, kurze Unterbrechung, Unterbrechung die nicht automatisiert wieder überwunden werden kann, vollständige Unterbrechung)?

Generell:

- Wo rührt die erforderliche Sicherheitseigenschaft her (z. B. Policy, Service Level Agreement (SLA), rechtliche Rahmenbedingung)?

4.2.2.7 Priorisierung der Assets und Schutzziele

Ein Verstoß gegen die Schutzziele kann verschieden starke Auswirkungen nach sich ziehen. Beispielsweise können die Folgen marginal sein, wenn durch Datendiebstahl die Daten eines einzelnen Kunden offengelegt wurden. Die Kompromittierung und Veröffentlichung des gesamten Kundendatensatzes könnte sich hingegen als katastrophal für das Unternehmensimage herausstellen. Die Folgen bei Nichtverfügbarkeit hängen in der Regel von der Dauer der Unterbrechung ab. Unter Umständen ist eine Verzögerung von wenigen Sekunden für einen Produktionsprozess tolerabel, während eine Verzögerung im selben Ausmaß in einem Energiekraftwerk schwerwiegende Folgen hat usw.

Für jedes Asset und die zugehörigen Schutzziele sollte eine Differenzierung erfolgen, unter welchen Umständen ein Verstoß gegen das Schutzziel als „vernachlässigbar", „marginal", „kritisch" oder „katastrophal" eingeschätzt werden muss. Die Einschätzungen sollten zum Zweck der besseren Nachvollziehbarkeit durch die Anführung der wichtigsten Argumente erläutert werden.

Je konkreter die zugrundeliegenden Informationen bezüglich verbundener Prozesse (Geschäftsprozesse, Produktionsprozesse etc.) und Rahmenbedingungen sind, umso einfacher wird die Priorisierung der Assets und Schutzziele.

Beispiel: Vertraulichkeit von Kundendaten

- Vernachlässigbar: Nie
- Marginal: < fünf Kunden betroffen
- Kritisch: < 20 Kunden betroffen
- Katastrophal: >= 20 Kunden betroffen oder mehrere Sicherheitsvorfälle pro Woche

Beispiel: Verfügbarkeit einer Komponente

- Vernachlässigbar: Unterbrechung < 5 Millisekunden
- Marginal: Unterbrechung < 0,5 Sekunden
- Kritisch: Unterbrechung < 5 Sekunden
- Katastrophal: Unterbrechung > 1 Minute

4.2.2.8 Aufstellung aller relevanten Rollen und zugehöriger Berechtigungen

Für die Durchführung einer Sicherheitsanalyse ist die Unterscheidung zwischen verschiedenen Rollen und ihren jeweiligen Privilegien bzw. Berechtigungen notwendig. Daher sollten die an den Prozessen und Abläufen beteiligten Rollen zunächst in Form einer Liste erfasst werden. Eine Rolle entspricht einer Gruppe von Nutzern in der jeder Nutzer über dieselbe Stufe an Privilegien verfügt. Eine Person kann mehreren Gruppen gleichzeitig angehören. Privilegien können z. B. Rechte sein, auf ein bestimmtes System zugreifen oder bestimmte Prozesse starten und stoppen zu können. Ist die Liste mit Rollen erstellt, können diesen die ihrer Aufgabe entsprechenden Berechtigungen zugewiesen werden.

Für Softwaresysteme muss außerdem die mögliche Rechteausweitung durch Zugehörigkeit einer Person zu mehreren Rollen erfasst werden. Als Ergebnis stehen zwei Listen. Die erste Liste enthält alle Rollen, die mit dem zu modellierenden System interagieren, zusammen mit einer Beschreibung der konkreten Nutzer und zugehörigen Berechtigungen. Die zweite Liste enthält alle möglichen Rechteausweitungen, die in relevanten Softwarekomponenten vorkommen können, also Fälle in denen ein Nutzer durch den einen oder anderen Mechanismus mehr oder weniger Berechtigungen erhält, als ihm über die Summe seiner Rollen eigentlich zugesteht.

Um die beteiligten Rollen zu identifizieren bietet sich die Verwendung von Use-Case-Szenarien an. Die Liste sollte detaillierte Informationen darüber enthalten, welche Eigenschaften die einzelnen Rollen haben und worin sie sich unterscheiden.

4.2.2.9 Klassifizierung von verarbeiteten Daten

Wie in Abschnitt 4.2.2.5 beschrieben, existieren verschiedene Kategorien von Assets im Rahmen industrieller Geschäfts- und Produktionsprozesse. Im Rahmen zunehmender Vernetzung gilt ein besonderes Augenmerk denjenigen Assets, die in digitaler Form vorliegen. Einige Assets werden ganz offensichtlich primär in digitaler Form verarbeitet und übertragen (z. B. Kundendaten), während andere Daten erst auf den zweiten Blick als wertvolles Asset ersichtlich werden. Ein Beispiel wären Fabrikationsdaten, die an eine Werkzeugmaschine übermittelt werden. Auf den ersten Blick handelt es sich dabei lediglich um Positions- bzw. Steuerdaten für ein Werkzeug. Auf den zweiten Blick wird jedoch deutlich, dass diese Daten wertvolles Konstruktionswissen enthalten können, in das u. U. viel Entwicklungsarbeit und Geld investiert wurde, es sich also um geistiges Eigentum handelt.

Es ist daher wichtig, für alle verarbeiteten Daten zu definieren, welche Rolle mit welchen Berechtigungen auf die Daten zugreifen darf. Die Erfassung der Daten kann in Form zweier Matrizen erfolgen. Die erste Matrix beschreibt, welche Rollen mit welchen Berechtigungen (Erstellen, Lesen, Schreiben, Löschen) auf welche Repräsentationen eines bestimmten Datums zugreifen dürfen.

Die zweite Matrix beschreibt, welche Rollen mit welchen Berechtigungen auf welche Repräsentationen eines Datums zugreifen können, obwohl dies eigentlich nicht gewünscht ist. Ein Beispiel wäre eine Rolle „Wartung“, die uneingeschränkten Zugriff auf eine Werkzeugmaschine erlaubt, obwohl der Wartungsmitarbeiter eigentlich keinen Zugriff auf Daten haben sollte, die in der Maschine verarbeitet werden.

Zusätzlich sollte erfasst werden, welche Assets betroffen sind, wenn eine Trennung von Berechtigungen fehlschlägt.

Ein Datum kann in einem von drei Zuständen vorliegen:

- Adressiertes Datum (Datum, welches irgendwo gespeichert vorliegt, z. B. Datenbank, Hauptspeicher, Datenträger usw.)
- Datum In-Transit (Datum, welches z. B. über ein Netzwerk übertragen wird)
- Datum in Verarbeitung (Datum, welches innerhalb eines Prozesses benutzt oder generiert wird)

Um passende Sicherheitsmaßnahmen ableiten zu können, müssen alle möglichen Zustände eines Datums aufgeführt werden. Wurde beispielsweise das Schutzziel Vertraulichkeit für ein Datum identifiziert, bringt es in den meisten Fällen nichts, die Datei verschlüsselt zu speichern, wenn sie später unverschlüsselt über einen unsicheren Kanal übertragen wird.

In Verarbeitung befindliche Daten müssen ebenfalls beschrieben werden, da diese Daten eher implementierungsspezifisch sind und es somit für die Sicherheitsanalyse wichtig ist zu wissen, welcher Prozess Daten generiert. So könnten Implementierung darauf angewiesen sein temporäre Kopien schützenswerter Datenrepräsentationen anzulegen. Im späteren Verlauf der Entwicklung des Systems könnte die Existenz dieser temporären Kopien übersehen werden und so bei der weiteren Bedrohungsanalyse ausgenommen werden. Des Weiteren ist es für die Sicherheitsanalyse nötig zu dokumentieren, welche Prozesse mit welcher Art von Daten arbeiten um prüfen zu können, wo im Gesamtsystem schützenswerte Daten verarbeitet werden und wie die Daten während der Verarbeitung geschützt werden. Daher muss dokumentiert werden, welche Daten von welchem Prozess bearbeitet werden und welche Daten von den Prozessen generiert werden.

Typische Datenassets könnten bspw. diese sein:

- Passwörter
- Kryptographische Schlüssel
- Zertifikate
- Datenbankeinträge
- Personenbezogene Daten (Namen, Geburtsdaten usw.)
- (Post-) Adressen, Telefonnummern, Email-Adressen
- Finanzielle Daten (z. B. Rechnungsdaten)
- Kreditkartendaten
- Auftragsdetails (Waren, Stückzahlen)

Zur Dokumentation der Zugriffsrechte auf Daten kann das CRUD-Verfahren (Create, Read, Update, Delete) genutzt werden. Für jedes Datum kann dabei eine Matrix mit den Spalten Erzeugen, Lesen, Ändern, Löschen und einer Spalte pro Akteur angelegt werden. In dieser Matrix wird dann

vermerkt, welche Zugriffsrechte jeder Akteur auf die entsprechenden Daten hat. Zusätzlich kann eine weitere Matrix pro Datum angelegt werden, die dokumentiert, welche Akteure welche Zugriffsrechte auf Daten haben, auf die sie eigentlich keinen Zugriff haben sollten. So sollten z. B. Administratoren für Wartungsarbeiten eigentlich keinen Zugriff auf diverse Daten haben. Jedoch erlaubt ihnen der administrative Zugang zu einem System oft auch das Auslesen und Manipulieren entsprechender Daten.

Im Anschluss wird eine weitere Matrix angelegt, für in den Zeilen alle Datenassets und in den Spalten die oben genannten Datenzustände (Adressiert, In-Transit, in Verarbeitung) enthält. Dabei soll in der Spalte „In-Transit“ dokumentiert werden, über welche Kanäle das Datum transportiert wird. Die Spalte „in Verarbeitung“ dokumentiert in welchen Modulen, Prozessen etc. das Datum verarbeitet wird. In der Spalte „Adressiert“ wird notiert wo die Daten letztlich abgelegt oder gespeichert werden, also Dateien, Datenbanken, aber auch nichtdigitale Medien.

4.2.2.10 Technologien, Plattformen und Architekturen

Die bei der Entwicklung einer industriellen Anlage/Lösung verwendeten Technologien und Architekturen bringen sowohl Vor- als auch Nachteile mit sich. Für eine Sicherheitsanalyse ist es wichtig zu wissen, welche Technologien für eine Anlage verwendet wurden, für welche Plattformen sich in der Anlage wiederfinden (Betriebssysteme, Systemarchitekturen) und ob ein architekturelles Schema zur Konzeption angewendet wurde (z. B. SCADA). Die Dokumentation dieser Eigenschaften ermöglicht es allgemeine Verwundbarkeiten der verwendeten Technologien und Architekturen bereits bei der Planung einer Anlage oder auch während dem Betrieb einer Anlage zu identifizieren und Gegenmaßnahmen einzuleiten. Folgende Ergebnisse werden in diesem Schritt erwartet:

- Auflistung relevanter Plattformen im Kontext der Anlage
- Auflistung von verwendeten Technologien der Anlage (Bussysteme, Netzwerke, etc.)
- Auflistung architektureller Konzepte die zur Erstellung der Anlage verfolgt wurden

Die Auflistungen sollen jeweils eine Begründung beinhalten, weshalb die jeweilige Plattform, Technologie und das Architekturkonzepte verwendet wurden, wie z. B. Kompatibilitätsgründe, Lizenzen, Preis, rechtliche Gründe etc.. So kann im weiteren Verlauf der Anlagenplanung und im Betrieb der Anlage eine Abwägung bzw. Aussage über die Verwendung oder den Austausch von Anlagenkomponenten getroffen werden.

Die von einer industriellen Anlage verwendeten Technologien, Plattformen und Architekturkonzepte sollten also dokumentiert werden. Dabei beschreiben Plattformen Betriebssysteme oder Hardwaresysteme, die entweder proprietäre Betriebssysteme oder eher bekannte Systeme wie Microsoft Windows, Linux, Unix etc. verwenden. Die Gründe, weswegen eine Plattform gewählt wurde sollen dabei ebenfalls kommentiert werden.

Neben den Plattformen müssen auch die verwendeten Technologien dokumentiert werden. Diese beinhalten unter anderem Softwarelösungen (z. B. Webserver, Kryptographiebibliotheken) und Middlewares (z. B. OPCUA, OSGi), Appliances (Firewalls, Proxies, Router) und Bussysteme (z. B. CAN, LIN, MOS, Zigbee, Profi-Bus, WLAN, Bluetooth).[145] Auch in dieser Auflistung ist es wichtig die Entscheidung zur Verwendung einer Technologie zu begründen. So werden z. B. in bestimmten Fällen sicherere Technologien bewusst nicht verwendet, da sie mit anderen Anforderungen einer Anlage, wie Echtzeit oder auch Kompatibilität zu Altsystemen, kollidieren.

Analog zum oben genannten Vorgehen wird mit architekturellen Konzepten verfahren. Sind solche Paradigmen für eine industrielle Lösung und ihre jeweiligen Komponenten festgelegt, können für die Entwicklung, den Aufbau und die Wartung Handlungsanweisungen und Best Practices gemäß den definierten architekturellen Konzepten angegeben werden. Beispiele für entsprechende Konzepte in ICS sind SCADA oder auch PLS (Verteile Steueranlagen, Prozessleitsystem, engl. Distributed Control System (DCS) oder Process Control System (PCS)). Da in I4.0 neben industriellen Steuerungen und Maschinen auch vermehrt IT-Systeme wesentliche Aspekte der Produktion prägen, müssen auch diese Systeme in einem Bedrohungsmodell erfasst werden. Dabei können Architekturkonzepte der IT-Komponenten z. B. folgende sein:

145 Beispielhafte Aufzählung; Abkürzungen sind im Abkürzungsverzeichnis enthalten.

- Web Application
- Client/Server
- Serviceorientierte Architektur (u.a. Cloud)
- Peer-to-Peer
- Verteilte Systeme

4.2.2.11 Auswahl geeigneter Ansätze zur Bedrohungsmodellierung

Derzeit existieren verschiedene Techniken zur Erfassung und Modellierung von Bedrohungen. Viele dieser Ansätze kommen klassischerweise aus der Softwareentwicklung, sind aber mit Anpassungen auch für den Einsatz in industriellen Szenarien tauglich. Durch die in I4.0 bedeutendere Rolle von Softwaresystemen in der Produktion schwinden die Grenzen zwischen reinen Produktionssystemen und IT-Systemen ohnehin mehr und mehr. Wie auch bei der Bedrohungsmodellierung von Softwaresystemen eignet sich nicht jede Modellierungstechnik für jedwede Art von industrieller Lösung. Hier gibt es z. B. Unterschiede im möglichen Detailierungsgrad des Modellierungsansatzes. So eignet sich z. B. eine Technik wie STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of privilege; siehe Abschnitt 4.2.2.13) sehr gut zum Modellieren einer Lösung oder Anlage, die aus mehreren Teilkomponenten mit Datenflüssen besteht. Jedoch eignet sich STRIDE nicht für die detaillierte Erfassung jeglicher Teilkomponenten eines komplexen Systems, da der Ansatz bei zu feiner Detaillierung zu enormen zu prüfenden Datenmengen führt. Daher muss zunächst entschieden werden, welcher Ansatz zur Bedrohungsmodellierung gewählt wird. In vielen Fällen ist es sinnvoll mehrere Techniken für verschiedene Teilaspekte eines Systems zu wählen. In diesem Sinne muss dokumentiert werden, welche Ansätze zur Bedrohungsmodellierung für welche Aspekte oder Komponenten des zu analysierenden Systems gewählt wurden. Die Dokumentation soll auch eine Begründung für die Auswahl beinhalten. So können einerseits bei einer Reevaluierung des Systems (z. B. bei einer Erweiterung) die gleichen Vorgänge, wie in der ursprünglichen Analyse verwendet werden. Andererseits erlaubt die lückenlose Dokumentation des Prozesses, im Falle des Eintritts einer unerwarteten Bedrohung, eine fundierte Fehleranalyse bei der Bedrohungsmodellierung.

Ein weiterer positiver Aspekt eines derart dokumentierten Ansatzes zur Bedrohungsanalyse ergibt sich aus der, auch in der industriellen Produktion vermehrten, Modularisierung von Anlagen- und Systemkomponenten. So kann das zu analysierende System in einem künftigen Szenario eine Teilkomponente eines komplexeren Systems repräsentieren. In diesem Falle kann zur Analyse des komplexeren Systems auf das Bedrohungsmodell der Teilkomponente zurückgegriffen werden, um redundante Arbeiten zu vermeiden. Im weiteren Verlauf des Dokuments werden einige Ansätze zur Bedrohungsmodellierung, wie z. B. STRIDE oder die datenbankgestützte Schwachstellenanalyse, vorgestellt.

4.2.2.12 Datenbankgestützte Schwachstellenanalyse

Ein leichtgewichtiger Einsatz zur Identifikation von Bedrohungen und Schwachstellen besteht darin, am Markt verfügbare Schwachstellendatenbanken, nach für das zu analysierende System relevanten, Schwachstellen zu durchsuchen. Ein Beispiel für eine solche Datenbank ist die frei verfügbare Datenbank CWE™ (Common Weakness Enumeration) der MITRE Corporation[146]. CWE™ ist ein öffentlicher Katalog mit ausführlichen Beschreibungen von allgemeinen Softwareschwachstellen sortiert nach Technologien, Eintrittszeitpunkt der Schwachstelle (Design, Implementierung, Betrieb ...), Konsequenzen beim Ausnutzen der Schwachstelle und weiteren Aspekten. Durch eine Recherche des Katalogs vor dem Hintergrund der gesammelten Systemeigenschaften aus den vorigen Schritten, kann eine für das zu analysierende System relevante Menge an Schwachstellen identifiziert werden.

Die NVD (National Vulnerability Database) und – ebenfalls von MITRE – CVE (Common Vulnerabilities and Exposures) sind weitere öffentliche Anlaufstellen, wobei der Datensatz der NVD auf den der CVE aufbaut. Im Gegensatz zur CWE listet die CVE konkrete Verwundbarkeiten von Softwaresystemen und in geringerem Maße auch von Hardwaresystemen. Zur Analyse einer derartigen Datenbank kann zum einen das Komponenteninventar, welches im ersten Schritt der Bedrohungsmodellierung angefertigt wird und die Auflistung verwendeter Plattformen und Technologien (siehe Abschnitt 4.2.2.10) genutzt werden. Das Resultat der Analyse ist eine Auflistung von sowohl allgemeinen, als auch spezifischen Schwachstellen und Verwundbarkeiten für das zu analysierende System. Bei der datenbankgestützten Schwachstellenanalyse ist eine regelmäßige Wiederholung der Analyse von großer Bedeutung. Schwachstellendaten-

146 Common Weakness Enumeration (CWE™), http://cwe.mitre.org/, zuletzt abgerufen am 16.07.2015.

banken werden im Allgemeinen regelmäßig aktualisiert und um neue Funde erweitert. Ohne die wiederholte Ausführung der Analyse könnten Verwundbarkeiten, die nach der initialen Analyse publik wurden, unentdeckt bleiben.

4.2.2.13 Identifizieren von Bedrohungen mittels STRIDE

Die STRIDE-Methode ist eine weit verbreitete Methode zur entwurfsgesteuerten Bedrohungsmodellierung aus dem Microsoft Security Development Lifecycle (SDL[147]). Bei letzterem handelt es sich um ein von Microsoft entwickeltes und selbst verwendetes Konzept zur Entwicklung sicherer Software. Das Konzept soll durch verschiedene Maßnahmen in einem definierten Prozess sicherstellen, dass offensichtliche Schwachstellen bei der Entwicklung systematisch erkannt und vermieden werden. Auf der technischen Ebene steht im Kern von SDL das Threat Modeling durch die STRIDE-Methode. STRIDE steht für Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege. Die Methode sieht eine systematische Bewertung von Prozessen, Daten, Schnittstellen, Systemgrenzen usw. vor, um eine automatisch generierte Handlungsanweisung zur Einhaltung bestimmter Schutzziele zu erzeugen.

Um diese Methode anzuwenden, ist mindestens ein Datenflussdigramm sinnvoll, welches eine High-Level-Sicht auf das gesamte System ermöglicht. Ein solches Diagramm sollte bereits im ersten Schritt erstellt worden sein, um die Beziehungen von externen Akteuren, Prozessen, Datenspeichern, Datenflüssen und Vertrauensgrenzen darzustellen (siehe Abschnitt 4.2.2.1). Der STRIDE-Methode folgend, wird nun ein System in seine relevanten Komponenten zerlegt, jede Komponente im Hinblick auf zutreffende Bedrohungen analysiert und für deren Entschärfung geeignete Maßnahmen festgehalten. Dieser Vorgang wird solange wiederholt, bis alle verbleibenden Bedrohungen als akzeptabel eingestuft worden sind.

An dieser Stelle ist das SDL Threat Modeling Tool[148] hervorzuheben, welches eine STRIDE-Analyse durch grafische Interaktion unterstützt und kostenlos von Microsoft erhältlich ist. Dieses Threat Modeling Tool hat den Anspruch, auch von Nicht-Security-Experten genutzt werden zu können. Dazu wird im ersten Schritt durch einfaches Drag & Drop von graphischen Templates das Security-Design eines Systems in Form eines Data-Flow-Diagram (DFD) gezeichnet und visualisiert (Design View). Als Templates stehen Prozesse, Datenflüsse, externe Akteure, Datenspeicher, Vertrauens-, Prozess- und Maschinengrenzen zur Verfügung.

Im zweiten Schritt werden wird nun automatisch eine Liste möglicher Bedrohungen erstellt, indem systematisch jedem Element im Datenflussdiagramm potentielle relevante Bedrohungen zugeordnet werden. Dabei kommen für bestimmte Elemente prinzipiell nur bestimmte Bedrohungen in Frage (siehe Tabelle 4–11). Durch die automatische Anwendung der Bedrohungstabelle auf ein Datenflussdiagramm wird eine potentielle lange Liste möglicher Bedrohungen generiert, die viele Einträge enthalten wird, die auf den ersten Blick irrelevant sind. Hier muss nun für jeden einzelnen Punkt der Liste dokumentiert werden, welche Auswirkungen im Schadensfall entstünden (Impact) und welche Gegenmaßnahmen in der Implementierung getroffen wurden (Solution) bzw. weshalb dieser Fall nicht zutreffend ist.

Im dritten Schritt ist eine Dokumentation von externen Abhängigkeiten und getroffenen Annahmen für die Ausführungsumgebung möglich. Am Ende sollte eine Tabelle stehen, die alle relevanten Bedrohungen des Systems auflistet.

Tabelle 4–11: Mögliche Bedrohungen für Elemente eines Datenflussdiagramms

Entität	Täuschung	Manipulation	Leugnung	Enthüllung	Dienstblockade	Rechteausweitung
Externe Akteure	X		X			
Datenfluss		X		X	X	
Datenspeicher		X	X	X	X	
Prozess	X	X	X	X	X	X

147 The Trustworthy Computing Security Development Lifecycle, https://msdn.microsoft.com/en-us/library/ms995349.aspx, zuletzt abgerufen am 16.07.2015.
148 http://msdn.microsoft.com/en-us/magazine/cc163519.aspx

4.2.2.14 Identifizieren von Bedrohungen mittels Bewertung von Angreifern

Es existieren mehrere Möglichkeiten, um Sicherheitsbedrohungen für ein System zu identifizieren. Dabei ist nicht jede Methode für jedes System anwendbar, da möglicherweise nicht alle notwendigen Informationen, wie z. B. Anwendungsszenarios oder Implementierungsdetails, vorliegen. Es wird daher im Rahmen dieser Studie der Ansatz verfolgt, die Vorzüge der verschiedenen Methoden sinnvoll zu kombinieren. Die im vorigen Abschnitt vorgestellte entwurfsgesteuerte Bedrohungsmodellierung (STRIDE-Methode) basiert darauf, welche Schnittstellen und Vertrauensgrenzen vorhanden sind. Durch den Entwurf geeigneter Diagramme kann systematisch für jedes Element im Diagramm analysiert werden, welche Bedrohungen auftreten könnten. Eine sinnvolle Ergänzung zur entwurfsgesteuerten Modellierung stellt eine so genannte angreifergesteuerte Bedrohungsmodellierung dar. Im Kern einer solchen angreifergesteuerten Bedrohungsmodellierung steht die Frage, wer an den Ressourcen interessiert sein könnte. Sie basiert darauf zu verstehen, welche Fähigkeiten die Angreifer besitzen und wie sie Sie angreifen könnten. So lassen sich auch Bedrohungen durch die Betrachtung unterschiedlicher Angreifer-Profile im Kontext des modellierten Systems ableiten. Dazu müssen auch die unterschiedlichen Motivationen von Angreifer-Typen in Verbindung mit der wirtschaftlichen Machbarkeit betrachtet werden.

Das Ergebnis einer solchen Analyse kann eine Tabelle mit High-Level-Bedrohungen durch verschiedene Typen mit unterschiedlichen Motiven sein. Die nachfolgende Tabelle (siehe Tabelle 4–12) mit verschiedenen Angreifer-Typen und Motivationen kann als Basis für die weitere Betrachtung dienen.

Tabelle 4–12: Angreifer-Typen und -Motivation

Angreifertyp	Beschreibung	Fähigkeiten	Motivation
Anwender	Anwender mit Zugriff auf IT-Systeme können versuchen, diese zu manipulieren, um ihre Arbeit zu erleichtern. Sie führen typischerweise keine bösen Absichten.	Niedrig	– Umgehen von Workflows eines Unternehmens – Komfortablere Nutzung einer Software-Schnittstelle mit schlechter Usability – Anpassung von IT-Systemen an eigene Anforderungen
Böswillige Angestellte	Böswillige Angestellte schädigen ihren Arbeitgeber oder andere Angestellte vorsätzlich.	Niedrig/ Mittel	– Erpressung – Rache – Ausschalten von Rivalen in Unternehmen, Karrieredruck – Verstecken von unrechtmäßigen oder unerlaubten Aktivitäten
Kleinkriminelle	Kriminelle, die IT-Systeme im kleinen Umfang zur unrechtmäßigen persönlichen Bereicherung angreifen. Angriffe sind typischerweise weder besonders organisiert, noch Bestandteil einer umfassenden kriminellen Strategie.	Niedrig/ Mittel	– Unrechtmäßige persönliche Bereicherung
Script-Kiddies	Personen, oftmals pubertär, mit wenig krimineller Energie, greifen IT-Systeme an, um ihr technisches Wissen auszuprobieren oder sich selbst zu behaupten.	Niedrig/ Mittel	– Hacken für Anerkennung
Hacktivists	Personen, die politisch motivierte Angriffe gegen IT-Systeme von Repräsentanten eines bestimmten politischen Systems oder Interessensgruppe richten. Ziele können IT-Systeme von Unternehmen sein, welche von den Angreifern als Gegner assoziiert werden.	Mittel	– Beeinträchtigung der Arbeitsabläufe von Unternehmen, welche als unmoralisch oder als gegen die eigene politische Meinung wahrgenommen werden. – Öffentliche Aufmerksamkeit auf das als böse wahrgenommene Unternehmen lenken.
Konkurrent	Konkurrierende Unternehmen können IT-Systeme angreifen, um die eigene wirtschaftliche Leistung auszuweiten oder die Aktivitäten oder Arbeitsabläufe des Konkurrenten zu behindern.	Mittel/ Hoch	– Industriespionage – Sabotage
Organisiertes Verbrechen	Kriminelle Organisationen greifen IT-Systeme als Teil einer umfassenden kriminellen Strategie an, um ihren Profit zu maximieren.	Hoch	– Illegale Aktivitäten mit monetärem Gewinn im großen Stil – Verstecken illegaler Aktivitäten – Erpressung – Verhindern von Ermittlungen

→

Tabelle 4–12: Angreifer-Typen und -Motivation (Fortsetzung)

Angreifertyp	Beschreibung	Fähigkeiten	Motivation
Geheimdienste	Geheimdienste führen Angriffe auf IT-Systeme primär für Aufklärungszwecke aus, aber zur Durchsetzung eigener spezifischer Interessen.	Hoch	– Auskundschaftung, Informationsdiebstahl – Manipulation von Informationen – Sabotage kritischer Infrastrukturen, Kriegsführung im Cyberspace

Im Zuge der Bedrohungsanalyse muss idealerweise für jede theoretisch mögliche Bedrohung eine Bewertung darüber stattfinden, welcher Typ Angreifer ein Interesse daran haben könnte. Dazu muss im Einzelfall untersucht werden, ob ein Angreifer des jeweiligen Typs im speziellen Fall seine Motive erreichen kann und welchen Aufwand er dafür betreiben müsste. Wenn der Lohn für einen erfolgreichen Angriff die Aufwendungen des Angreifers dafür übersteigt, kann von einer realistischen Bedrohung ausgegangen werden. Um den möglichen Lohn für einen erfolgreichen Angriff abzuschätzen, muss im ersten Schritt überprüft werden, ob die speziellen Funktionen oder Eigenschaften der betreffenden Systemkomponente es dem Angreifer überhaupt erlauben, mittels geeigneter Aktionen seine Ziele zu erreichen. Dazu können folgende Fragen hilfreich sein:

- Werden in der betreffenden Systemkomponente Informationen verarbeitet, die für den jeweiligen Angreifer-Typ von Wert sind und ggf. mit welcher Motivation?
- Können potentielle Angreifer davon profitieren, die Verfügbarkeit oder Integrität der betreffenden Systemkomponente zu beeinträchtigen?

Für die identifizierten Angreiferklassen, die in Frage kommen, müssen im zweiten Schritt abgeschätzt werden, welcher Aufwand für den Angriff zu betreiben ist. Dabei sollte im Fokus stehen, wie einfach ein Angreifer mit der entsprechenden Komponente in Kontakt kommt und ob nicht die gleichen Ziele auch auf anderem Wege mit geringerem Aufwand erreicht werden können, ohne die betreffende Komponente anzugreifen. Wenn die Entscheidung schwierig fällt, ob ein Angriff plausibel erscheint oder nicht, kann es hilfreich sein, den Worst Case anzunehmen.

Um abzuschätzen, wie einfach ein Angreifer mit einer bestimmten Komponente in Kontakt gelangen kann, mag beispielsweise ein Blick darauf hilfreich sein, ob ein Angreifer dieser Klasse auch ein regulärer Systemanwender sein kann, ob ein Zugriff aus der Ferne mit der Komponente möglich ist, oder ob dies erst durch vorhergehendes Social-Engineering mit bspw. Spear-Phishing möglich ist. Je mehr Aufgaben ein Angreifer benötigt, um Zugriff auf eine Komponente zu erhalten, noch bevor der eigentliche Angriff erfolgen kann um die gesteckten Ziele zu erreichen, desto geringer ist die Wahrscheinlichkeit, dass ein Angriff tatsächlich gelingt.

Ein Beispiel stellt das ERP-System dar, dass im Intranet (Office-IT) eines Unternehmens betrieben wird. Die Angestellten haben i.d.R. leichten Zugriff auf das Webinterface der Software-Lösung. Sie können auch leicht die Zugangsdaten von Kollegen stehlen, in dem sie bspw. beim Login über deren Schulter schauen oder einen Hardware-Keylogger an deren PC einstecken.

Im Vergleich dazu ist es für einen Konkurrenten des Unternehmens ungleich schwerer, Zugriff auf das ERP-System zu erhalten. Möglicherweise müsste ein Mitbewerber zunächst einen Angestellten des anzugreifenden Unternehmens bestechen.

Als finalen Schritt, auf Basis der gesammelten Schätzungen, muss nun entschieden werden, ob eine Angreiferklasse tatsächlich für das System relevant ist und dadurch auch eine tatsächliche Gefährdung darstellt. Dazu muss für jeden in Frage kommenden Angreifertyp das Verhältnis aus Kosten und Nutzen abgewogen werden. Unglücklicherweise gibt es dafür keine universelle Formel. Im Allgemeinen ist es sinnvoll, vom Worst-Case-Szenario auszugehen, dass für den jeweiligen Einsatzzweck einer Systemkomponente plausibel erscheint.

Am Ende der angreifergesteuerten Bedrohungsmodellierung soll eine Tabelle mit nachfolgenden Spalten stehen, die beschreibt, welcher Typ von Angreifer eine bestimmte Komponente angreifen könnte, seine wahrscheinlichen Motive, die notwendigen Schritte, um den Angriff durchzuführen, sowie die möglichen negativen Auswirkungen auf den Betreiber.

4.2.2.15 Priorisieren von Bedrohungen

In den vorherigen Abschnitten wurde ein umfangreiches Modell zur Beschreibung von I40-Systemlandschaften und zur Ermittlung von Bedrohungen mittels verschiedenster Methoden vorgestellt. Der Zweck dieses Schrittes ist es nun, die Signifikanz der gesammelten Bedrohungen im Gesamtkontext zu bestimmen. Dabei kann die Entscheidung, welche Bedrohung oder Typ von Bedrohung mehr oder weniger wichtig ist, nicht verallgemeinert werden, da dies unter anderen Faktoren davon abhängt, wo die betroffene Systemkomponente zum Einsatz kommt.

Deshalb ist es sinnvoll, die Priorisierung von Bedrohungen anhand von Schutzzielen vorzunehmen, die bereits in den vorigen Abschnitten spezifiziert (siehe Abschnitt 4.2.2.6) und gewichtet (siehe Abschnitt 4.2.2.7) wurden. Das Ziel ist es, alle Bedrohungen den Schutzzielen zuzuordnen und dadurch eine Priorisierung ableiten zu können. Dazu soll in diesem Schritt eine entsprechende Tabelle erstellt werden, welche den identifizierten Bedrohungen jeweils mindestens ein entsprechendes Schutzziel zuordnet und mittels Abwägung von Gewichtung der Schutzziele und dem Ausmaß der negativen Auswirkungen eine Priorisierung der Bedrohungen ermöglicht. Dabei ist es essentiell, jede Bedrohung mit jedem Schutzziel zu betrachten, da eine Bedrohung potentiell auch eine Gefährdung mehrerer Schutzziele bedeuten kann. Bei der Bewertung einer Bedrohung im Hinblick auf ein konkretes Schutzziel muss dessen Gewichtung (vernachlässigbar, marginal, kritisch, katastrophal) mit den negativen Auswirkungen im Falle eines erfolgreichen Angriffs abgewogen werden. In vielen Fällen wird es daher nicht möglich sein, eine exakte Bewertung vorzunehmen. In diesen Fällen ist es ausreichend, die Schätzung des Schadensausmaßes zur Priorisierung heranzuziehen. Es sollte für jeden Fall notiert werden, auf Basis welcher Annahmen eine Bewertung oder Schätzung stattgefunden hat. Als mögliche Annahmen könnten beispielsweise folgende Begründungen herangezogen werden:

- Die Produktion hat Vorrang: Dieser Satz gilt bis heute und wird voraussichtlich gültig bleiben, bis ein ungeplanter Produktionsausfall nachweislich weniger monetäre Verluste bedeutet, als ein IT-Sicherheitsvorfall.
- Die Sicherheit des eigenen Unternehmens hat Vorrang: Damit ist gemeint, dass die vorrangigen Interessen eines Unternehmens zunächst der Wahrung der eigenen Sicherheit, und erst danach der Sicherheit des Kunden oder Partnern gilt.
- Daten sind wichtiger als Prozesse: Während sich der Verlust oder Diebstahl von Daten nicht rückgängig machen lässt, können Prozesse einfach neu aufgesetzt werden.

4.3 Top 10 der Bedrohungen

Das BSI identifizierte auf Basis seiner Analysen und Industriekooperationen zur Cyber-Sicherheit eine **Liste von 10 Bedrohungen** die für Systeme zur Fertigungs- und Prozessautomatisierung besonders relevant sind (Abbildung 4–5, nächste Seite).[149] Der VDMA bat seine Mitglieder den bereits im Jahr 2012 vom BSI veröffentlichten Satz an Bedrohungen im Hinblick auf die Relevanz im Bereich der eigenen Produktion einzuschätzen[150]. Menschlichem Fehlverhalten und Sabotage wurde dabei die höchste Bedeutung beigemessen. Im Folgenden wird die Bedeutung dieser Bedrohungen vor dem Hintergrund der in Kapitel 4.1 vorgestellten Fallbeispiele diskutiert und damit in den I4.0-Kontext übertragen. Gleichzeit erfolgt eine Einordnung im Hinblick auf die oben eingeführten Fallgruppen. Wichtig ist im Hinblick auf die Bedrohungen die Unterscheidung zwischen Primärangriffen und Folgeangriffen. Der Fokus bei den vom BSI zusammengestellten Bedrohungen liegt auf Primärangriffen mit denen Angreifer in industrielle Anlagen eindringen. Die Bedrohung durch primäre Angriffe nimmt im I4.0-Kontext aufgrund von vielen Internet-verbundenen Komponenten, Anlagen, Standorten und Unternehmen nicht ab. Was sich im Kontext der I4.0 allerdings ändert ist, dass ein Angriff viel weitreichendere Folgen haben kann. Einerseits ist nicht unwahrscheinlich, dass die angegriffenen Komponenten direkten Zugriff auf immer umfangreichere Datenbestände haben und andererseits wachsen durch den hohen Grad der Vernetzung, den die intensive Kommunikation der Komponenten untereinander notwendig macht, die Möglichkeiten für einen Angreifer sich durch Folgeangriffe sukzessive im Unternehmen oder im Verbund von Unternehmen auszubreiten. Darüber hinaus wächst mit der zunehmenden Komplexität der IT-Infrastruktur auch die Gefahr von technischem Fehlverhalten.

149 BSI (2014): Industrial Control System Security – Top 10 Bedrohungen und Gegenmaßnahmen v1.1, März 2014. https://www.bsi.bund.de/ACS/DE/_/downloads/BSI-CS_005.pdf?__blob=publicationFile&v=2, zuletzt abgerufen am 19.11.2015.

150 VDMA (2013): VDMA-Studie: Status Quo der Security in Produktion und Automation 2013/2014, S. 13, http://www.vdma.org/documents/105969/142443/VDMA%20Studie%20Security/82324cfa-2df6-4c4e-ae21-490a26e30d0c

Abbildung 4–5: Die wichtigsten Bedrohungen für Systeme zur Fertigungs- und Prozessautomatisierung

Nr. (Nr. alt)	Top 10 2014	Top 10 2012
1 (2)(3)	Infektion mit Schadsoftware über Internet und Intranet	Unberechtigte Nutzung von Fernwartungszugängen
2 (6)	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	Online-Angriffe über Office- /Enterprise-Netze
3 (-)	Social Engineering†	Angriffe auf eingesetzte Standardkomponenten im ICS-Netz
4 (5)	Menschliches Fehlverhalten und Sabotage	(D)DoS Angriffe
5 (1)	Einbruch über Fernwartungszugänge	Menschliches Fehlverhalten und Sabotage
6 (-)	Internet-verbundene Steuerungskomponenten†	Einschleusen von Schadcode über Wechseldatenträger und externe Hardware
7 (10)	Technisches Fehlverhalten und höhere Gewalt	Lesen und Schreiben von Nachrichten im ICS-Netz‡
8 (-)	Kompromittierung von Smartphones im Produktionsumfeld†	Unberechtigter Zugriff auf Ressourcen‡
9 (-)	Kompromittierung von Extranet und Cloud-Komponenten†	Angriffe auf Netzwerkkomponenten‡
10 (4)	(D)DoS Angriffe	Technisches Fehlverhalten und höhere Gewalt

Legende: †NEU – ‡ENTFALLEN (weil Folgeangriff)
Quelle: BSI (2014): Industrial Control System Security – Top 10 Bedrohungen und Gegenmaßnahmen v1.1, Seite 2)

Die wichtigste Bedrohung von Systemen zur Fertigungs- und Prozessautomatisierung stellt die Infektion mit Schadsoftware dar. Die Infektion kann sowohl über Internet und Intranet aber auch über Wechseldatenträger und externe Hardware erfolgen. Angriffe über Internet und Intranet sind in der Regel auf Schwachstellen in Komponenten angewiesen. Unternehmensnetze – vor allem Office-Netze, zunehmend aber auch Produktionsnetze – nutzen Standardkomponenten für die laufend neue Schwachstellen bekannt werden[151]. Während es selbstverständlich ist, dass Office-Netze an das Internet angebunden sind, werden Office-Netze zunehmend mit Produktionsnetzen und auch Produktionsnetzte direkt mit dem Internet verbunden. Angriffe über Wechseldatenträger und externe Hardware setzen einen zumindest vorübergehenden Zugriff auf entsprechende, im Unternehmen oder Unternehmensverbund verwendete Komponenten oder Zugang zum System voraus.

Die Bedrohung ist vor allem für das Fallbeispiel aus der Automobilindustrie sowie das Fallbeispiel aus der chemischen Industrie von Bedeutung. In beiden Fallbeispielen wird auf Probleme bei der sauberen Trennung von Netzwerken bzw. Netzwerksegmenten hingewiesen. Dadurch werden Folgeangriffe nach einer Infektion mit Schadsoftware deutlich einfacher. Die Zusammenhänge zwischen der Sicherheit in Office-Netzen und der Sicherheit in Produktionsnetzen sind häufig nicht transparent. Anhand der Fallbeispiele lassen sich zahlreiche Aspekte verdeutlichen. Aus dem Fallbeispiel aus der Automobilindustrie geht klar hervor, dass die Angst vor einem Produktionsausfall oft deutlich größer ist als die Angst vor den Gefahren im Bereich der IT-Sicherheit. Darüber hinaus wird auf Probleme bei der Wartung der IT-Komponenten hingewiesen. Das zeitnahe Patchen von Schwachstellen bei Standardkomponenten oder ändern von Parametern ist nur schwer mit den Anforderungen der industriellen Produktion zu vereinbaren. Im Rahmen des Fallbeispiels aus der chemischen Industrie wird die besondere Problematik bei der Vernetzung von mehreren Standorten hervorgehoben. Die Bedrohung der Infektion mit Schadsoftware über Internet und Intranet geht in erster Linie von Außentätern aus. Die Angriffe können zielgerichtet oder auch nicht zielgerichtet sein. Prinzipiell ist aber auch ein Angriff durch Innentäter auf diesem Wege denkbar. Die Bedrohung der Infektion mit Schadsoftware über Wechseldatenträger und externe Hardware geht hingegen eher vom Kreis der Partner einer Kooperation aus. Es ist aber sowohl ein gezielter Angriff eines Innentäters vorstellbar als auch das Fehlverhalten eines Mitarbeiters der den Wechseldatenträger zuvor mit einem bereits infizierten System in Verbindung brachte. Prinzipiell ist aber auch ein gezielter Angriff durch Außentäter auf diesem Wege denkbar. Es ist nicht unüblich, dass Fremdpersonal eigene Wechseldatenträger mit sich führt.

151 BSI (2013): ICS-Security-Kompendium, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile

Auch menschliches Fehlverhalten und Sabotage stuft das BSI als wichtige Bedrohung ein. Diese Bedrohung betrifft sowohl das im Umfeld von Systemen zur Fertigungs- und Prozessautomatisierung tätige Personal als auch externes Personal egal ob Zutritt zu den Anlagen besteht oder aus der Ferne gearbeitet wird. Die Bedrohung ist vor allem für das Fallbeispiel aus der Werkzeugindustrie von Bedeutung. Aus dem Fallbeispiel wird die Problematik ersichtlich, dass eine Vertrauensbeziehung notwendig ist und vielfach Kompromisse zwischen Komfort und Sicherheit eingegangen werden müssen. Bei der Bedrohung wird angenommen, dass der Schaden durch Personen aus dem Kreis der Partner einer Kooperation herbeigeführt wird, entweder mit böser Absicht (Sabotage) oder ohne böse Absicht (menschliches Fehlverhalten). Social Engineering ist eine Methode, um unberechtigten Zugang zu Daten oder IT-Systemen zu erlangen. Mitarbeiter werden dabei zu unbedachten und fahrlässigen Handlungen verleitet. Prinzipiell kann jedes Unternehmen Opfer von Social Engineering werden. Keines der Fallbeispiele beschreibt eine Situation die explizit auf die Bedrohung durch Social Engineering hindeuten würde. Berücksichtigt werden sollte allerdings, dass eine mangelhafte Trennung von Netzen im Unternehmen oder im Unternehmensverband den Schaden durch Social Engineering deutlich vergrößern kann. Die Bedrohung durch Social Engineering geht in erster Linie von zielgerichteten Angriffen von Außentätern aus. Prinzipiell ist aber auch ein Angriff durch Innentäter auf diesem Wege denkbar.

Eine weitere wichtige Bedrohung ist der Einbruch über Fernwartungszugänge. Bei Systemen zur Fertigungs- und Prozessautomatisierung sind externe Zugänge für Wartungszwecke weit verbreitet. Das Fallbeispiel aus dem Maschinen- und Anlagenbau stellt verschiedene Ansätze zur Realisierung von Fernwartungszugängen in den Mittelpunkt der Diskussion. Es wird darauf hingewiesen, dass im I4.0-Kontext nicht nur eine immer größere Zahl an Fernwartungszugängen erforderlich ist, sondern die Daten auf den gewarteten Systemen immer mehr Einblicke in die Produktion erlauben. Auch im Hinblick auf einzelne Anlagen müssen Hersteller zunehmend Techniker von Zulieferern von IT-Komponenten in die Wartung einbeziehen. Im Rahmen des Fallbeispiels werden verschiedene Ansätze zur Absicherung von Fernwartungszugängen diskutiert.
Die Bedrohung durch Einbruch über Fernwartungszugänge geht in erster Linie von zielgerichteten Angriffen von Außentätern aus. Prinzipiell ist aber auch ein Angriff durch Innentäter auf diesem Wege denkbar. Die Kompromittierung von Smartphones im Produktionsumfeld stellt einen Sonderfall der Bedrohung durch Einbruch über Fernwartungszugänge dar, bei dem durch den Einsatz von Smartphones oder Tablets zur Anzeige und Veränderung von Betriebs- und Produktionsparametern eine zusätzliche Angriffsfläche erzeugt wird. Ähnlich verhält sich die Situation auch bei Internet-verbundenen Steuerungskomponenten die vor allem deshalb problematisch sind, da nach dem Bekanntwerden von Schwachstellen ein zeitnahes Einspielen von Patches häufig nicht möglich ist. Die Bedrohung durch Internet-verbundene Steuerungskomponenten geht in erster Linie von Angriffen von Außentätern aus. Keines der Fallbeispiele beschreibt eine Umgebung in der Smartphones oder Tablets zur Fernwartung zum Einsatz kommen oder Steuerungskomponenten direkt mit dem Internet verbunden wären.

Bei Fällen von technischem Fehlverhalten und höherer Gewalt sind nicht handelnde Personen sondern sonstige Ereignisse für den Schaden verantwortlich. Software-Fehler in IT-Komponenten, die zu unvorhergesehenem Fehlverhalten führen können, lassen sich ebenso wenig ausschließen wie mögliche Hardwaredefekte und Netzwerkausfälle. Im Hinblick auf die Fallbeispiele lässt sich am ehesten ein Bezug zum Fallbeispiel aus der Automobilindustrie sowie zum Fallbeispiel aus der Verpackungsindustrie herstellen. Während im ersten Fall aufgrund von technischem Fehlverhalten Sicherheitsmaßnahmen umgangen werden, kommt es im zweiten Fall zum Einsatz einer besonders komplexen IT-Infrastruktur wodurch sich die Wahrscheinlichkeit von technischem Fehlverhalten erhöht.

Eine weitere Bedrohung stellt die Kompromittierung von Extranet- und Cloud-Komponenten dar. Der Trend zum Outsourcing von IT-Komponenten hält auch in der Industrie Einzug. Während Outsourcing für Komponenten, die unmittelbar reale Prozesse steuern, aufgrund von Echtzeitanforderungen normalerweise nicht in Frage kommt, gibt es zunehmend Anbieter von Komponenten im Bereich Datenerfassung und –verarbeitung in Historians oder zur Berechnung von komplexen Modellen für die Konfiguration von Maschinen oder die Optimierung von Herstellungsprozessen. Auch sicherheitsspezifische Komponenten werden mitunter cloudbasiert angeboten. Derzeit ist die Nutzung von Cloud-Komponenten insbesondere für KMU interessant, da der eigenverantwortliche Betrieb der Komponenten häufig nicht wirtschaftlich möglich wäre. Beispielsweise platzieren Anbieter von Fernwartungslösungen die Clientsysteme für den Fernzugriff in der Cloud. Auf diesem Wege kann auch der Bogen von dieser Bedrohung zu den Fallbeispielen gespannt werden. Im Fallbeispiel aus der Werkzeugindustrie wird unter anderem die Option beschrieben, dass die Fernwartungsplattform von einem Dienstleister betrieben wird.

Mittels Denial-of-Service-(DoS)-Angriffen können vernetzte IT-Komponenten durch eine sehr hohe Anzahl an Anfragen überlastet werden. Ein derartiger Angriff ist sowohl bei drahtgebundenen als auch bei drahtlosen Verbindungen möglich. Die Bedrohung durch DoS-Angriffe geht in erster Linie von Außentätern aus. Im Kontext der Fallbeispiele ist diese Bedrohung nicht von Relevanz.

4.4 Bedrohungsszenarien aus rechtlicher Sicht

4.4.1 Kooperationsstruktur und Risiken

Die rechtliche Bewertung von Sicherheitsrisiken in der I4.0 muss sich letztlich am Einzelfall orientieren, da die rechtliche Bewertung, etwa in einem behördlichen oder gerichtlichen Verfahren stets alle Umstände des Einzelfalls einbeziehen muss. Für die Zwecke dieser Studie ist jedoch eine Zusammenfassung in maßgebliche Fallgruppen erforderlich. Daher werden nachfolgend zunächst die maßgeblichen Fallgruppen anhand eines abstrahierenden Modells beschrieben, durch die wesentliche Sicherheitsaspekte der I4.0 abgebildet werden können (4.4.1.1). Sodann werden die aus rechtlicher Sicht spezifischen Risiken der I4.0 in Fallgruppen zusammengefasst (4.4.1.2).

4.4.1.1 Kooperationsstrukturen in der Industrie 4.0

Für die rechtliche Betrachtung von Risiken in der I4.0 ist die rechtliche Struktur der Kooperation von großer Bedeutung. Bei der sich derzeit entwickelnden Kooperation in der I4.0 sind aus rechtlicher Sicht sehr viele Fallgruppen denkbar und auch in der Praxis relevant. Es gibt eine ganze Reihe unterschiedlicher Kriterien, anhand derer rechtlich relevante Fallgruppen gebildet werden können.

Organisation der Kooperation/vertragliche Beziehungen

Die Organisation der Kooperation ist für die rechtliche Bewertung zentral, zumal diese stets mit vertraglichen Beziehungen zwischen den Partnern einhergeht. Die vertraglichen Beziehungen, aus denen sich für die IT-Sicherheit relevante Pflichten und Verantwortlichkeiten ergeben, sind für die rechtliche Betrachtung in allen Bereichen von großer Bedeutung.

Insoweit sind mehrere Strukturen denkbar:

Lineare Struktur

Die Kooperation kann ganz oder in Teilbereichen in einer linearen Struktur erfolgen. In einer linearen Struktur hat jeder Partner eine rechtliche Beziehung nur mit dem oder den vor und hinter ihm stehende Mitglied einer Leistungskette. Musterbeispiele sind Lieferketten, bei denen jeweils ein Beteiligter seinerseits Zulieferungen erhält und sein Produkt an den nächsten Beteiligten weitergibt. Bei I4.0 geht die Zusammenarbeit aber typischerweise darüber hinaus.

Sternförmige Struktur

Die Kooperation kann ganz oder in Teilbereichen eine sternförmige Struktur aufweisen. Bei dieser Struktur gibt es einen zentralen Partner, der vertragliche Beziehungen zu allen übrigen Partnern aufweist, die untereinander aber keine oder nur ausnahmsweise vertragliche Beziehungen unterhalten. Die sternförmige Struktur der Kooperation findet sich in der Industrie sehr häufig, Sie liegt etwa der sog. Just-in-time-Produktion zugrunde. Bei dieser bestehen direkte Vertragsbeziehungen grundsätzlich nur im Verhältnis zum Endhersteller, der die Produktion koordiniert.[152] Zweiseitige Verträge zwischen den einzelnen Beteiligten bestehen dagegen typischerweise nicht.[153,154]

Die sternförmige Struktur dürfte auch in Bezug auf die Aspekte der I4.0 in der Praxis am häufigsten zu finden sein. Im Fallbeispiel „Logistik“ ist die Zusammenarbeit im Ausgangspunkt sternförmig organisiert.

152 Rohe, Netzverträge, S. 389.
153 Rohe, Netzverträge, S. 389.
154 Kleinknecht, in Martinek/Semler/Habermeier/Flohr, Vertriebsrecht, § 70 Rn. 58; Rohe, Netzverträge, S. 412.

Netzstruktur

Die Kooperation kann als netzförmige Struktur ausgestaltet sein. Hier bestehen vertragliche Beziehung zwischen allen oder den meisten Partnern. Ein Musterbeispiel ist etwa ein Joint Venture mit mehreren Beteiligten. Die Netzstruktur ist der sternförmigen Struktur ähnlich, wenn es einen zentralen Partner gibt. In diesen Fällen gegen sternförmige Struktur und Netzstruktur in der Praxis fast übergangslos ineinander über. Im Fall des Joint Venture ist dies oft der Fall, wenn eine gemeinsame Joint Venture-Gesellschaft besteht, die der Mittelpunkt der gemeinsamen Aktivität ist.

Das Fallbeispiel „Logistik“ (dazu 4.1.4.1) kann auch als Netzstruktur ausgestaltet sein. Insoweit bestehen mehrere Ansätze. Teilweise sind einzelne Bereiche in netzförmiger Kooperation zusammengeschlossen. Beispiele sind etwa Einkaufsgemeinschaften für Rohstoffe (im Fallbeispiel Paper Supply Plattform), Zusammenarbeit von Produktionswerken im Rahmen von CPMS Interplant, werksübergreifende Transportplanung.

Darüber hinaus ergibt sich eine netzförmige Struktur in Bezug auf das spezifische Kooperationselement der Industrie 4.0, wenn alle Beteiligten, die per Internet kooperieren und wechselseitig auf Systeme zugreifen, miteinander einen Rahmenvertrag über die Nutzung des Systems schließen. Dies wird bisher, soweit ersichtlich, jedoch nur selten praktiziert.

Belegenheit (Sitz, Niederlassung) der Beteiligten

Die Belegenheit der an der Kooperation beteiligten Unternehmen ist für fast alle Rechtsfragen wichtig: im Datenschutzrecht etwa für das anwendbare Datenschutzrecht sowie für die materiellen Anforderungen an die Zusammenarbeit, im Vertragsrecht für das anwendbare Recht, Leistungsort, im Haftungsrecht insbesondere für das anwendbare Recht.

Hier sind Unterscheidungen zu treffen danach, ob die Partner im Inland, in einem anderen Staat des Europäischen Wirtschaftsraums (EWR), oder in einem anderen Staaten (Drittstaat) ansässig sind.

Soweit, wie bei einer sternförmigen Situation, aber oft auch bei Netzstruktur der Zusammenarbeit, ein zentraler Partner vorhanden ist, ist der Ort des zentralen Partners in der Praxis von entscheidender Bedeutung.

Branchenzugehörigkeit der Partner

Die Branchenzugehörigkeit der Kooperation ist aus rechtlicher Sicht vor allem für die Anwendbarkeit branchenspezifischer Normen relevant. Auch bei der Bewertung allgemeiner Normen ergeben sich durch die Berücksichtigung branchenspezifischer Interessenlagen Besonderheiten.

Im Rahmen dieser Studie müssen die unzähligen Konstellationen auf wenige Fallgruppen zurückgeführt werden. Für die rechtliche Analyse der Risiken wird daher ein abstrahierendes Modell gebildet, in dem möglichst viele sicherheitsrelevante Aspekte abgedeckt werden können. Dabei sind vor allem die Aspekte zu berücksichtigen, die sich aus dem organisatorischen Charakter der Zusammenarbeit ergeben. Die erforderliche Differenzierung erfolgt in innerhalb der abstrakten Fallgruppen durch Bildung von Unterfallgruppen und sonstige Differenzierungen. Da die praxisrelevanten Fallgruppen und Differenzierungen insoweit stark vom jeweiligen Rechtsbereich abhängen, wird diese weitere Differenzierung bei den einzelnen Kapiteln (4.4.2–4.4.7) durchgeführt.

Bei der Bildung der Fallgruppen wird wegen der zentralen Bedeutung vor allem die Struktur der Zusammenarbeit und der Ort der Beteiligten berücksichtigt. Es werden daher zwei Grundkonstellationen betrachtet, die durch Varianten weiter ausdifferenziert werden. Zur Vereinfachung wird von der Branchenzugehörigkeit so weit wie möglich abstrahiert und von einem Produktionsbetrieb ausgegangen.

1. Grundkonstellation: Sternförmige Kooperationsstruktur mit einem zentralen Partner im Inland.

   Als wichtige Unterfallgruppen werden hier vor allem die Fälle einbezogen, dass Partner ausschließlich im Inland, oder auch im EWR oder auch in Drittstaaten tätig sind.

2. Grundkonstellation: Netzförmige Kooperation ohne zentralen Partner mit Partnern in verschiedenen Staaten.

   Wichtige Unterfallgruppen ergeben sich auch hier aus der Belegenheit der Partner (EWR, Drittstaaten).

4.4.1.2 Risiken und Schadensszenarien in der Industrie 4.0

Für die rechtliche Bewertung der IT-Sicherheit in der I4.0 sind die maßgeblichen Risiken und Schadensszenarien von großer Bedeutung. In der Praxis sind diese überaus vielfältig und können nicht abschließend erfasst werden. Aus rechtlicher Sicht lassen sich aber zwei große Fallgruppen bilden:

Handlungen aus dem Kreis der Partner führen zu einem Schaden

Hier können die unterschiedlichsten Handlungen und Schadensszenarien von Bedeutung sein. Dabei sind zwei Unterfallgruppen von besonderem Interesse:

- Unterbliebene oder fehlerhafte Zulieferungen können zu Störungen führen und Schäden verursachen. IT-Spezifisch wäre etwa die Übermittlung fehlerhafter Daten, die zu Störungen führen können. Besonders weitreichende Folgen können entstehen, wenn durch fehlerhafte Daten Produkte fehlerhaft sind und bei Dritten, (Abnehmer, Unbeteiligte) Schäden verursachen.

  Beispiel: Aufgrund fehlerhafter Daten eines Zulieferers werden Bremsanlagen eines KFZ fehlerhaft gebaut. Der Endabnehmer verursacht einen Unfall, bei dem Dritte geschädigt werden.

- Veränderungen oder Löschung von Daten durch einen Partner, etwa einen Zulieferer, können zu Störungen führen und Schäden verursachen.

- Verstöße gegen Rechtsnormen, z. B. Datenschutznormen, Ausfuhrbestimmungen, können, etwa aufgrund behördlichen Einschreitens, zu Einschränkungen, z. B. Untersagung der Produktion oder Sanktionen führen.

Eingriffe Dritter oder sonstige Ereignisse führen zu Schäden

Die zweite große Fallgruppe betrifft Schäden durch Eingriffe von außen, also von Dritten, die nicht Partner der Kooperation sind. Ein Aspekt der IT-Sicherheit ist etwa Hacking mit Datenverlust oder Datenmanipulation, oder auch Verlust der Vertraulichkeit von Information (z. B. Geschäftsgeheimnisse). Es können aber auch Prozesse oder Anlagen geschädigt werden.

Das BSI berichtet in seinem Lagebericht 2014 von einem gezielten Angriff auf ein Stahlwerk, bei dem die Täter über das Büronetz auf das Produktionsnetz zugriffen und die Steuerung so massiv störten, dass ein Hochofen nicht geregelt heruntergefahren werden konnte und massive Schäden eintraten.[155]

In die zweite große Fallgruppe gehören auch Schäden, die durch sonstige Ereignisse, etwa Naturereignisse oder sonst nicht kontrollierbares Ereignis, etwa Zufall, „Ausreißer“, oder, praktisch sehr häufig, Störungen, deren Ursache nicht geklärt werden kann.

Das Fallbeispiel „Inbetriebnahme unter Zeitdruck“ enthält ein Beispiel für ein Schadensszenario der zweiten Fallgruppe.

Die unmittelbare Ursache der Störung entstand ohne Mitwirkung aus dem Kreis der Kooperationspartner. Hier ist aber von Bedeutung, welche Maßnahmen die Partner in Bezug auf die Störung treffen. Durch die gewählte Maßnahme können, wie im Fallbeispiel illustriert, auch neue Risiken entstehen. Wenn etwa aufgrund des Abschaltens der Firewall ein Eingriff Dritter erfolgt, etwa Daten ausgespäht, verändert oder gelöscht werden, könne sich für die Rechtsfolgen in mehreren Rechtsbereichen ergeben, etwa im Datenschutzrecht, oder im Bereich der vertraglichen und außeraußervertraglichen Haftung.

Die genannten Fallgruppen können, obwohl sie für viele Rechtsfragen sehr unterschiedlich zu beurteilen sind, in einem Sachverhalt zusammentreffen. Und dies geschieht auch häufig. Wenn beispielsweise im Fallbeispiel „Inbetriebnahme unter Zeitdruck“ die Störung durch Übermittlung fehlerhaften Datenmaterials eines Partners verursacht wurde, liegt insoweit ein Fall der ersten Fallgruppe vor. Für den weiteren Geschehensablauf, insofern die Maßnahmen, die im Rahmen der Störungsbeseitigung getroffen werden, können aber Aspekte der zweiten Fallgruppe eine Rolle spielen, wenn etwa im Rahmen der Störungsbeseitigung die Firewall abgeschaltet wird und sodann ein Eingriff eines Dritten (z. B. Hacking) erfolgt, liegt insoweit wiederum ein Fall der zweiten Fallgruppe vor.

Besonders wichtig sind allerdings Angriffe, bei denen Dritte zunächst einen Partner angreifen und dessen Handlungen ausnutzen, um das eigentliche Ziel zu erreichen. Dies ist etwa dann der Fall, wenn Passwörter von Partner ausgespäht werden.

155 BSI, Die Lage der IT-Sicherheit in Deutschland 2014, Ziff. 3.3.1 (S. 31).

Ein gutes Beispiel ergibt sich aus dem Lagebericht des BSI 2014. Das BSI beichtet von Angriffen der sog. Dragonfly-Gruppe auf Produktionsnetze, bei denen zunächst die Hersteller von Industriesteuerungssystemen angegriffen wurden und deren Programme mit Schadprogrammen versehen wurden, so dass die Kunden der Softwarehersteller mit dem Steuerungssystem auch Schadprogramme auf ihren Systemen installierten.[156]

Auch das soeben genannte Beispiel eines Angriffs auf ein Stahlwerk könnte im Rahmen der I4.0 in dieser Weise ablaufen, indem etwa bei einem Partner der initiale Angriff erfolgt.

Diese mögliche Verbindung der Fallgruppen in einem komplexen Sachverhalt ändert aber nichts dran, dass aus rechtlicher Sicht wesentlich danach zu unterscheiden ist, ob die Handlung, die unmittelbar zu einem Schaden führt, von einem Partner oder von einem Dritten ausgeht.

4.4.2 Vertragsrechtliche Aspekte

Im Bereich des Vertragsrechts sind für Kooperationen in der I4.0 vor allem zwei Aspekte von Bedeutung. Zum einen ist zu fragen, welche Pflichten die Beteiligten in Bezug auf IT-Sicherheit und Abwehr von Schadensszenarien haben. Zum anderen stellt sich die Frage, welche Haftungsfolgen für die Beteiligten in den verschiedenen Schadensszenarien denkbar sind.

Pflichten und Haftung der Beteiligten können sich unmittelbar aus Gesetz, aber auch aus den zwischen den Beteiligten geschlossenen Verträgen ergeben. Letztere sind von besonderem Interesse, da die Parteien hier entsprechend ihrer Interessenlage ihr Verhältnis privatautonom regeln können.

In diesem Abschnitt wird zunächst dargestellt, welche rechtlichen, insbesondere vertraglichen Beziehungen zwischen den Beteiligten bestehen (4.4.2.1) und welchem Recht sie unterliegen (4.4.2.2). Sodann wird untersucht, welche Pflichten die Beteiligten in Bezug auf die IT-Sicherheit in der I4.0 treffen (4.4.2.3).

4.4.2.1 Schuldvertragliche und gesellschaftsvertragliche Kooperation

Die Kooperation in der I4.0 kann rechtlich sehr unterschiedlich ausgestaltet sein. Aus der Sicht des deutschen Rechts sind insbesondere eine schuldvertragliche Grundlage und eine gesellschaftsrechtliche Kooperation von Bedeutung. Die Abgrenzung hat für die jeweilige Kooperationsstruktur zu erfolgen.

Die sternförmige Struktur zeichnet sich, wie (oben 4.4.1.1) dargestellt, dadurch aus, dass nicht alle Beteiligten vertraglich miteinander verbunden sind, sondern ein Beteiligter, der – rechtlich – im Mittelpunkt der Kooperation steht, vertragliche Beziehungen zu den anderen Beteiligten unterhält.

Bei solchen sternförmigen Strukturen kommt eine gesellschaftliche Verbindung aller Beteiligter nicht in Betracht. Vielmehr werden zwischen den Beteiligten Schuldverträge geschlossen. Dies wird etwa für die Just-in-time-Produktion angenommen.[157]

Ebenso wird bei der Kooperation in der Industrie 4.0, soweit sie sternförmig organisiert ist, keine Gesellschaft zwischen den Beteiligten gebildet. Vielmehr werden zwischen dem zentralen Beteiligten und den übrigen Beteiligten, teilweise auch zwischen den übrigen Beteiligten untereinander, Schuldverträge geschlossen.

Bei einer netzförmigen Struktur, bei der alle Beteiligten untereinander vertraglich verbunden sind (dazu oben 4.4.1.1), ist die Abgrenzung zwischen der schuldrechtlichen und gesellschaftsvertraglichen Beziehung schwieriger. Dies gilt entsprechend, soweit ein Teil der Beteiligten, etwa untereinander, durch ein mehrseitiges Vertragsverhältnis verbunden ist.

Ein klassisches Beispiel für eine vertragliche Netzstruktur ist, wie dargestellt, das Joint Venture. Bei Joint Ventures wird zwischen Equity Joint Ventures (auch „inkorporierte Joint Venture“ genannt), bei denen die Partner eine Gesellschaft gründen[158] und Contractual Joint Ventures, bei denen die Kooperation zwischen den Partnern vor allem auf schuldrechtlicher Ebene stattfindet,[159] unterschieden.

156 BSI, Die Lage der IT-Sicherheit in Deutschland 2014, Ziff. 3.3.3. (S. 32).
157 Rohe, Netzverträge, S. 389.
158 Elfring, NZG 2012, 895; Khalilzadeh, GmbHR 2013, 232, 233.
159 Elfring, NZG 2012, 895; Khalilzadeh, GmbHR 2013, 232.

Equity Joint Ventures kommen typischerweise für längerfristige, über einzelne Projekte hinausgehende Kooperationen zum Einsatz. In diesen Fällen wird regelmäßig bewusst eine Gesellschaft, meist in Form einer Kapitalgesellschaft, gegründet.

Contractual Joint Ventures liegen regelmäßig bei projektbezogenen Kooperationen, in der Industrie etwa der Abgabe eines Angebots zur gemeinsamen Durchführung eines Auftrags (z. B. Errichtung eines Bauwerks) vor und sind zumeist auf eine begrenzte Zeit ausgerichtet.[160] Dabei kann sich eine formale Gesellschaftsgründung, etwa zur Durchführung eines Auftrags, anschließen.

Bei Contractual Joint Ventures, wie generell bei der Bildung von Konsortien zur Durchführung eines Projekts, wird neben schuldrechtlichen Beziehungen zwischen den Beteiligten auch eine Gesellschaft, aus deutscher Sicht regelmäßig eine BGB-Gesellschaft, gegründet. [161]

Bei der netzförmigen Kooperation im Rahmen von I4.0 kommt es entscheidend darauf an, ob mehrseitige Rechtsbeziehungen beschlossen werden. Dabei ist zwischen der Lieferbeziehung und der Kooperationsbeziehung bzw. zwischen dem Lieferelement und dem Kooperationselement eines Vertrags zu differenzieren.

In Bezug auf das Kooperationselement können mehrseitige Verträge, auch konkludent (ohne ausdrückliche Vereinbarung) geschlossen werden. Soweit das mehrseitige Kooperationsverhältnis eine gemeinsame Willensbildung vorsieht, wird dieses Verhältnis als Gesellschaft zu qualifizieren sein. Denkbar ist aber auch, dass lediglich Schutzpflichten gegenüber allen Beteiligten übernommen werden. In diesem Fall bestehen lediglich schuldrechtliche Beziehungen.

Bei einer gesellschaftsrechtlichen Beziehung ist die Kooperation, soweit nicht formal eine Gesellschaft (z. B. eine GmbH) gegründet wird, aus Sicht des deutschen Gesellschaftsrechts regelmäßig als BGB-Gesellschaft einzuordnen, die auch formlos geschlossen werden kann.

Soweit die Kooperationsbeziehung der I4.0 schuldrechtlicher Art ist, können unterschiedliche Vertragsarten von Bedeutung sein. Dabei ist zu berücksichtigten, dass, insbesondere bei der sternförmigen Struktur, zwischen dem zentralen Beteiligten und den übrigen Beteiligten, typischerweise Lieferbeziehungen bestehen, die auf Kauf-, Werk-, Werklieferungs-, Dienstverträgen oder gemischten Verträgen beruhen. In diesen Fällen werden die Lieferverträge durch Nebenpflichten zu den spezifischen Aspekten der Kooperation in der I4.0 erweitert. Alternativ kann neben der Lieferbeziehung auch ein separater Kooperationsvertrag geschlossen werden, etwa in Form eines Rahmenvertrags, in den die Kooperationsaspekte aufgenommen sind.

Unabhängig von der konkreten Ausgestaltung der Lieferbeziehung besteht damit jedenfalls zwischen dem Hauptpartner und den übrigen Beteiligten eine vertragliche Beziehung, die die kooperationsbezogenen Pflichten beider Partner begründet.

Auch bei einer netzförmigen Kooperation ist zwischen dem Lieferelement und dem Kooperationselement zu differenzieren. Wie dargestellt, ist bei der netzförmigen Kooperation das Kooperationselement oft in Form einer Gesellschaft ausgestaltet. Auch bei multilateralen Kooperationsbeziehungen kann aber, wie dargestellt, das Kooperationselement schuldrechtlich ausgestaltet sein.

4.4.2.2 Anwendbares Recht

Für die Pflichten der Beteiligten in Bezug auf IT-Sicherheit und ihre Haftung kommt es wesentlich darauf an, welchem Recht die Kooperationsbeziehung unterliegt. Für die Bestimmung des hierauf anwendbaren Rechts kommt es darauf an, ob die Kooperation schuldvertraglich oder gesellschaftsvertraglich ausgestaltet ist (dazu oben 4.4.1.1).

Bei Schuldverträgen (schuldvertragliche Gestaltung der Kooperation) richtet sich das anwendbare Recht nach der Rom I–VO, die den Vertragsparteien die Möglichkeit der freien Rechtswahl bietet (dazu oben 4.4.1.2). Soweit die Kooperationspartner davon Gebrauch machen, unterliegt der Vertrag dem gewählten Recht (dazu oben 4.4.1.2).

Haben die Parteien keine Rechtswahl getroffen, richtet sich das auf Schuldverträge anwendbare Recht nach Art. 4 Rom I–VO (siehe dazu oben 4.4.1.2). Im Rahmen des Art. 4 Rom I–VO ist nach der Vertragsstruktur und der Vertragsart bzw. Leistungsbeziehung zu unterscheiden. Dabei ist danach zu differenzieren, ob ein selbständiger Kooperationsvertrag geschlossen wurde oder ob die Kooperation als Neben-

160 Khalilzadeh, GmbHR 2013, 232, 233; Wirbel, in Münchener Handbuch des Gesellschaftsrechts, Bd. 1, § 28 Rn. 2.
161 Khalilzadeh, GmbHR 2013, 232, 233; Wirbel, in Münchener Handbuch des Gesellschaftsrechts, Bd. 1, § 28 Rn. 2

pflicht des Liefervertrags ausgestaltet ist. Selbständige Kooperationsverträge lassen sich keinem der in Art. 4 Abs. 1 Rom I–VO aufgeführten Verträge zuordnen. Nach Art. 4 Abs. 2 Rom I–VO unterliegt der Vertrag somit grundsätzlich dem Recht des Staates, in welchem die Partei, die die für den Vertrag charakteristische Leistung erbracht hat, ihren gewöhnlichen Aufenthalt hat. Die Ermittlung der charakteristischen Leistung wird bei dem Kooperationsvertrag, wie oben dargestellt, häufig nicht möglich sein.[162] In diesem Fall richtet sich das anwendbare Recht nach Art. 4 Abs. 4 Rom I–VO. Der Vertrag unterliegt somit dem Recht des Staates, zu dem er die engste Verbindung aufweist. Die engste Verbindung ist anhand einer Abwägung der Umstände des Einzelfalls und der kollisionsrechtlichen Interessen der Parteien zu ermitteln.[163] In der Regel wird der Schwerpunkt des Vertrags auf Seiten des Hauptpartners liegen, bei dem die zweiseitigen Verträge mit den Partnern zusammenlaufen. Art. 4 Abs. 4 Rom I–VO führt daher zur Anwendung des Rechts des Hauptpartners.

Soweit das Kooperationselement dagegen als Nebenpflicht in einen Liefervertrag einbezogen ist, lässt sich der Vertrag typischerweise einem der in Art. 4 Abs. 1 Rom I–VO aufgeführten Verträge zuordnen. Bei einem Kaufvertrag wäre danach gemäß Art. 4 Abs. 1 lit. a Rom I–VO das Recht anwendbar, in dem der Verkäufer seinen gewöhnlichen Aufenthalt hat. Bei juristischen Personen ist der Ort des gewöhnlichen Aufenthalts nach Art. 19 Abs. 1 S. 1 Rom I–VO der Ort ihrer Hauptverwaltung. Wenn der Lieferant seine Hauptverwaltung also im Ausland hätte und der Hauptpartner im Inland, wäre ausländisches Recht anwendbar. Es stellt sich jedoch die Frage, ob nicht eine offensichtlich engere Beziehung gem. Art. 4 Abs. 3 Rom I–VO zum Recht des Staates, in dem der Hauptpartner seine Hauptverwaltung hat, gegeben ist. Dies wird in einigen Fällen, aber nicht durchgehend der Fall sein und hängt sehr vom Einzelfall ab. Wenn etwa ein ausländischer Rohstofflieferant aufgrund einer just-in-time-Lieferbeziehung in ein I4.0-System eingebunden ist, besteht nicht schon wegen etwaiger Nebenpflichten in Bezug auf die Nutzung der Kooperation eine wesentlich engere Beziehung zum Hauptpartner.

Dies lässt sich am Fallbeispiel „Logistik“ verdeutlichen: Wenn der Produzent von Wellpappe im Inland ansässig ist, ein Lieferant von Rohstoffen aber im Ausland, so weist Art. 4 Rom I–VO auf das Recht des Lieferanten. Die Einbindung in eine Industrie 4.0-Kooperation wie dieser führt in Bezug auf die Lieferbeziehung nicht zu einer wesentlich engeren Verbindung mit dem Inland.

Dies führt dazu, dass insbesondere bei sternförmigen internationalen Kooperationen in der I4.0 die objektive Anknüpfung nach Art. 4 Rom I–VO regelmäßig zur Anwendbarkeit unterschiedlicher Rechtsordnungen auf die einzelnen Vertragsbeziehungen führt.

Sowohl die Rechtswahl nach Art. 3 Rom I–VO, insbesondere aber die objektive Anknüpfung nach Art. 4 Rom IVO können somit dazu führen, dass kooperationsbezogene Pflichten der Beteiligten unterschiedlichen Rechtsordnungen unterliegen.

Dies kann zu erheblichen Problemen führen. Daher sollte versucht werden, die kooperationsbezogenen Elemente möglichst aller Beziehungen im Wege der Rechtswahl einer einheitlichen Rechtsordnung zu unterwerfen. Neben materiellen Gesichtspunkten (dazu unten 4.4.2.3) spricht auch dies dafür, die kooperationsbezogenen Pflichten der Beteiligten in einer separaten Vereinbarung zu regeln.

Bei gesellschaftsrechtlichen Verbindungen ist das anwendbare Recht nach den – gesetzlich nicht ausdrücklich geregelten – Regeln des internationalen Gesellschaftsrechts zu ermitteln. Danach ist zu differenzieren, ob eine Gesellschaft nach dem Recht eines EU-Mitgliedsstaats wirksam gegründet wurde, da dann die Niederlassungsfreiheit zu beachten ist.[164] Diese Feststellung kann Schwierigkeiten bereiten, wenn keine formale Gesellschaftsgründung erfolgt, sondern, wie dargestellt, eine Kooperationsform gewählt wird, die aus deutscher Sicht eine BGB-Gesellschaft begründet. Wenn man zur Vereinfachung annimmt, dass die Kooperation ihren Schwerpunkt bei einem in Deutschland ansässigen Partner hat, ist deutsches Gesellschaftsrecht maßgeblich[165] und ist die Kooperation als BGB-Gesellschaft einzuordnen.

162 So ist die Anknüpfung nach Art. 4 Abs. 4 Rom I–VO etwa auch beim Joint Venture Vertrag maßgeblich, Ferrari, in Ferrari/Kieninger/Mankowski [u.a.], Art. 4 Rom I–VO Rn. 80.
163 Martiny in MüKo, Art. 4 Rom I–VO Rn. 311 ff.
164 Siehe dazu im Einzelnen Spahlinger, in Spahlinger/Wegen, Internationales Gesellschaftsrecht, Rn. 135 ff.
165 Vgl. Spahlinger, in Spahlinger/Wegen, Internationales Gesellschaftsrecht, Rn. 59 ff.

4.4.2.3 Schutzpflichten zur IT-Sicherheit in der Industrie 4.0

4.4.2.3.1 Überblick

In diesem Abschnitt wird untersucht, welche Schutzpflichten in Bezug auf IT-Sicherheit das vertragliche Kooperationsverhältnis in der I4.0 begründet. Da die Inhalte der Kooperation häufig nicht oder nur teilweise ausdrücklich geregelt sind, sind die Pflichten häufig im Wege der Vertragsauslegung mit Blick auf den Zweck der Kooperation zu ermitteln.

Typische Inhalte der Kooperationsbeziehung sind Rücksichtnahmepflichten, Informationspflichten und Mitwirkungspflichten der Beteiligten. Daneben finden sich auch Regelungen zur Haftung bei Pflichtverletzungen, z. B. in Form von Vertragsstrafen oder Haftungsbegrenzungen. Die Vertragsfreiheit erlaubt den Parteien, die Pflicht zur Sicherung der IT im Einzelnen zu regeln. Sinnvollerweise ist eine solche Regelung zu treffen, da die Kooperationspartner so detaillierte und bedarfsorientierte Lösungen finden können. Es stellt sich jedoch die Frage, welche Maßstäbe gelten, wenn die IT-Sicherheit vertraglich nicht oder nur lückenhaft geregelt wurde.

Hier sind vor allem Pflichten in Bezug auf die IT-Sicherheit von Interesse. Aufgrund der Vielzahl der möglichen Fallgestaltungen in der Praxis können diese hier nur exemplarisch untersucht werden. Im Zentrum der Untersuchung steht daher die Frage, in welchem Umfang vertragliche Pflichten der Beteiligten zur Sicherung der IT-Infrastruktur bestehen, also etwa, welche Schutzmaßnahmen die Beteiligten zur Sicherung ihrer Infrastruktur treffen müssen. So ist etwa im Fallbeispiel „Inbetriebnahme“ (oben 4.1.1, insb. 4.1.1.2) von Bedeutung, ob eine Pflicht zur Aufrechterhaltung einer Firewall bestand, die durch das Abschalten verletzt wurde.

Nachfolgend wird zunächst die rechtliche Grundlage der Pflicht zur Sicherung der technischen Infrastruktur (4.4.2.3.2) und sodann der Umfang der Schutzpflicht (4.4.2.3.3) untersucht.

4.4.2.3.2 Grundlage der Pflicht zur Vornahme von Schutzmaßnahmen

Zunächst stellt sich die Frage, ob die Kooperationspartner vertraglich verpflichtet sind, ihre IT zum Schutz ihrer Vertragspartner gegen Eingriffe Dritter zu sichern. Eine entsprechende Pflicht kann, auch wenn sie im Vertrag nicht ausdrücklich geregelt ist, in Form einer Nebenpflicht nach § 241 Abs. 2 BGB bestehen. Das Bestehen von Nebenpflichten ist abzuleiten aus der zwischen den Parteien bestehenden Interessenlage. Nebenpflichten bestehen umso eher, je mehr die Parteien auf eine vertrauensvolle Zusammenarbeit angewiesen sind.[166] Entscheidend sind dabei zum einen das Schutzbedürfnis des Vertragspartners und zum anderen die Zumutbarkeit der Sicherheitsmaßnahmen.

Eine vertragliche Pflicht zum Schutz der IT wird heute in Fällen, in denen Vertragspartner über elektronische Kommunikationsnetze Daten austauschen und mit Eingriffen Dritter zu rechnen ist, allgemein bejaht. Zwar ist die Diskussion bisher auf Einzelfälle beschränkt, überordnete Grundsätze sind bisher nicht formuliert worden. Es lässt sich aber feststellen, dass eine solche Schutzpflicht, in den Fällen, in denen sie diskutiert wird, jedenfalls dem Grunde nach bejaht wird.

So wird etwa im Online Banking angenommen, dass die Bank im Verhältnis zu ihren Kunden eine vertragliche Pflicht zum Schutz des Systems gegen Angriffe Dritter trifft.[167] Ebenso treffen aber auch den Kunden vertragliche Pflichten zugunsten der Bank zum Schutz seiner eigenen IT.[168] Diese Pflicht ist – seit 2009 – im Giroverhältnis in § 675l BGB teilweise ausdrücklich gesetzlich geregelt.

In Bezug auf die vertraglichen Schutzpflichten von Internetnutzern wurde in einer aktuellen Dissertation[169] aufgezeigt, dass sich aus der Vertragsbeziehung, sei es ein Vertrag über die Nutzung des Online Banking, sei es ein Vertrag über die Nutzung eines Online Shops oder sonst eines Dienstes im WWW, regelmäßig eine vertragliche Pflicht des Internetnutzers zum Schutz seiner eigenen IT gegen Eingriffe Dritter ergibt. Diese Pflicht ergibt sich, soweit sie

166 Sutschet, in BeckOK BGB, § 241 Rn. 44.

167 LG Nürnberg-Fürth, 28.04.2008 – 10 O 11391/07, BeckRS 2008, 26304; Borges/Schwenk/Stuckenberg/Wegener, Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 296 f.; Borges, Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis, 2011, S. 201 f.; Karper, DuD 2006, 353, 357; Kind/Werner, CR 2006, 353, 357 f.; Recknagel, Vertrag und Haftung im Online Banking, 2005, S. 206; Schulte am Hülse/Klabunde, MMR 2010, 84, 87. Zu BTX: Reiser, WM 1986, 1401, 1403.

168 LG Nürnberg-Fürth, 28.04.2008 - 10 O 11391/07, BeckRS 2008, 26304; AG Wiesloch, CR 2008, 600, 602; Borges/Schwenk/Stuckenberg/Wegener, Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 284 f.; Borges, Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis, 2011, S. 160 f; Maihold, in Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, § 55 Rn. 134 ff; Mühlenbrock/Dienstbach, MMR 2008, 630, 631; Schulte am Hülse/Klabunde, MMR 2010, 84, 87; Spindler, MMR 2008, 7, 10; Werner, K&R 2008, 554, 555.

169 Hossenfelder, Pflichten zur Abwehr von Malware und Phishing in Sonderverbindungen, 2013.

nicht ausdrücklich geregelt ist, gemäß § 241 BGB als vertragliche Nebenpflicht aus dem Vertragsverhältnis.[170]

Eine Pflicht von Unternehmen zum Schutz ihrer eigenen IT zugunsten ihrer Vertragspartner, wird durchgängig bejaht.[171] Auch hier ergibt sich die Pflicht, soweit nicht speziell geregelt, als vertragliche Nebenpflicht aus § 241 BGB.[172]

Vertragliche Schutzpflichten ergeben sich nicht zuletzt dadurch, dass Vertragspartner regelmäßig verpflichtet sind, gesetzliche Schutzpflichten, etwa aus Datenschutzrecht, oder aus Verkehrspflichten, zu wahren. Damit wird die gesetzliche Schutzpflicht auch als vertragliche Schutzpflicht in das Vertragsverhältnis einbezogen.

Als Zwischenergebnis ist festzuhalten, dass Vertragspartner beider Seiten, also sowohl des Anbieters eines Dienstes, also auch dessen Kunden, soweit sie über Internet kommunizieren, vertragliche Schutzpflichten zum Schutz ihrer technischen Infrastruktur gegen Eingriffe Dritter zugunsten ihrer Vertragspartner treffen.

Im Rahmen der Zusammenarbeit in der I4.0 bestehen folglich auf Seiten aller Beteiligten vertragliche Schutzpflichten zugunsten der jeweiligen Vertragspartner.[173]

4.4.2.3.3 Umfang der Sicherungspflichten

Der Umfang der vertraglichen Sicherungspflicht bestimmt sich, entsprechend dem Maßstab des § 241 BGB, nach der Erforderlichkeit und der Zumutbarkeit der jeweiligen Schutzmaßnahme. Es ist also für jede in Betracht kommende Maßnahme im ersten Schritt zu prüfen, ob diese für das erstrebte Schutzziel – hier: Abwehr von Eingriffen Unbefugter – geeignet und erforderlich ist, und ob sie dem Verpflichteten zumutbar ist.

Bei dieser Abwägung ist auf Seiten der Geeignetheit und Erforderlichkeit der Maßnahme das Schutzbedürfnis des Vertragspartners von Bedeutung. Dies ist wiederum anhand einer Vielzahl von Faktoren zu ermitteln, die sich in zwei Gruppen zusammenfassen lassen. Zum einen ist das Schutzgut zu berücksichtigen, also etwa die Schadenshöhe im Fall eines Eingriffs, und zum anderen ist die Wahrscheinlichkeit eines Eingriffs von Bedeutung.

Im Rahmen der I4.0 kommt es also darauf an, welche Schäden durch einen Eingriff erfolgen können. Diese können, wie der vom BSI aufgezeigte Fall des Angriffs auf ein Stahlwerk belegt, sehr hoch sein. Weiterhin kommt es darauf an, ob Angriffe, oder ein spezifischer Angriff, gegen den sich eine bestimmte Schutzmaßnahme richten soll, wahrscheinlich ist, oder aber, als entgegengesetztes Extrem, lediglich theoretisch möglich erscheint.

Aus diesen Grundsätzen folgt, dass die Anforderungen an vertragliche Schutzpflichten ganz einzelfallbezogen sind. Es ist also auch im Rahmen der I4.0 jeweils im Einzelfall zu ermitteln, welche technischen Schutzmaßnahmen geboten sind.

Es haben sich gleichwohl für Einzelfragen in der Diskussion Ergebnisse ergeben, die auch für I4.0 herangezogen wurden.

So ist etwa anerkannt, dass jeder – auch private – Internet-Nutzer verpflichtet ist, seine Rechner durch aktuellen Malwareschutz zu sichern. Auch bei privaten Internetnutzer ist anerkannt, dass jedenfalls eine vorinstallierte Firewall nicht deaktiviert werden darf.

Für Unternehmen zählt der Schutz der IT durch eine Firewall zu der grundlegenden Sicherheitsmaßnahme, die stets erforderlich und zumutbar sein wird. Entsprechend besteht eine vertragliche Nebenpflicht der Beteiligten zur Unterhaltung einer Firewall. Das Abschalten der Firewall, wie im Beispiel „Inbetriebnahme“ (oben 4.1.1.2) beschrieben, ist damit grundsätzlich eine Verletzung dieser Pflicht. Es kann zwar im Einzelfall geboten sein, eine Firewall vorübergehend abzuschalten, etwa wenn eine durch die Firewall verursachte technische Störung nicht anders behoben werden kann.

Das Beispiel zeigt die typische Interessenkollision in Bezug auf IT-Sicherheit auf. Der grundsätzlich gebotenen Schutzmaßnahme – Betrieb der Firewall – steht ein erhebliches, ebenfalls schützenswertes, Interesse, die Einsatzfähigkeit eines Produktionsbetriebs, gegenüber. Hier ist im Rahmen der Zumutbarkeit der Maßnahme abzuwägen.

170 Hossenfelder, Pflichten zur Abwehr von Malware und Phishing in Sonderverbindungen, 2013, insb. S. 285 f.
171 Beucher/Uzerath, MMR 2013, 362, 367; Borges, Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis, 2011, S 201 betr. Pflichten von Diensteanbietern im Internet; Heckmann, MMR 2006, 280, 281. Abstellend auf den Einzelfall Roth/Schneider, ITRB 2005, 19, 20.
172 Beucher/Uzerath, MMR 2013, 362, 367; Borges, a.a.O., S. 201; Roth/Schneider, ITRB 2005, 19, 20.
173 Inwieweit Dritte, etwa andere Beteiligte, in den Schutzbereich einbezogen sind, kann im Rahmen dieser Untersuchung nicht erörtert werden.

Durch die Kooperation in der I4.0 tritt hier aber eine Situation auf, die bei klassischen Produktionsbetrieben nicht bestand. Soweit nämlich lediglich der eigene Betrieb gefährdet ist, konnte die Entscheidung über den Verzicht auf eine Schutzmaßnahme unter Betrachtung lediglich der eigenen Vor- und Nachteile getroffen werden. Soweit aber, wie in der I4.0 typisch, Dritte betroffen sein können, sind auch deren Schutzinteressen zu berücksichtigten. Daher wäre das Abschalten einer Firewall über einen längeren Zeitraum, jedenfalls ohne alternative Schutzmaßnahmen, im Ergebnis wohl stets pflichtwidrig.

Einen Schwerpunkt der Diskussion zu den Anforderungen an IT-Sicherheit liegt, im Hinblick auf Identitätsmissbrauch im Internet, bei den Anforderungen an Authentisierungssysteme. Diese haben auch in der I4.0 größte Bedeutung, da die Steuerung der Systeme durch Authentisierungsmittel wie Passwörter abgesichert wird.

In der rechtlichen Diskussion dieser Frage nimmt das Online Banking eine besondere Stellung ein. Hier ist anerkannt, dass Banken vertraglich verpflichtet sind, zugunsten ihrer Kunden hinreichend sichere Authentisierungssysteme vorzuhalten.[174]

Allerdings ist durchaus umstritten, welche Anforderungen zu stellen sind, insbesondere, welches Maß an technischer Sicherheit geboten ist. So hat etwa das Kammergericht im Jahr 2010 entschieden, dass die Verwendung des klassischen PIN/TAN-Verfahrens durch eine Bank im Jahr, bei dem eine beliebige TAN aus einer Liste verwendet werden konnte, wegen der Gefahr von Phishing pflichtwidrig sei.[175] Das Gericht führte aus, dass das alte Verfahren bei einer Mehrzahl der Kreditinstitute nicht mehr im Einsatz sei und ein geringeres Schutzniveau als das neuere iTAN-Verfahren biete.[176] Unbeachtlich sei der Einwand, auch das iTAN-Verfahren könne mit entsprechenden Angriffen überwunden werden. Entscheidend sei, dass das neue System eine höhere Sicherheit bot und die Gefahr eines Angriffs verringere.[177]

Der Bundesgerichtshof hat zur Frage, ob das iTAN-Verfahren, das ebenfalls recht leicht überwunden werden kann, hinreichend sicher ist, in seinem Grundsatzurteil von 2012 zum Identitätsmissbrauch im Online Banking nicht entschieden.[178] Dabei ist aber zu berücksichtigen, dass sich der BGH auf einen Sachverhalt aus dem Jahr 2008 bezog.[179]

Entsprechende vertragliche Pflichten werden auch in anderen Bereichen angenommen. So ist etwa auch der Betreiber eines Internet-Auktionshauses verpflichtet, seine Plattform hinreichend abzusichern.[180] Ob die Authentisierung durch Nutzername und Passwort dieser Pflicht genügt, ist bisher jedoch nicht geklärt. Aufgrund des hohen Missbrauchsrisikos wird eine solche Pflicht aber künftig wohl anzunehmen sein, sofern sich insoweit keine neue Situation ergibt.[181]

Als Zwischenergebnis zum Umfang der Schutzpflichten lässt sich festhalten, dass bei Vertragsverhältnissen, in denen Vertragspartner über Internet kommunizieren, regelmäßig vertragliche Nebenpflichten zum Schutz ihrer technischen Systeme gegen Eingriffe Dritter treffen. Hinsichtlich des gebotenen Umfangs der Schutzmaßnahmen besteht weitgehend Einigkeit darin, dass ein angemessener Schutz erforderlich ist. Jedoch besteht erhebliche Rechtsunsicherheit darin, welche Maßnahmen im konkreten Fall als angemessen anzusehen sind. Darüber hinaus ist auch nicht geklärt, nach welchen Kriterien die Angemessenheit zu bestimmen ist.

4.4.3 Aspekte des Haftungsrechts

4.4.3.1 Gegenstand der Untersuchung

In diesem Abschnitt werden wichtige Aspekte der Haftung aufgrund gesetzlicher Normen untersucht. Auch hier muss die Untersuchung exemplarisch erfolgen. Daher werden die allgemeinen Haftungsnormen betrachtet, die im deutschen Recht im Deliktsrecht des BGB, den §§ 823 ff. BGB, geregelt sind. Weitere Haftungsnormen sind etwa im Datenschutzrecht und im Immaterialgüterrecht enthalten.

174 LG Düsseldorf, 19.1.2011, 23 S 163/10, BeckRS 2012, 10192; KG, MMR 2011, 338, 339; Borges/Schwenk/Stuckenberg/Wegener, Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 296 f.; Borges, Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis, 2011, S. 201 f.; Kind/Werner, CR 2006, 353, 357 f.; Schulte am Hülse/Klabunde, MMR 2010, 84, 88.

175 KG, MMR 2011, 338, 339

176 KG, MMR 2011, 338, 339 f.

177 KG, MMR 2011, 338, 339 f.

178 Der BGH weist darauf hin, die Revision habe die Feststellung des Berufungsgerichts, die Bank habe mit dem iTAN-Verfahren im Jahr 2008 ihrer Pficht zur Verwendung eines hinreichend sicheren Systems nachgekommen, nicht angegriffen., MMR 2012, 484, 486 Rn. 31.

179 BGH, MMR 2012, 484, 486 Rn. 31.

180 Borges, in Borges, Rechtsfragen der Internetauktion (2. Aufl.), S. 403. Zur Pflicht des Betreibers zur Verhinderung von Namensverletzungen auch BGH, NJW 2008, 3714, 3715 – Namensklau im Internet.

181 Borges, in Borges, Rechtsfragen der Internetauktion (2. Aufl.), S. 403.

In der I4.0 können, wie oben (4.4.1.2) dargestellt, ganz unterschiedliche Szenarien zu Schäden bei Beteiligten und Dritten führen. Für die Pflichten und Haftung nach deliktischen Normen sind vor allem Schadensszenarien von Interesse, bei denen Dritte, die dem Verursacher nicht vertraglich verbunden sind, geschädigt werden. Daher werden der Untersuchung in diesem Abschnitt folgende Fallgruppen zugrunde gelegt.

- Schäden bei einem unbeteiligtem Dritten, ausgelöst durch fehlerhafte Daten eines Partners;
- Schaden an Daten durch Eingriff eines Partners, etwa durch versehentliche Veränderung oder Löschung wertvoller Daten;
- Schäden durch Eingriff eines unbekannten Dritten, welcher durch einen Sicherheitsmangel eines Partners ermöglicht wurde.

Im Folgenden wird zunächst dargestellt, welches Haftungsrecht bei der internationalen Kooperation in der I4.0 anwendbar ist.

4.4.3.2 Anwendbares Recht

Das anwendbare Deliktsrecht bestimmt sich, wie oben (3.3.2.1) dargestellt, nach der Rom II–VO. Danach richtet sich das anwendbare Deliktsrecht bei internationalen Sachverhalten nach dem Recht des Staates, in dem der Schaden eingetreten ist, also dem Erfolgsort, soweit nicht beide Parteien zum Zeitpunkt des schädigenden Ereignisses ihren gewöhnlichen Aufenthaltsort in demselben Staat hatten oder eine offensichtlich engere Verbindung zum Recht eines anderen Staates besteht oder ein Recht gewählt wurde.[182] Die Ermittlung des anwendbaren Rechts wird im Folgenden für die drei oben genannten Schadensszenarien dargestellt.

4.4.3.2.1 Anwendbares Recht bei Verletzung Unbeteiligter

Bei der Verletzung unbeteiligter Dritter ist der Erfolgsort der entscheidende Anknüpfungspunkt. In der Regel ist somit gemäß Art. 4 Abs. 1 Rom II–VO das Recht desjenigen Staates anwendbar, in welchem der Schaden des Dritten eingetreten ist, also in welchem Staat der Dritte verletzt wurde. Wird beispielsweise ein Auto mit defekter Bremsanlage in Deutschland verkauft, es kommt aber zu einem Unfall in Polen, liegt der Erfolgsort in Polen und polnisches Recht ist anwendbar.

Eine Rechtswahl ist in dieser Fallgruppe nur sehr eingeschränkt möglich. Eine zwischen den Kooperationspartnern getroffene Rechtswahl kann einen unbeteiligten Dritten, wie Art. 14 Abs. 1 S. 2 Rom II–VO klarstellt, nicht binden. Eine Rechtswahl im Verhältnis zu Geschädigten, zu denen keine vorherige Vertragsbeziehung besteht, kommt allenfalls im Einzelfall in Betracht.

4.4.3.2.2 Anwendbares Recht bei Datenveränderung

Im Falle der versehentlichen Datenveränderung oder Datenlöschung durch einen Partner ist der nach Art. 4 Abs. 1 Rom II–VO maßgebliche Erfolgsort derjenige Ort, an welchem die Daten verändert bzw. gelöscht werden. Der Erfolgsort wird in dieser Fallkonstellation beim Belegenheitsort des Servers gesehen, auf dem die Daten im Zeitpunkt der Schädigung gespeichert waren.[183]

Regelmäßig wird sich in dieser Fallgruppe jedoch die Frage stellen, ob gem. Art. 4 Abs. 3 Rom II–VO eine offensichtlich engere Verbindung zum Recht eines anderen Staates besteht. Dies kommt auf den Einzelfall an.

Wenn Daten eines Beteiligten geschädigt sind, wird es häufig zur akzessorischen Anknüpfung an das Vertragsstatut kommen. Nach Art. 4 Abs. 3 S. 2 Rom II–VO, kann sich eine offensichtlich engere Verbindung insbesondere aus einem bereits bestehenden Rechtsverhältnis zwischen den Parteien ergeben, welches mit der betreffenden unerlaubten Handlung in enger Verbindung steht.[184] Ein sachlicher Zusammenhang zwischen dem Rechtsverhältnis und der unerlaubten Handlung besteht etwa, wenn durch die unerlaubte Handlung Pflichten aus dem Rechtsverhältnis verletzt wurden.[185]

182 Siehe dazu oben 3.3.2.1.
183 Vgl. Intveen/Hilber/Rabus, in Hilber (Hrsg.): Handbuch Cloud Computing, Teil 2 Rn. 180; Nordmeier, MMR 2010, 151, 154; Stögmöller, in Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 6 Rn 362.
184 Siehe dazu auch oben 3.3.2.1.
185 Hohloch, in Erman, Art. 4 Rom II–VO, Rn. 17a; Junker, in MüKo, Art. 4 Rom II–VO Rn. 52.

Soweit ein Vertragsverhältnis zwischen Geschädigtem und Schädiger besteht, wie es bei einer Netzstruktur[186] regelmäßig der Fall ist, verstößt die Datenveränderung regelmäßig gegen Pflichten aus dem zugrundeliegenden schuldrechtlichen oder gesellschaftsrechtlichen Verträgen, so dass gemäß Art. 4 Abs. 3 S. 2 Rom II–VO eine akzessorische Anknüpfung an das Statut der Kooperationsvereinbarung erfolgt.

Bei einer sternförmigen Kooperation[187] wird zwischen Schädiger und Geschädigtem oft kein Vertragsverhältnis vorliegen. Allerdings wird gleichwohl meist eine offensichtlich engere Verbindung i.S. des Art. 4 Abs. 3 S. 1 Rom II–VO mit dem Recht des Staates vorliegen, dem die Kooperationsvereinbarung unterliegt, da beide Parteien mit dem zentralen Partner vertraglich verbunden sind. Wenn darüber hinaus gegen eine Pflicht aus dem Vertrag verstoßen wird, spricht dies zusätzlich für das Vorliegen einer engeren Verbindung.

Soweit zwischen Schädiger und Geschädigtem eine vertragliche Beziehung vorliegt, kann hierin auch eine vorherige Rechtswahl für die deliktische Haftung vorgenommen werden. Da ein kollisionsrechtlicher Gleichlauf von vertraglicher und deliktischer Haftung erwünscht ist, ist eine Rechtswahl regelmäßig empfehlenswert.

4.4.3.2.3 Anwendbares Recht bei mangelhafter Schutzmaßnahme

Bei der Haftung eines Partners aufgrund einer unterlassenen oder mangelhaften Schutzmaßnahme ist nach Art. 4 Abs. 1 Rom II–VO der maßgebliche Erfolgsort zu ermitteln. Dieser ist dort belegen, wo letztlich das Schutzgut verletzt wird und nicht etwa dort, wo die Schutzmaßnahme unterlassen wird.

Der Erfolgsort hängt damit entscheidend davon ab, wo das verletzte Schutzgut zum Zeitpunkt der Schädigung belegen ist. Soweit Datenverarbeitungssysteme (Hardware, Software) geschädigt werden, ist der Lageort der jeweiligen Hardware maßgeblich. Bei der Löschung oder Veränderung von Daten kommt es, wie oben dargestellt, auf den Lageort des Rechners an, auf dem die Daten gespeichert sind. Wenn beispielsweise ein Angriff auf Daten erfolgt, die in Deutschland gehostet waren, ist deutsches Recht auch auf die Haftung eines französischen Partners wegen einer unterlassenen Schutzmaßnahme anwendbar. Waren die gleichen Daten in China gehostet, führt die Rom II–VO zur Anwendung chinesischen Rechts.

Auch in dieser Fallgruppe wird, genauso wie in der Fallgruppe der Datenveränderung durch aktives Tun eines Kooperationspartners, regelmäßig eine engere Verbindung zu dem Recht bestehen, dem die Kooperationsbeziehung unterliegt. Auch hier ist eine Rechtswahl nach Art. 14 Rom II–VO möglich und empfehlenswert.

4.4.3.3 Gesetzliche Schutzpflichten der Kooperationspartner

4.4.3.3.1 Grundlagen

Nach deutschem Recht können sich gesetzliche Verhaltenspflichten und eine Haftung der Kooperationspartner bei Pflichtverletzung aus einer Vielzahl unterschiedlicher Normen ergeben.

Eine Haftung nach dem allgemeinen Deliktsrecht des BGB ergibt sich zum einen nach der Generalklausel des § 823 Abs. 1 BGB, die im Wesentlichen die Verletzung eines durch § 823 Abs. 1 BGB geschützten Rechtsguts sowie die Verletzung einer gegenüber jedermann bestehenden Verhaltenspflicht voraussetzt. Eine solche Pflichtverletzung kann sowohl in einem positiven Verstoß gegen ein Verhaltensgebot, etwa die aktive Zerstörung eines Gegenstands, also auch im Unterlassen einer rechtlich gebotenen Handlung, etwa dem Unterlassen einer Schutzmaßnahme bestehen. Nicht zuletzt bei Schäden in der Informationstechnologie gehen die Verletzung durch aktives Tun und durch Unterlassen quasi übergangslos ineinander über.

Nach § 823 Abs. 2 BGB besteht eine Haftung auch bei Verletzung eines Schutzgesetzes. Im Unterschied zur Haftung nach § 823 Abs. 1 BGB kommt es hier nicht auf die Schädigung eines spezifischen Schutzguts an. Vielmehr ist jeglicher Schaden, auch der so genannte reine Vermögensschaden, ersatzfähig.

Die unzähligen und teilweise extrem komplexen und schwierigen Fragen der gesetzlichen Haftung im Zusammenhang mit IT können hier nur zu einem geringen Teil untersucht und bestenfalls skizziert werden.

186 Siehe dazu oben 4.4.1.1.
187 Siehe dazu oben 4.4.1.1.

In den oben (4.4.3.1) genannten Schadensszenarien sind zentrale Aspekte der Haftung in der I4.0 angesprochen. Daher werden die Haftungsaspekte nachfolgend anhand der Schadensszenarien dargestellt.

4.4.3.3.2 Pflichtverletzung bei Verletzung Dritter

Im ersten Schadensszenario, der Verletzung eines unbeteiligten Dritten aufgrund Verwendung fehlerhafter Daten eines Partners, ist der Aspekt der Verantwortlichkeit aufgrund eines Beitrags, der mittelbar zu einem Schaden führt, angesprochen.

In einer solchen Situation wird sich der Dritte meist zunächst an den Beteiligten halten, mit dem er unmittelbar Kontakt hat. In der Praxis wird es daher meist um einen Regress zwischen den Kooperationspartnern gehen. Gleichwohl ist von Interesse, ob und unter welchen Voraussetzungen eine deliktische Verantwortung des Beteiligten in Betracht kommt, von dem das Datenmaterial stammt.

Die Verletzung eines geschützten Rechtsguts i.S.d. § 823 Abs. 1 BGB, etwa Gesundheit oder Eigentum, wird in diesen Fällen meist vorliegen.[188] Entscheidend ist, ob die Schädigung dem Urheber der Daten zugerechnet werden kann. Bei mittelbarer Verursachung von Schäden ist anerkannt, dass eine Zurechnung nur in Betracht kommt, wenn eine Pflicht bestand, die Verletzungsgefahr zu vermeiden.[189] Dabei ist im Rahmen des § 823 Abs. 1 BGB ausschließlich der Verstoß gegen eine gegenüber jedermann bestehende Verhaltensflicht (Verkehrspflicht) maßgeblich. Die dogmatische Einordnung von Verkehrspflichten ist umstritten. So werden sie etwa der objektiven Zurechnung[190] oder der Rechtswidrigkeit[191] zugeordnet oder gar als Schutzgesetz i.S.d. § 823 Abs. 2 BGB[192] gesehen. Für die hier interessierenden Fragen ist die dogmatische Zuordnung jedoch unerheblich.

Die Haftung nach § 823 Abs. 1 BGB wegen Verletzung einer Verkehrspflicht kann auch im Fall einer mittelbaren Schädigung bestehen. Maßgeblich ist allein, ob eine deliktische, d.h. gegenüber jedermann bestehende Pflicht zur Vermeidung der Schädigung bestand. Die Verkehrspflichten, die mit der Sorgfaltspflicht i.S.d. § 276 BGB der Sache nach identisch sind,[193] sind aufgrund einer Interessenabwägung zwischen dem Schutzinteresse des (potentiell) Geschädigten und der Zumutbarkeit der Verhaltens für den (potentiellen) Schädiger abzuwägen. Unter dem Gesichtspunkt der Zumutbarkeit ist daher von Bedeutung, welcher Aufwand von den Kooperationspartnern zur Vermeidung fehlerhafter Daten verlangt werden kann. Dies beurteilt sich nach dem von den Daten ausgehendem Gefahrenpotential. Je größer die potentiellen Gefahren für Rechtsgüter Dritter, desto größerer Aufwand muss betrieben werden, um Fehler zu vermeiden. Werden etwa Bremsanlagen hergestellt, die im Falle ihres Versagens Leib und Leben einer unbestimmten Anzahl an Menschen gefährden, sind sehr hohe Anforderungen zu stellen.

4.4.3.4 Pflichtverletzung bei Datenveränderung

Soweit in der I4.0 durch einen Kooperationspartner Daten eines anderen Partners gelöscht oder verändert werden, wird eine vertragliche Haftung im Vordergrund stehen, soweit zwischen dem Schädiger und dem Geschädigten eine Vertragsbeziehung besteht, wie es bei einer netzartigen Struktur der Kooperation der Fall ist. Insbesondere bei einer sternförmigen Struktur wird dies aber nicht stets der Fall sein, da es vorkommen kann, dass durch das Verhalten eines Zulieferers Datenmaterial eines anderen Zulieferers oder Abnehmers des zentralen Partners geschädigt wird. In einer solchen Konstellation hat die deliktische Haftung, die kein Vertragsverhältnis voraussetzt, besondere praktische Bedeutung.

Dieses Schadensszenario spricht die für I4.0 zentrale Frage an, inwieweit Datenmaterial ein Schutzgut des § 823 Abs. 1 BGB darstellt.

Nach verbreiteter Ansicht, stellt die Löschung von Daten typischerweise auch eine Verletzung des Eigentums am Datenträger dar.[194] Dies wird damit begründet, dass die

188 Bei Verletzung aufgrund von Produkten kommt auch eine Haftung nach dem Produkthaftungsgesetz (ProdHaftG) in Betracht, die auch den Produzenten eines Teilprodukts treffen kann (vgl. Wagner, in MüKo BGB, § 4 ProdHaftG Rn. 8).
189 Schiemann, in Erman, § 823 Rn. 77; Werner, Verkehrspflichten privater IT-Nutzer in Bezug auf die Vermeidung von Schadsoftware, S. 126.
190 Krause, in Soergel, § 823 Anh. II Rn. 14; Staudinger, in Schulze, § 823 Rn. 51.
191 Esser/Schmidt, AT/2, S. 69.
192 v. Bar, JZ 1979, 728, 730.
193 Wagner, in MüKo BGB, § 823 Rn. 311.
194 OLG Karlsruhe, NJW 1996, 200, 201; Jickeli/Stieper, in Staudinger, § 90 Rn. 19.

Löschung von Daten nicht ohne phylische Veränderung des entsprechenden Datenträgers selbst möglich ist.[195] Eine deliktische Haftung lässt sich nach dieser Ansicht jedoch nicht begründen, wenn der Eigentümer des Datenträgers und der zur Nutzung der Daten Berechtigte auseinanderfallen.[196] Diese Situation liegt typischerweise in Fällen des Cloud Computing vor, in denen der Cloud-Nutzer Daten auf Servern speichert, die im Eigentum des Cloud-Anbieters stehen.

Auch im Bereich der I4.0 ist denkbar, dass zur Produktion benötigte Daten auf fremden Servern gespeichert werden und somit ein auf einer Eigentumsverletzung am Datenträger basierender deliktischer Anspruch des „Datenberechtigten" ausgeschlossen ist.

Unter anderem um diese Lücken im Haftungssystem zu schließen, werden in der Literatur verschiedene Ansätze zur Annährung des Schutzes von Daten und Sachen diskutiert. Teilweise wird vertreten, dem „Datenberechtigten" stehe ein Besitzrecht an den Daten zu, dessen Verletzung Ansprüche nach § 823 Abs. 1 BGB auslöse.[197] Andere wenden dagegen die Vorschriften über Sachen bzw. das Eigentum auf Daten direkt[198] oder analog[199] an.

In diesem Zusammenhang wird häufig das ASP-Urteil des BGH[200] zitiert. In diesem Urteil hat der BGH bei der Beurteilung vertraglicher Ansprüche aus einem Vertrag über Bereitstellung von Softwareanwendungen (Application Service Providing (ASP)) die Auffassung vertreten, „dass eine auf einem Datenträger verkörperte Standardsoftware als bewegliche Sache anzusehen ist, auf die je nach der vereinbarten Überlassungsform Miet- oder Kaufrecht anwendbar ist".[201] Hieraus lässt sich für die hier interessierende Frage, ob Daten generell als Sachen im Sinne des § 823 Abs. 1 BGB als Sache anzusehen ist, nicht allzu viel herleiten, da es dem BGH um die Anwendung des Mietrechts auf ASP-Verträge, nicht um die Anwendung des § 823 Abs. 1 BGB auf Datenveränderung ging.

Teilweise wird in der Literatur auch ein Recht am eigenen Datenbestand als sonstiges Recht i. S. d. § 823 Abs. 1 BGB angesehen.[202] Für ein solches Recht spreche auch die Anerkennung des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme durch das BVerfG.[203]

Ein weiteres zentrales Problem bei Veränderung oder Löschung von Daten ist die Zuordnung des „Dateneigentums" oder des sonstigen Rechts an den Daten zu einer Person. Dateneigentümer soll nach einer Auffassung der Literatur derjenige sein, der den Skripturakt durchführt, also die Daten erstellt.[204] Dieser Aspekt wird bisher aber nicht näher diskutiert.

Soweit Daten verändert werden, die der Ersteller der Daten auf eigenen Rechnern speichert, wird man eine Eigentumsverletzung annehmen können. Allerdings sind die Fragen des ersatzfähigen Schadenumfangs bisher auch nicht geklärt.

Die Rechtsprechung hat sich zur Anwendung des § 823 Abs. 1 BGB auf Daten als solche, soweit erkennbar, bisher nicht geäußert. Die Rechtslage bleibt daher insoweit unklar.

4.4.3.5 Pflichtverletzung bei Sicherheitslücken

Das dritte Schadensszenario spricht eine der schwierigsten Fragen der Verantwortlichkeit für Schäden in der Informationstechnologie an, die insbesondere bei der Kooperation in der I4.0 von Bedeutung sein kann. Das Risiko von Schäden durch bewusste Eingriffe Dritter, die meist mit dem Stichwort „Hacking" zusammengefasst werden, trägt zunächst der jeweils unmittelbar Geschädigte, also derjenige dessen Systeme oder Daten geschädigt wurden. Im Fall des Angriffs gegen das Stahlwerk[205] wäre dies der Eigentümer des Hochofens und des Werkes, dessen Betrieb gestört wurde.

195 Jickeli/Stieper, in Staudinger, § 90 Rn. 19.
196 Jickeli/Stieper, in Staudinger, § 90 Rn. 19.
197 Spindler, ZGE 3 (2011), 129, 147.
198 Libertus, MMR 2005, 507, 508; Zu auf einem Datenträger verkörperten Computerprogrammen: Henssler, MDR 1993, 489, 490; Kloos/Wagner, CR 2002, 865, 866; König, NJW 1993, 3121, 3122; Marly, BB 1991, 432, 435; Sedlmeier/Kolk, MMR 2002, 75, 77.
199 Hoeren, MMR 2013, 486, 491.
200 BGH, NJW 2007, 2394.
201 BGH, NJW 2007, 2394, Rn. 15.
202 Schaub, in Prütting/Wegen/Weinreich, BGB, § 823 Rn 80; Spindler, in BeckOK BGB, § 823 Rn. 93.
203 Schaub, in Prütting/Wegen/Weinreich, BGB, § 823 Rn 80
204 Hoeren, MMR 2013, 486, 487 ff.
205 Siehe dazu oben 4.4.1.2.

Bei der I4.0 kommt aber das Spezifikum hinzu, dass der Angriff meist in mehreren Abschnitten geführt wird und dabei auch andere Beteiligte involviert werden. Im Fall des Angriffs gegen das Stahlwerk, bei dem der Angreifer zunächst einen Phishing-Angriff nutzt, um Zugriff auf die Bürosoftware zu erhalten, könnte im Zusammenhang mit der I4.0 ein solcher Angriff auch gegen einen Kooperationsbeteiligten erfolgen, so dass im zweiten Schritt über Systeme des betreffenden Kooperationsbeteiligten der eigentliche Angriff auf den Betreiber des Stahlwerks erfolgt. In diesem Fall stellt sich auch unter dem Gesichtspunkt einer deliktischen Haftung die Frage, ob der Kooperationsbeteiligte, der Opfer eines solchen Angriffs im Vorfeld wurde, seinerseits dem letztlich Geschädigten (im Beispiel: Betreiber des Stahlwerks) wegen seines mittelbaren Beitrags, etwa einer Sicherheitslücke, zum Schadensersatz verpflichtet ist. Auch hier wird häufig eine Haftung innerhalb von Vertragsverhältnissen im Vordergrund stehen. Daneben, oder, sofern keine vertragliche Beziehung bestand, ausschließlich, kann sich eine Haftung nach § 823 BGB ergeben. In diesem Fall kommt es darauf an, ob der Beteiligte eine Verkehrspflicht verletzt hat.

Die somit angesprochenen Verkehrspflichten wirken zudem in das vertragliche Pflichtenprogramm hinein. Wie (oben 4.4.3.3.2) bereits angesprochen, sind Verkehrspflichten innerhalb von Vertragsverhältnissen zugleich Gegenstand einer vertraglichen Schutzpflicht i.S.d. § 241 BGB.[206]

Der Umfang der Verkehrspflichten in Bezug auf IT-Sicherheit wird bisher kaum erörtert. In der Literatur werden einzelne Fallgruppen diskutiert. So werden Verkehrspflichten der Internetnutzer zum Schutz ihrer eigenen technischen Infrastruktur angenommen.[207] Als konkrete Pflicht werden hier der Einsatz eines aktuellen Virenschutzes[208] und die regelmäßige Aktualisierung des Betriebssystems angenommen.[209] Private Internetnutzer sind zwar nicht verpflichtet, eine Firewall einzurichten, dürfen eine bereits vorinstallierte Firewall aber auch nicht ohne triftigen Grund deaktivieren.[210] Betreiber eines WLAN sind nach verbreiteter Auffassung zur Verschlüsselung des WLAN verpflichtet.[211]

Verkehrspflichten zum Schutz der IT werden auch für Betreiber von Webdiensten[212] oder Anbieter von Cloud Computing angenommen.[213] Darüber hinaus gelten die für private Internetnutzer genannten Pflichten mindestens auch für Unternehmen, wobei die Anforderungen darüber wesentlich hinausgehen können. Hier sind die Pflichten aber stark vom Einzelfall abhängig. Das AG Köln beispielsweise verneinte für einen Verlag die Pflicht zur Einrichtung einer Firewall.[214] Eine solche Pflicht dürfte aber für Unternehmen, die im Rahmen von I4.0 per Internet agieren, durchgehend bestehen.

Der Inhalt von Verkehrspflichten zur Gewährleistung von IT-Sicherheit kann durch andere Gesetze beeinflusst werden. Zwar ist der Inhalt von Verkehrspflichten im Rahmen von § 823 Abs. 1 BGB autonom zu ermitteln.[215] Jedoch wird angenommen, dass die gesetzlichen Verhaltenspflichten zugleich eine deliktische Verkehrspflicht im Sinne eines Mindeststandards begründen.[216]

206 Ernst, in MüKo BGB, § 280 Rn. 104; Borges, Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis, S. 166.
207 Borges, Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis, S. 146.
208 Borges, Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis, S. 146; Libertus, MMR 2005, 507, 509; Werner, Verkehrspflichten privater IT-Nutzer in Bezug auf die Verbreitung von Schadsoftware, S. 175 wohl auch Ernst, CR 2006, 590, 593. Koch, NJW 2004, 801, 806 nimmt eine solche Pflicht nur im b2c Verhältnis an.
209 Borges, NJW 2010, 2624, 2625; Werner, Verkehrspflichten privater IT-Nutzer in Bezug auf die Verbreitung von Schadsoftware, S. 166. Siehe zum Meinungsstand bezüglich der Häufigkeit der Aktualisierung: Borges, Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis, S. 161.
210 Werner, Verkehrspflichten privater IT-Nutzer in Bezug auf die Verbreitung von Schadsoftware, S. 163; eine Pflicht zur Einrichtung einer Firewall für private Nutzer fordernd wohl Ernst, CR 2006, 590, 593. Für das Online-Banking bejahte diese Pflicht jedoch das LG Köln, MMR 2008, 259, 261.
211 BGHZ 185, 330, 340 Rn. 34 – Sommer unseres Lebens; OLG Düsseldorf, MMR 2008, 256, 257; LG Frankfurt/M., MMR 2011, 401, 402; LG Frankfurt/M., GRUR 2013, 507, 509; Roggenkamp, jurisPR-ITR 12/2006, Anm. 3.
212 Borges, Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis, S. 194 m.w.N.
213 Wicker, MMR 2014, 715, 717.
214 AG Köln 21.12.1998, 125, C 533/98.
215 BGH, NJW 1987, 372, 373; BGHZ 139, 43, 46 f.; BGHZ 139, 79, 83; BGH NJW, 2001, 2019, 2020; BGH NJW-RR 2003, 1459, 1460; BGH, NJW 2008, 3775, 3777; Borges, Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis, S. 142.
216 BGH, NJW 1987, 372, 373; BGH NJW, 2001, 2019, 2020; BGH, NJW-RR 2003, 1459, 1460; Borges, Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis, S. 143; Hager, in Staudinger, § 823 Rn. E 34; Spindler, in BeckOK BGB, § 923 Rn. 251. Behördliches Gebot als Mindeststandard: BayOblG, NJW-RR 2002, 1249, 1250.

Die Verkehrspflichten können aber über gesetzliche Verhaltenspflichten hinausgehen. So hat der BGH etwa entschieden, dass gesetzliche Kennzeichnungspflichten etwa das Mindestmaß der (deliktischen) Instruktionspflichten eines Herstellers im Hinblick auf sein Produkt darstellen, diese können aber darüber hinausgehen können. Konkret verlangte der BGH im Rahmen der Instruktionspflicht (§ 823 I BGB) die Angabe aller notwendigen Informationen, die der Verwender benötigt, um das Produkt ohne Gefahren für sich und andere zu verwenden.[217] Im Fall eines Sägewerks entschied der BGH, dass der Betreiber des Sägewerks zwar im Rahmen seiner Verkehrssicherungspflicht die gesetzlichen Normen und Unfallverhütungsvorschriften der Berufsgenossenschaft beachten müsse, er aber zum Schutz vor Gefahren, die nicht von den Unfallverhütungsvorschriften erfasst seien, auch über diese Normen hinaus Schutzmaßnahmen ergreifen müsse.[218]

Als Ergebnis der bisherigen Diskussion lässt sich festhalten, dass das Bestehen einer Sicherheitslücke die Verletzung einer deliktischen Pflicht darstellen kann, deren Gegenstand im Einzelfall aufgrund einer Interessenabwägung zu ermitteln ist. Gesetzliche Sicherheitspflichten stellen häufig einen Mindeststandard für Verkehrspflichten dar. Diese können aber über gesetzliche Schutzpflichten hinausgehen.

4.4.4 Aspekte des Datenschutzes

Da die datenschutzrechtlichen Normen, wie oben[219] bereits erläutert, nur dann Anwendung finden, wenn auch personenbezogene Daten erhoben, verarbeitet und genutzt werden, haben wir zur Erläuterung datenschutzrechtlicher Risiken in Bezug auf I4.0 unterstellt, dass im Zuge der einzelnen Produktionsschritte, die im Rahmen einer Produktionskette erfolgen, stets auch personenbezogene Daten zwischen den einzelnen beteiligten Partnern (Rechtseinheiten) ausgetauscht werden, z. B.

- Kundendaten in Form spezieller Kundenspezifikationen, die elektronisch auf einem Bauteil hinterlegt und von den bearbeitenden Maschinen in der Produktionskette zwecks Umsetzung ausgelesen werden und/oder
- Beschäftigtendaten, die auf einzelnen Bauteilen elektronisch hinterlegt werden, um nachvollziehbar zu halten, welcher Mitarbeiter von welchem Beteiligten für das jeweilige Bauteil zuletzt verantwortlich zeichnete.

Unter Zugrundelegung dieser Annahme wird für die erläuterten Grundkonstellationen[220] das anwendbare Recht untersucht und die Einschätzung der damit verbundenen rechtlichen Risiken nach dem gegenwärtig geltenden deutschen und europäischen Datenschutzrecht erläutert. Künftige Entwicklungen, wie das etwaige Inkrafttreten des Entwurfs einer EU-Datenschutzgrundverordnung werden ebenfalls berücksichtigt.

Die bereits oben dargestellten Grundkonstellationen[221] haben wir für diese Zwecke wie folgt aufgegliedert:

1. *Grundkonstellation: Sternförmige Kooperationsstruktur mit einem zentralen Partner im Inland*
   a. *Beteiligte Partner sitzen ausschließlich im bundesdeutschen Inland*
   b. *Beteiligte Partner sitzen auch im EWR-Ausland*
   c. *Beteiligte Partner sitzen auch in Drittstaaten*

2. *Grundkonstellation: Netzförmige Kooperation mit Partnern in verschiedenen Staaten ohne einen zentralen Partner*
   a. *Beteiligte Partner sitzen ausschließlich im bundesdeutschen Inland*
   b. *Beteiligte Partner sitzen auch im EWR-Ausland*
   c. *Beteiligte Partner sitzen auch in Drittstaaten*

Es ergeben sich insoweit folgende datenschutzrechtliche Risiken und Herausforderungen in Bezug auf die unterschiedlichen Grundkonstellationen:

4.4.4.1 Grundkonstellation 1a)

Bei der Grundkonstellation 1a) handelt es sich um eine sternförmige Kooperationsstruktur mit einem zentralen Partner im Inland und weiteren Partnern ausschließlich mit Sitz im Inland, wobei personenbezogene Daten zwischen den verschiedenen Partnern, insbesondere zwischen dem zentralen Partner und den jeweils anderen Partnern, ausgetauscht werden.

217 BGH, NJW 1987, 372, 373.
218 BGH, NJW-RR 2003, 1459, 1460.
219 Hierzu oben Ziff. 3.3.3.1.
220 Hierzu oben Ziff. 4.4.1.
221 Hierzu oben Ziff. 4.4.1.

4.4.4.1.1 Bestehende Risiken nach dem Bundesdatenschutzgesetz („BDSG“)

Im Zusammenhang mit der Grundkonstellation 1a) kommen in datenschutzrechtlicher Hinsicht sowohl rechtliche als auch wirtschaftliche Risiken in Betracht. Im Einzelnen:

4.4.4.1.1.1 Datenumgang ohne hinreichenden Erlaubnistatbestand

Grundsätzlich setzt jeder Umgang mit personenbezogenen Daten einen Erlaubnistatbestand voraus, d.h. eine Einwilligungserklärung der Betroffenen oder eine rechtliche Vorschrift voraus (§ 4 Abs. 1 BDSG).[222] Jede Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch einen beteiligten Partner in der Produktionskette bedarf deshalb einer entsprechenden Legitimation. Ausgehend vom zentralen Partner sind dies die Erhebung der Daten, z. B. beim Kunden, deren Speicherung und Nutzung im Rahmen seines Produktionsabschnitts sowie deren Übergabe an die weiteren Partner im Rahmen der Produktionskette, die die Daten dann ihrerseits erheben, im Rahmen ihrer Produktionsstrecke nutzen und sodann an den zentralen Partner wieder zurückgeben.

Beispiel (1):

Ein Kunde (natürliche Person) bestellt für sich einen PKW über den Online-Konfigurator eines Automobilherstellers. Hierbei wählt er eine Speziallackierung für die Dekorleisten des Innenraums aus. Dies wird über das Web Frontend an das Backend-System des Herstellers übergeben und von dort über EDI an den Zulieferer übergeben. Dieser überführt die Daten in seine Produktionsumgebung und versieht das entsprechende Rohbauteil mit einem Transponder, der eindeutige Informationen zu Farbcode, Endkunden und Automobilhersteller vorhält. Dieser Transponder wird von der gesamten Produktionsanlage des Zulieferers ausgelesen und gemäß der dort hinterlegten Spezifikationen automatisiert bearbeitet, fertiggestellt, an die Logistik übergeben und von dort aus an den Hersteller einschließlich Transponder übersandt. Beim Hersteller angekommen, wird der Transponder ausgelesen, der Bestellung des Kunden zugeordnet und in den dortigen Produktionsprozess des PKW eingebunden. Dieser Prozess läuft dabei in vergleichbarer Form auch mit den Zulieferern anderer Bauteile des PKW ab.

Das Beispiel zeigt, dass in der gesamten Produktionskette Kundendaten erhoben, verarbeitet und genutzt werden, sodass jeder der Partner für seinen Produktionsabschnitt entsprechende Erlaubnistatbestände nachweisen können muss. Gelingt ihm dies nicht und geht er gleichwohl mit den entsprechenden personenbezogenen Daten um, wäre dies als „unbefugte Erhebung oder Verarbeitung personenbezogener Daten“ i.S.v. § 43 Abs. 2 Nr. 1 BDSG zu qualifizieren. Die zuständige Datenschutzaufsichtsbehörde kann dies mit einem Bußgeld von bis zu 300.000 EUR ahnden. Im Einzelfall kann dieses Bußgeld allerdings auch höher bemessen sein, dies namentlich dann, wenn ein Bußgeld von 300.000 EUR nicht genügen würde, um den wirtschaftlichen Vorteil, den der jeweilige Partner aus der rechtswidrigen Datenverarbeitung gezogen hat, vollständig abzuschöpfen, § 43 Abs. 3 S. 2 und 3 BDSG. Bei bestehender Bereicherungsabsicht, was insbesondere in Betracht zu ziehen ist, wenn die rechtswidrige Datenverarbeitung in Kauf genommen wird, um die Produktion effektiv fortführen zu können, ist auch eine Freiheitsstrafe von bis zu zwei Jahren möglich, wenngleich die Tat nur auf Antrag verfolgt wird, § 44 Abs. 1 und 2 BDSG. Daneben drohen stets auch erhebliche Reputationsrisiken, die erfahrungsgemäß gerade bei Produzenten mit Endkundengeschäft auch erhebliche wirtschaftliche Nachteile nach sich ziehen können. Daneben sind auch Schadensersatz- und Unterlassungsansprüche der betroffenen Kunden und Mitarbeiter möglich, was insbesondere gilt, wenn diesen hieraus auch ein monetärer Schaden entstanden ist, §§ 823, 1004 BGB; 7 BDSG.

Dem ist entsprechend entgegenzutreten, wobei die folgenden Instrumente in Betracht kommen[223]:

Einholung einer Einwilligung

Zunächst kann eine Einwilligungserklärung der Betroffenen (z. B. Kunden und Beschäftigte) in die konkrete Datenverarbeitung durch einen oder mehrere Partner in der Produktionskette eingeholt werden. Insoweit empfiehlt sich die Einwilligungseinholung durch den Partner, bei dem die Daten erstmals erhoben werden. Hinsichtlich personenbezogener Kundendaten ist dies bei der hier in Frage stehenden Grundkonstellation in aller Regel der zentrale Partner (bei unserem o. g. Beispiel also der Automobilhersteller), bezüglich Beschäftigten- und sonstigen personenbezogenen Daten (z. B. Ansprechpartnerdaten anderer Partnerunternehmen) indes der jeweilige Partner, bei dem die Daten erstmals erhoben werden.

222 Hierzu oben Ziff. 3.3.3.1.
223 Hierzu oben Ziff.

Bei der Einwilligungseinholung ist dabei darauf zu achten, dass diese dann die gesamte Verarbeitungskette über alle Partner hinweg legitimiert, also so ausgestaltet ist, dass sie auch zu Gunsten aller anderen Partner in der Produktionskette wirkt. Anderenfalls ließe sich nicht ausschließen, dass innerhalb der Produktionskette eine Legitimationslücke entstünde, was es mit Blick auf die allseits zu erfüllenden datenschutzrechtlichen Compliance-Anforderungen naturgemäß zu vermeiden gilt.

Bei der Einwilligungseinholung ist weiter zu beachten, dass diese an formelle und materielle Wirksamkeitsvoraussetzungen geknüpft ist, vgl. § 4a BDSG. Werden diese nicht eingehalten, weil z. B. der Einwilligende vor Erteilung der Einwilligung nicht umfassend über alle Schritte der Datenverarbeitung einschließlich deren Zwecke und Empfänger in der Produktionskette informiert wird[224], kann dies zur Unwirksamkeit der Einwilligung führen. Dasselbe gilt, wenn die für die Einwilligung gemäß § 4a Abs. 1 S. 1 BDSG ebenfalls erforderliche Freiwilligkeit nicht gegeben ist, wie dies insbesondere für im Beschäftigungsverhältnis erteilte Einwilligungen diskutiert wird.[225] Entscheidet sich ein Partner die in der Produktionskette stattfindenden Nutzungen von Beschäftigtendaten gleichwohl über Einwilligungserklärungen abbilden zu wollen, dann empfiehlt sich insoweit ein einheitliches und dokumentiertes Vorgehen. Insoweit empfehlen sich etwa arbeitsvertragliche Regelungen, wobei darauf zu achten ist, dass datenschutzrechtliche Einwilligungen im Arbeitsvertrag einer besonderen Hervorhebung bedürfen (§ 4a Abs. 1 S. 4 BDSG) und aus Dokumentationsgründen auch möglichst gesondert unterzeichnet werden sollten.

Daneben gelten zahlreiche weitere formelle Anforderungen an die Einwilligung, wenn diese elektronisch – via Mobile-App oder Onlineportal – eingeholt wird. Letzteres dürfte im Industrie 4.0-Kontext gerade in Bezug auf die Einholung von Kundendateneinwilligung der Regelfall sein. So zeigt etwa auch unser Ausgangsbeispiel, dass der Automobilhersteller eine Kundeneinwilligung höchstwahrscheinlich über das Web Frontend seines Konfigurators einholen würde. Ist dies aber festzustellen, unterliegt er dem Telemediengesetz (TMG) und muss gemäß § 13 Abs. 1 und 2 TMG weiter sicherstellen, dass

- der Betroffene seine Einwilligung bewusst und eindeutig erteilt hat,
- die Einwilligung protokolliert wird,
- der Betroffene den Inhalt der Einwilligung jederzeit abrufen kann und
- er die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann, er hierüber bei Einwilligungserteilung unterrichtet wird und der Inhalt der Unterrichtung jederzeit für ihn abrufbar ist.

Insgesamt gilt, dass eine unwirksame Einwilligungserteilung nicht über das in § 4 Abs. 1 BDSG statuierte grundsätzliche Verbot des Umgangs mit personenbezogenen Daten hinweghelfen kann. Folglich gilt es zur Vermeidung der eingangs erläuterten Risiken eine unzureichende Einwilligungsausgestaltung unbedingt auszuschließen. Soweit die Einwilligung nur dazu dienen soll, Verarbeitungsrisiken zu minimieren, weil der die Daten ersterhebende Partner davon ausgeht, dass sich der Umgang mit diesen Daten in der Produktionskette auch auf andere Erlaubnistatbestände (dazu sogleich) stützen lässt, ist darauf zu achten, dass die Einwilligung so formuliert wird, dass durch deren Verweigerung möglicherweise ebenfalls eingreifenden Erlaubnistatbestände nicht gesperrt werden.

Betriebsvereinbarungen und Tarifverträge

Die Nutzung von Beschäftigtendaten im Rahmen der Produktionskette lässt sich im bestimmten Umfang grundsätzlich auch über Betriebsvereinbarungen und Tarifverträge abbilden.[226]

Tarifverträge scheiden für die Regelung konkreter Verarbeitungssituationen allerdings indes in aller Regel aus, da die Tarifvertragsparteien (Arbeitgeber/-verbände und Gewerkschaften) zu solchen betrieblichen Einzelfragen üblicherweise nicht verhandeln, sondern regelmäßig Themen im Zusammenhang mit den sonstigen Arbeitskonditionen (insbes. Entgelt, Arbeitszeit und Urlaubsanspruch) im Fokus stehen.

224 Hierzu Behling/Abel/Ringel, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 10 Rn. 118.

225 Ob eine freiwillige Einwilligungserklärung eines Beschäftigten an seinen Arbeitgeber aufgrund des im Arbeitsverhältnisses bestehenden faktischen Zwangs möglich ist, ist bspw. umstritten, vgl hierzu Behling/Abel/Gola, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 8 Rn. 10; Däubler/Hjort/Schubert/Wolmerath/Hilbrans, Arbeitsrecht, 3. Aufl. 2013, BDSG § 4a, Rn. 3.

226 BAG, Urt. V. 25.9.2013 – 10 AZR 270/12; Behling/Abel/Kynast, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 8 Rn. 136.

Entsprechend kommen in erster Linie Betriebsvereinbarungen in Betracht, um Datennutzungen im Rahmen der Produktionskette zu legitimieren. Diesen kommt wegen § 77 Abs. 4 S. 1 Betriebsverfassungsgesetz (BetrVG) eine sog. normative Wirkung zu, was der wesentliche Grund dafür ist, dass sie als Erlaubnistatbestände i.S.d. BDSG anerkannt sind[227]. Gleichwohl ist umstritten, ob sie nur solche Datennutzungen legitimieren können, die auch nach dem BDSG erlaubt wären.[228] Mit einer – bereits älteren – Entscheidung des *Bundesarbeitsgerichts*[229] (BAG) lässt sich dies durchaus vertreten, wenngleich auch das BAG klarstellte, dass die Regelungen jedenfalls an den *„grundgesetzlichen Wertungen, zwingendem Gesetzesrecht und den sich aus allgemeinen Grundsätzen des Arbeitsrechts ergebenden Beschränkungen"* auszurichten seien. Entsprechend besteht zwar ein gewisser Gestaltungsspielraum[230]; was aber eindeutig nach dem BDSG untersagt ist, kann auch nicht ohne weiteres allein über eine Betriebsvereinbarung legitimiert werden.

Aber selbst wenn dies sichergestellt ist, kommen Betriebsvereinbarungen als Legitimationsinstrument naturgemäß nur in dem Umfang in Betracht, wie sie überhaupt abgeschlossen werden können. So setzt die Möglichkeit zum Abschluss einer Betriebsvereinbarung zunächst voraus, dass ein (Gesamt-/Konzern-)Betriebsrat gewählt worden ist. Ist dies der Fall und können sich die Betriebsparteien über die Einzelheiten der Datennutzung im Rahmen der Produktionskette verständigen, kann die Betriebsvereinbarung diese Nutzung grundsätzlich auch in Bezug auf Arbeitnehmer i.S.v. § 5 Abs. 1 und 2 BetrVG legitimieren. Wegen § 5 Abs. 3 BetrVG kann die Datennutzung von leitenden Angestellten allerdings nicht über Betriebsvereinbarungen geregelt werden, weshalb vor dem Abschluss von Betriebsvereinbarungen zu klären ist, welche Daten von welchen Mitarbeitern im eigenen Produktionsabschnitt überhaupt betroffen sind.

Je nach Art der organisatorischen Aufstellung des jeweiligen Partners (konzernbezogene Matrixorganisation, einheitsbezogene Linienorganisation), dessen rechtlicher Ausgestaltung (Einzelunternehmen oder Gruppe) und der Reichweite der Datennutzung in dem eigenen Produktionsabschnitt (Einzelbetrieb, mehrere Betriebe oder konzernweit) muss die Betriebsvereinbarung als Einzelbetriebsvereinbarung(en), Gesamt- oder Konzernbetriebsvereinbarung ausgestaltet werden, was ebenfalls davon abhängig ist, ob eine überbetriebliche Angelegenheit gegeben und eine überbetriebliche Regelung erforderlich ist oder nicht, vgl. § 50 Abs. 1 S. 1, 1. Hs BetrVG. Letzteres erscheint zumindest naheliegend, wenn der Produktionsabschnitt eines Partners über mehrere seiner Betriebe verläuft und dies durchweg mit der Nutzung von Arbeitnehmerdaten verbunden ist.

Kommt nach dem zuvor Ausgeführten eine Betriebsvereinbarung als Legitimationsinstrument in Betracht, bleibt zu beachten, dass diese weder mit arbeitsvertraglichen Regelungen zum Nachteil der Arbeitnehmer kollidieren darf (sog. Günstigkeitsprinzip)[231] noch (wegen § 77 Abs. 3 BetrVG) mit tarifvertraglichen Regelungen. Ein entsprechender Abgleich muss also vor dem Abschluss entsprechender Betriebsvereinbarungen unbedingt erfolgen, was insbesondere gilt, wenn Arbeitsverträge datenschutzrechtliche Regelungen enthalten, insbesondere wenn Einwilligungserklärungen hierüber eingeholt worden sind.

Abschließend ist darauf hinzuweisen, dass die Betriebsvereinbarung auch ein gutes Instrument darstellt, um die i.d.R. ohnehin gebotene Einbindung des Betriebsrates nach §§ 80 Abs. 1 Nr. 1; 87 Abs. 1 Nr. 6 BetrVG sicherzustellen, zumal der Abschluss i.d.R. auch immer zu einem Verbrauch eventueller Zustimmungsvorbehalte führen dürfte.[232]

Eine Schwäche der Betriebsvereinbarung im Kontext von I4.0 liegt freilich darin, dass diese zunächst nur betriebliche Wirkung entfaltet. Selbst wenn ihr aber eine überbetriebliche Wirkung, wie bspw. bei Abschluss einer Konzernbetriebsvereinbarung, zukommt, beschränkt sich der größtmögliche Anwendungsbereich auf konzernangehörige Unternehmen. Sie kann also grundsätzlich nur die Datenverarbeitung im Produktionsabschnitt eines Partners legitimieren, nicht aber in der gesamten Produktionskette. Dies ist gerade im Vergleich zur Einwilligungserklärung ein zunächst ins Auge stechender Nachteil. Dieser lässt sich allerdings ggfs. darüber beseitigen, dass die Regelungen der Betriebsvereinbarungen über vertragliche Regelungen mit den anderen Partnern auch diesen ggü. (über Unterwerfungsvereinbarungen oder der Vereinbarung gleichlautender Betriebsvereinbarungen) verbindlich gemacht werden. Dass eine solche Möglichkeit

227 Behling/Abel/Gola, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 8 Rn. 17; Gola/Schomerus, BDSG, 11. Aufl. 2012, § 4 Rn. 10.
228 Behling/Abel/Gola, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 8 Rn. 17; Gola/Schomerus, BDSG, 11. Aufl. 2012, § 4 Rn. 10.
229 Beschl. v. 27.5.1986 – 1 ABR 48/84.
230 Behling/Abel/Gola, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 8 Rn. 17.
231 Vgl. hierzu Richardi/Richardi, BetrVG, 14. Aufl. 2014, § 77 Rn. 141 ff.
232 Vgl. nur Thüsing/Granetzny, Beschäftigtendatenschutz und Compliance, 2. Aufl. 2014, § 20 Rn. 79 m.w.N.

besteht, wird auch für organisationsübergreifende internationale Datentransfers diskutiert[233], weshalb nicht ersichtlich ist, warum dies nicht auch für bloß innerdeutsche Sachverhalte in Betracht zu ziehen sein soll. Selbstverständlich setzt eine solche Regelung allerdings die vorherige Abstimmung zwischen allen Partnern in der Produktionskette voraus, da hiervon naturgemäß auch die Betriebsparteien aller Partner betroffen sind.

Gerade weil die Legitimationswirkung von Betriebsvereinbarungen den zuvor erläuterten Beschränkungen und Herausforderungen unterliegt, ist ein besonnenes und gleichzeitig genaues Vorgehen erforderlich, da eventuelle Fehler die Legitimation der Nutzung von Mitarbeiterdaten in der Produktionskette beeinträchtigen können. Dies wiederum ist mit den eingangs erläuterten Risiken verbunden, welche es entsprechend zu vermeiden gilt.

Eingreifen eines gesetzlichen Erlaubnistatbestandes (§§ 28, 32 BDSG)

Sofern weder Einwilligungen noch Betriebsvereinbarungen in Betracht kommen, um die Nutzungen von personenbezogenen Daten in der Produktionskette zu legitimieren, verbleibt nur der Rückgriff auf die gesetzlichen Erlaubnistatbestände der §§ 28 Abs. 1 S. 1 Nr. 1 und 2, Abs. 2; § 32 Abs. 1 S. 1 BDSG und deren Vorliegen ist jeweils im Einzelfall dezidiert zu prüfen. Wie bereits an anderer Stelle ausgeführt, hängt ein Eingreifen dieser Erlaubnistatbestände entscheidend davon ab, inwieweit die Nutzung der jeweiligen Datenarten in der Produktionskette erforderlich ist.

Diese Frage wird sich häufig vor allem in Bezug auf Beschäftigtendaten stellen, deren Umgang sich zunächst an § 32 Abs. 1 S. 1 BDSG messen lassen muss. Danach ist der Umgang mit Beschäftigtendaten erlaubt, wenn dies zum Zwecke der Durchführung des Beschäftigungsverhältnisses auch erforderlich ist. Gerade im Rahmen von I4.0 wird sich eine solche Erforderlichkeit häufig aber nur sehr schwer begründen lassen, was insbesondere dann gilt, wenn das mit der jeweiligen Datenverarbeitung verfolgte Ziel auch auf einem anderen, weniger eingriffsintensiven Wege realisiert werden kann. Denn es genügt für die Erforderlichkeit i.S.v. § 32 Abs. 1 S. 1 BDSG nicht, dass die jeweils in Frage stehenden Datenverarbeitungen für das Arbeitsverhältnis nützlich sind, sie müssen vielmehr hierfür auch geboten sein.[234] Hieran wird es aber gerade im Kontext von I4.0 häufig fehlen.

Beispiel (2):

Ein Mitarbeiter zeichnet in einem Bereich der Produktionskette für die Herstellung eines Motorenteils eines Kraftfahrzeuges verantwortlich, da er den Herstellungsprozess in seinem Bereich überwacht. Dies wird elektronisch auf dem Bauteil vermerkt. Hintergrund dessen ist, dass während des gesamten Herstellungsprozesses nachvollziehbar bleiben soll, welcher Mitarbeiter welches Partners für welches Bauteil pro Herstellungsschritt verantwortlich ist, damit dieser im Falle eventueller Probleme mit diesem Bauteil im weiteren Produktionsprozess leicht und schnell ermittelt und angesprochen werden kann.

Genauso gut ließe sich dieser Mitarbeiter aber auch anhand des Schichtbuches bei dem Partner, bei dem dieser beschäftigt ist, ermitteln. Der Ermittlungsaufwand wäre nur wesentlich höher und würde entsprechend mehr Zeit in Anspruch nehmen. Dies allerdings scheuen die Partner in der Produktionskette, da eine längere Identifizierungszeit gerade im Falle von Problemen zu Produktionsverzögerungen führen kann. Deshalb haben sie sich darauf verständigt, dass ein eindeutiges Identifikationsmerkmal (z. B. Name, Personalnummer) elektronisch auf dem Bauteil hinterlegt werden muss.

Dieses Beispiel zeigt, dass zwar der Vermerk des Identifikationsmerkmals der verantwortlichen Mitarbeiters auf dem Bauteil für die Produktion und damit auch für die Durchführung seines Beschäftigungsverhältnisses nützlich ist, keinesfalls aber erforderlich. Eine Legitimation dieser Verarbeitung seiner Daten über § 32 Abs. 1 S. 1 BDSG scheidet deshalb aus.

Daher stellt sich die Frage, ob sich diese Verarbeitung ggfs. über § 28 Abs. 1 S. 1 Nr. 2 ggfs. i.V.m. Abs. 2 Nr. 2a BDSG legitimieren lässt. So könnten, wie von diesen Vorschriften vorausgesetzt, berechtigte Interessen des Partners, bei dem dieser Mitarbeiter beschäftigt ist, und berechtigte Interessen der anderen Partner in der Produktionskette bestehen, die eine Speicherung seiner Daten auf dem Bauteil erforderlich machen. Da unter einem berechtigten Interesse im Sinne dieser Vorschrift nach überwiegender Auffassung jedes *„nach vernünftiger Erwägung durch die Sachlage gerechtfertigte [Interesse], also ein tatsächliches Interesse, das wirtschaftlicher oder ideeller Natur sein kann“*[235], verstanden wird, kommt eine Legitimation dieser Speicherung über § 28 Abs. 1 S. 1 Nr. 2 ggfs. i.V.m. Abs. 2 Nr. 2a BDSG durchaus

233 Gola/Schomerus, BDSG, 11. Aufl. 2012, § 4c Rn. 10.
234 Gola/Schomerus, BDSG, 11. Aufl. 2012, § 32 Rn. 12.
235 Gola/Schomerus, BDSG, 11. Aufl. 2012, § 28 Rn. 24.

in Betracht. Denn die Datenspeicherung auf dem Bauteil erfolgt, um eine schnelle Kontaktaufnahme im Falle von Problemen zu ermöglichen und um eine Produktionsverzögerung zu vermeiden oder zumindest gering zu halten.

Allerdings ist es hoch umstritten, ob § 28 Abs. 1 und 2 BDSG eine Verarbeitung von Beschäftigtendaten noch legitimieren kann, wenn diese von § 32 Abs. 1 S. 1 BDSG nicht gedeckt ist.[236] Da diese Frage nicht rechtssicher aufgelöst werden kann, wird ohne eine Klarstellung bei der Verarbeitung von Beschäftigtendaten im Rahmen von I4.0 häufig eine rechtliche Unsicherheit verbleiben, wenn diese allein auf gesetzliche Erlaubnistatbestände gestützt wird. Damit einher gehen dann die eingangs erläuterten Risiken, d.h. insbesondere besteht die Gefahr von Bußgeldern und Schadensersatzansprüchen.

Weniger riskant erscheint der Rückgriff auf die gesetzlichen Erlaubnistatbestände, wenn, wie in unserem Beispiel (1), die Verarbeitung von (End-)Kundendaten in Frage steht. So werden etwa Automobilhersteller kaum eine andere Wahl haben als andere Zulieferer mit der Produktion von Fertigungsteilen zu beauftragen und diesen dabei die vom Kunden festgelegten Spezifikationen mitzuteilen. Deshalb spricht viel dafür, dass sich die entsprechende Datenweitergabe in der Produktionskette auf § 28 Abs. 1 S. 1 Nr. 1 BDSG stützen lässt. Denn danach ist die Speicherung und Übermittlung von personenbezogenen Daten erlaubt, wenn dies zur Durchführung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Das bei unserem Beispiel (1) in Frage stehende Schuldverhältnis ist der Kaufvertrag, der sich nur erfüllen lässt, wenn die Spezifikationsdaten an den Zulieferer weitergegeben werden und die Zuordnung zur Bestellung des Kunden durchgehend möglich bleibt. Denn anderenfalls ließe sich das Bauteil nach der Herstellung durch den Zulieferer und Übersendung an den Automobilhersteller als zentralen Partner nicht mehr dessen Bestellung zuordnen. Einzig fraglich ist insoweit, ob es erforderlich ist, dass der Name des Kunden in unserem Beispiel (1) auch für den Zulieferer lesbar bleibt. Dies wird man in aller Regel wohl verneinen müssen, da das Bauteil der Bestellung des Kunden auch bei bloßer Verwendung eines Pseudonyms (z. B. Kundenummer bei Automobilhersteller) zuordenbar bleiben müsste. Die Verwendung von Klarnamen hat deshalb in aller Regel zu unterbleiben, was letztlich auch mit den zu beachtenden Grundsätzen von Datenvermeidung und -sparsamkeit (§ 3a BDSG) korrespondiert.

Allerdings bedeutet die grundsätzliche Möglichkeit eines Rückgriffs auf gesetzliche Erlaubnistatbestände nicht, dass die Betroffenen darüber im Unklaren gelassen werden dürfen, an wen ihre Daten gelangen. So muss der Betroffene bei der Erhebung seiner Daten gemäß § 4 Abs. 3 BDSG über Folgendes unterrichtet werden, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat:

- Über die Identität der verantwortlichen Stelle,
- über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und
- über die Kategorien von Empfängern; dies allerdings nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss.

Da dieselben Transparenzpflichten auch bei der Einholung einer Einwilligung bestehen, dürfte es sich selbst dann, wenn das Eingreifen eines gesetzlichen Erlaubnistatbestandes wahrscheinlich erscheint, als zweckmäßig erweisen, dennoch eine Einwilligung einzuholen. Denn wenn der Betroffene (insbes. Kunde) ohnehin über alle Verarbeitungsschritte zu unterrichten ist, kann er auch gebeten werden, hierin einzuwilligen. Dies erhöht die Rechtssicherheit und erleichtert die Beweisführung im Streitfalle.

Scheidet die parallele Einwilligungseinholung indes aus, verbleibt ohnehin stets das Risiko, dass die zuständige Datenschutzaufsicht oder ein Gericht den im Zusammenhang mit I4.0 erfolgenden Datenumgang als nicht erforderlich anzusehen und deshalb als bußgeldbewehrt oder schadensersatzpflichtig zu qualifizieren. Dies ist das größte abstrakte Risiko, das verbleibt, wenn der Umgang mit personenbezogenen Daten im Rahmen von I4.0 allein auf gesetzliche Erlaubnistatbestände gestützt werden soll.

Auftragsdatenverarbeitungsvereinbarung („ADV-Vereinbarung“)

Eine datenschutzrechtliche Legitimation kann des Weiteren über die Vereinbarung einer wirksamen Auftragsdatenverarbeitung gemäß § 11 BDSG („ADV“) herbeigeführt werden. So führt die ADV gemäß § 3 Abs. 8 S. 3 BDSG dazu, dass die Übermittlung von personenbezogenen Daten zwischen dem Auftraggeber (z.B. zentraler Partner) und dem Auftragnehmer (z.B. Partner in der Produktionskette) keiner weiteren Legitimation bedarf (sog. Privilegierungswirkung der

236 Zum Meinungsstand vgl. ausführlich BeckOK DatenSR/Riesenhuber, BDSG, 10. Edition, Stand: 1.11.2014, § 32 Rn. 26.

ADV).[237] Dies bedeutet allerdings nicht, dass hierdurch die gesamte bei dem Aufragnehmer stattfindende Datenverarbeitung ebenfalls privilegiert wäre. Diese bleibt vielmehr genauso legitimationsbedürftig wie dies ohne ADV-Vereinbarung der Fall wäre. Der einzige Unterschied besteht im Falle einer ADV darin, dass hierfür der Auftraggeber und gerade nicht der Auftragnehmer datenschutzrechtlich verantwortlich zeichnet (§ 3 Abs. 7, 2. Alt. BDSG).

Der Legitimationsgewinn einer ADV-Vereinbarung ist deshalb überschaubar, zumal sie ohnehin nur in Betracht kommt, wenn die materiellen Voraussetzungen für eine ADV tatsächlich auch erfüllt sind, also ein oder mehrere Partner in der Produktionskette für einen anderen Partner personenbezogene Daten weisungsgemäß und ohne ein Eigenermessen verarbeiten.[238] Dies dürfte eher selten der Fall sein, da die Verarbeitung von personenbezogenen Daten in der Produktionskette i. d. R. Neben- und nicht Hauptzweck sein dürfte und überdies nicht selten auch in eigenem Ermessen erfolgen wird. Nur wenn alle wichtigen Produktionsschritte einer Produktionskette von dem zentralen Partner selbst ausgeführt werden und die übrigen Partner bloß (datenverarbeitende) Hilfstätigkeiten bei der Produktion ausführen, kommt eine ADV-Situation überhaupt in Betracht.

Deshalb liegt es nahe, dass sich die ADV im Umfeld von Industrie 4.0 eher auf die Fälle beschränken wird, die auch heute schon klassische Fälle der ADV darstellen bzw. der Fallgruppe der ADV zuzuordnen sind. So dürfte aufgrund des vernetzten Arbeitens bei Industrie 4.0 etwa dem Datenclearing eine bedeutende Rolle zukommen, das aber auch heute schon i.d.R. als ADV ausgestaltet ist. Ähnliches dürfte in Bezug auf Fernwartungen gelten, die auch heute schon zum Standard bei der Maschinenwartung zählen und weitestehend den Regeln der ADV unterfallen (vgl. § 11 Abs. 5 BDSG).

Zu beachten ist in jedem Falle, dass eine ADV-Vereinbarung niemals den Datenaustausch zwischen Auftraggeber und Auftragnehmer legitimiert, wenn die materiellen ADV-Voraussetzungen nicht erfüllt sind. Fehlt es hieran und greifen keine anderweitigen Erlaubnistatbestände ein, drohen auch bei vereinbarter ADV dieselben Risiken, die ohne vereinbarte ADV bestehen würden, also insbesondere wiederum Bußgelder und Schadensersatzforderungen. Dasselbe gilt, wenn zwar die Voraussetzungen für eine ADV erfüllt sind und ein entsprechender Vertrag geschlossen worden ist, die im Rahmen der ADV erfolgende Datenverarbeitung aber nicht von einem Erlaubnistatbestand gedeckt ist. Der Unterschied besteht dann nur darin, dass nicht die die Daten tatsächlich verarbeitende Stelle (Auftragnehmer) das Rechtswidrigkeitsrisiko trägt, sondern weitestgehend der Auftraggeber. Dies hat auch zur Folge, dass der Auftraggeber dafür haftet, wenn personenbezogene Daten, die der Auftragnehmer für ihn verarbeitet, bei diesem abhandenkommen (z. B. weil ein Partner in der Produktionskette, der als Auftragsdatenverarbeiter agiert, einem Hackereingriff ausgesetzt wird) und ggfs. bestehende Meldepflichten gegenüber Aufsichtsbehörden und Betroffenen nach § 42a BDSG nicht erfüllt werden. Zwar kann diese Meldepflicht nur bei sog. Risikodaten, z. B. Bank- und Kreditkarteninformationen und sog. sensitive Daten (§ 3 Abs. 9 BDSG), entstehen, wird sie aber verletzt, drohen wiederum Bußgelder, die im Grundsatz 300.000 EUR nicht übersteigen, sowie Schadensersatzforderungen der Betroffenen. Entsprechend sind im Rahmen einer ADV auch stets Regelungen dazu zu treffen, wann und wie der Auftraggeber über Unregelmäßigkeiten bei der Datenverarbeitung durch den Auftragnehmer zu informieren ist.

Die weiteren Regelungsinhalte folgen aus der Vorschrift des § 11 Abs. 2 S. 2 BDSG. Werden diese nicht umgesetzt (z. B. das Schriftlichkeitserfordernis oder die Pflicht zur Festlegung konkreter technisch-organisatorischer Maßnahmen) drohen Bußgelder, die 50.000 EUR grundsätzlich nicht übersteigen, § 43 Abs. 1 Nr. 2b, Abs. 3 BDSG. Dasselbe gilt, wenn sich der Auftraggeber vor Beginn der Auftragsdatenverarbeitung nicht von den beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt, §§ 11 Abs. 2 S. 4 und 5 i.V.m. § 43 Abs. 1 Nr. 2b, Abs. 3 BDSG.

4.4.4.1.1.2 Fehlen hinreichender technisch-organisatorischer Maßnahmen

Jenseits der Verletzung bestehender Meldepflichten nach § 42a BDSG können aber auch anderweitige Risiken entstehen, wenn im Rahmen der Produktionskette keine hinreichenden technisch-organisatorischen Maßnahmen zum Schutz der hierbei verarbeiteten Daten getroffen werden. So ist jedes Unternehmen, das personenbezogene Daten erhebt, verarbeitet oder nutzt gemäß § 9 S. 1 BDSG verpflichtet, die technischen und organisatorischen Maßnah-

237 Behling/Abel/Albrecht, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 4 Rn. 66.
238 Simitis/Petri, BDSG, 8. Aufl. 2014, § 11 Rn. 22.

men (sog. „TOM“) zu treffen, die erforderlich sind, um die Ausführung des BDSG zu gewährleisten. Dies setzt nach der Anlage zu § 9 S. 1 BDSG u.a. hinreichende Maßnahmen der Zugangs-, Zutritts- und Weitergabekontrolle voraus, die ihrerseits darauf abzielen müssen, dass Unbefugte keinen Datenzugriff erhalten. Neben den materiell-rechtlichen Anforderungen an die Erhebung, Verarbeitung und Nutzung personenbezogener Daten regelt § 9 BDSG und seine Anlage somit die Anforderungen an die Datensicherheit, die die Einhaltung der Erlaubnisnormen sicherstellen soll.[239]

Sind keine oder nur unzureichende TOM in der Produktionskette getroffen worden und kommt es in der Folge etwa zu sog. Datendiebstählen kann dies Schadensersatzpflichten gegenüber denjenigen auslösen, deren Daten abhandengekommen sind (insbes. Kunden/Mitarbeiter). Als Anspruchsgrundlage ist hierbei § 823 Abs. 2 BGB i.V.m. § 9 S. 1 BDSG in Betracht zu ziehen. Begründet zwar der bloße Datenverlust in aller Regel noch keinen für die Betroffenen ersatzfähigen (materiellen) Schaden, stellt sich die Lage häufig anders dar, wenn die abhanden gekommenen Daten von dem unberechtigten Dritten dazu genutzt werden, die Betroffenen rechtsgeschäftlich zu verpflichten (z.B. weil Bank- oder Kreditkartendaten gestohlen worden sind). So bezifferte Sony den Schaden bei den im Jahre 2011 öffentlich gewordenen Datenverlusten nach Verlautbarungen in der Presse mit 1.2 Millionen Euro, wobei Kursverluste noch nicht eingerechnet sind.[240]

Eine durchgehende technisch-organisatorische Datensicherheit in der Produktionskette sicherzustellen, ist deshalb von grundsätzlicher Bedeutung, dies nicht zuletzt auch deshalb, weil hierdurch auch dem Verlust von Betriebs- und Geschäftsgeheimnissen entgegengetreten wird.

4.4.4.1.2 Bestehende Risiken unter Zugrundelegung des aktuellen Entwurfs[241] der EU Datenschutzgrundverordnung („DS-GVO-E“)

Auch nach dem geplanten Inkrafttreten der DS-GVO-E, der das BDSG nach seinem Inkrafttreten an vielen Stellen überlagern wird, bestehen die zuvor erläuterten Risiken dem Grunde nach fort. Sie verändern sich allerdings graduell, worauf nachfolgend näher eigegangen werden soll:

Zunächst ist es wichtig zu beachten, dass auch nach dem Inkrafttreten des DS-GVO-E das sog. Verbot mit Erlaubnisvorbehalt bezüglich des Umgangs mit personenbezogenen Daten voraussichtlich weiter fortbestehen wird.[242] Entsprechend wird auch künftig der Umgang mit personenbezogenen Daten nur erlaubt sein, wenn eine Einwilligung vorliegt oder dieser von einer Rechtsvorschrift gedeckt ist. Folglich werden auch nach dem Inkrafttreten die einzelnen Schritte des Datenumgangs durch die jeweiligen Partner in der Produktionskette einer datenschutzrechtlichen Legitimation bedürfen. Fehlt eine solche Legitimation, besteht wiederum ein Risiko, dass ein Bußgeld verhängt wird. Dies wird nach dem jetzigen Gesetzgebungsstand allerdings wesentlich höher ausfallen können als dies derzeit der Fall ist. So sieht Art. 79 Abs. 2a lit. c DS-GVO-E Bußgelder von bis zu 100.000.000 EUR oder fünf Prozent des weltweiten Jahresumsatzes vor, je nachdem, was höher liegt. Dies bedeutet, dass die finanzielle Tragweite eventueller Datenschutzverstöße in der Produktionskette leicht existenzbedrohende Ausmaße annehmen kann.[234]

Zur Eindämmung dieses Risikos wird es zukünftig von noch grundsätzlicherer Bedeutung sein, sicherzustellen, dass der Umgang mit personenbezogenen Daten in der Produktionskette durchgehend datenschutzrechtlich legitimiert ist. Hierzu kommen wiederum Einwilligungen der Betroffenen in Betracht, deren Wirksamkeit allerdings an strenge Erfordernisse geknüpft sein wird (Art. 6 Abs. 1 lit. a. DS-GVO-E); überdies können weiterhin Betriebsvereinbarungen (Art. 9 Abs. 2 lit. b. DS-GVO-E) und gesetzliche Erlaubnistatbestände (Art. 6 Abs. 1 lit. b.-f. DS-GVO-E) als Erlaubnistatbestände herangezogen werden. Die Privilegierungswirkung einer ADV-Vereinbarung wird nach jetzigem Stand des Gesetzgebungsverfahrens dagegen entfallen[244],

239 Hierzu unten Ziffer 5.2.2.1.1und Ziffer 5.4.2.
240 Vgl. Spiegel Online v. 03.06.2011 (abrufbar unter http://www.spiegel.de/netzwelt/web/erneuter-datenklau-hacker-lieben-sony-a-766391.html).
241 Sog. LIBE-Entwurf des Europäischen Parlaments.
242 Art. 6 LIBE-Entwurf.
243 Vgl. auch Behling/Abel/Behling, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 1 Rn. 6.
244 Vgl. hierzu Roßnagel/Kroschwald, ZD, 2014,495, 497.

was es bereits heute zweckmäßig erscheinen lässt, den Datenaustausch in der Produktionskette nicht (allein) über Auftragsdatenverarbeitungsverträge zu legitimieren.

Überdies werden mit Inkrafttreten des DS-GVO-E erhöhte Anforderungen an die Datenschutzorganisation eines jeden Partners in der Produktionskette gestellt. Es werden Datenschutzrisikoanalysen, -folgenabschätzungen und -Compliance-Reviews gesetzlich vorgeschrieben, die neben dezidierten Datenschutzrisikoanalysen auch hinreichende Kontrollen und Dokumentationen voraussetzen, die bei Verlangen auch der zuständigen Datenschutzaufsicht nachzuweisen sind (vgl. Art. 32a, 33, 33a DS-GVO-E).[245]

Darüber hinaus ist nach Art. 23 DS-GVO-E sicherzustellen, dass die Grundsätze von „privacy by design“ und „privacy by default“ über die gesamte Produktionskette eingehalten werden, wobei grundsätzlich jeder Partner die datenschutzrechtliche Verantwortung für seinen Produktionsbereich trägt. Zwar werden damit vor allem die auch heute schon zu beachtenden Grundsätze der Erforderlichkeit und der Datensparsamkeit sowie -vermeidung betont und weiter ausdifferenziert, die Einhaltung dieser Grundsätze müssen dann aber bereits für die Konzeptionierung von Verarbeitungsverfahren nachgewiesen werden, was umfassende Dokumentationen erfordert. Nicht zuletzt vor dem Hintergrund der in dem DS-GVO-E vorgesehenen hohen Bußgelder empfiehlt es sich daher schon heute, die Anforderungen von privacy by design[246] und privacy by default[247] zu erfüllen.

4.4.4.2 Grundkonstellation 1b)

Bei der Grundkonstellation 1b) handelt es sich um eine sternförmige Kooperationsstruktur mit einem zentralen Partner im Inland und weiteren Partnern mit Sitz im Inland sowie innerhalb des Europäischen Wirtschaftsraums („EWR“). Zwischen den unterschiedlichen Partnern, insbesondere zwischen dem zentralen Partner und den jeweils anderen Partnern, werden personenbezogene Daten ausgetauscht.

4.4.4.2.1 Bestehende Risiken nach dem BDSG

Die in dieser Grundkonstellation 1b) nach dem BDSG bestehenden Risiken stellen sich zunächst nicht anders dar als in der Grundkonstellation 1a). Diese Risiken können sich allerdings verändern, sobald die Produktionskette das EWR-Ausland erreicht und der dabei stattfindende Umgang mit personenbezogenen Daten gemäß § 1 Abs. 5 S. 1 BDSG den nationalen datenschutzrechtlichen Anforderungen unterfällt.

So geht das BDSG bei Sachverhalten mit EWR-Bezug vom sog. Sitzprinzip aus, d. h. das insoweit anzuwendende nationale Recht richtet sich nach dem Recht des Ortes, an dem die für die in Rede stehende Datenverarbeitung verantwortliche Stelle ihren Sitz hat.[248]

Hat also bspw. einer der Partner seinen Sitz in den Niederlanden und werden diesem wie in unserem obigen Beispiel (1) Kundendaten übermittelt, richtet sich die Rechtmäßigkeit des Datenumgangs in den Niederlanden grundsätzlich allein nach niederländischem Datenschutzrecht. Etwas Anderes kommt nur in Betracht, wenn der niederländische Partner im Zuge einer Auftragsdatenverarbeitung i.S.v. § 11 BDSG tätig wird, weil dies in materiell-rechtlicher Hinsicht dann so behandelt wird, als würde der primäre Partner (aus Deutschland) selbst die Daten in den Niederlanden verarbeiten.[249]

Sofern aber – wie regelmäßig bei grenzüberschreitenden Sachverhalten – das Datenschutzrecht eines anderen Mitgliedsstaates Anwendung findet, besteht das Risiko, dass hierüber zusätzliche Anforderungen an den Umgang mit personenbezogenen Daten zu erfüllen sind, die bei Nichteinhaltung von den lokalen Aufsichtsbehörden auch sanktioniert werden können. Insbesondere bestehen nach ausländischem Recht häufig spezielle Meldepflichten bei den Aufsichtsbehörden oder es werden – wie in Österreich[250] – auch bloße Unternehmensdaten als personenbezogene Daten eingestuft, die dann entsprechend auch nur bei Vorliegen eines Erlaubnistatbestandes verarbeitet werden dürfen.

Entsprechend ist bei bestehendem EWR-Bezug stets auch die Anwendbarkeit der maßgeblichen Datenschutzgesetze

245 Vgl. hierzu Behling/Abel/Behling, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 1 Rn. 42 ff.
246 Hierzu oben Ziff. 3.3.3.3.
247 Hierzu oben Ziff. 3.3.3.3.
248 Gola/Schomerus, BDSG, 11. Aufl. 2012 § 1 Rn. 27.
249 Vgl. Dammann, RDV 2002, 70, 73.
250 Vgl. Art. 2, § 4 Nr. 3 Österreichisches Datenschutzgesetz.

zu prüfen und sicherzustellen, dass in der gesamten Produktionskette Datenschutzverstöße unterbleiben.

4.4.4.2.2 Bestehende Risiken unter Zugrundelegung des DS-GVO-E

Die in dieser Grundkonstellation 1b) bestehenden Risiken, die aus dem DS-GVO-E folgen stellen sich insgesamt grundsätzlich nicht anders dar als im Zusammenhang mit der Grundkonstellation 1a) ausgeführt.

Da der DS-GVO-E aufgrund des Verordnungscharakters bei seinem Inkrafttreten unmittelbar in allen Mitgliedsstaaten gelten wird[251], führt dies zu einer grundsätzlichen Vereinheitlichung des Datenschutzrechts innerhalb der EU. Von der Grundkonstellation 1a) abweichende Risiken können daher nur dann hinzutreten, wenn trotz des Verordnungscharakters einzelstaatliche Regelungen möglich bleiben, was nach jetzigem Stand jedenfalls für den Beschäftigtendatenschutz vorgesehen ist, vgl. Art. 82 Abs. 1 DS-GVO-E. Insoweit gilt es daher die nationalen gesetzgeberischen Entwicklungen zu beobachten. Entscheidende Abweichungen von den grundsätzlichen Regelungen des DS-GVO-E werden aber ohnehin nicht möglich sein, da Art. 82 Abs. 1 DS-GVO-E vorsieht, dass die nach derzeitigem Gesetzgebungsstand noch möglichen einzelstaatlichen Regelungen in jedem Falle *„im Einklang mit den Regelungen dieser Verordnung“*, also der Datenschutz-Grundverordnung stehen müssen.

4.4.4.3 Grundkonstellation 1c)

Bei der Grundkonstellation 1c) handelt es sich um eine sternförmige Kooperationsstruktur mit einem zentralen Partner im Inland und weiteren Partnern mit Sitz im Inland sowie mit Sitz im Ausland, d.h. sowohl innerhalb des EWR als auch außerhalb des EWR (sog. Drittstaaten). Zwischen den unterschiedlichen Partnern, insbesondere zwischen dem zentralen Partner und den jeweils anderen Partnern, werden personenbezogene Daten ausgetauscht.

4.4.4.3.1 Bestehende Risiken nach dem BDSG

Neben den unter 4.4.4.1.1 und 4.4.4.2.1 beschriebenen Risiken, treten bei der Grundkonstellation 1 c) noch weitere datenschutzrechtliche Risiken hinzu, die daraus folgen, dass ein oder mehrere Partner in Drittstaaten sitzen.

So greift in diesem Falle eine zweistufige Prüfungsfolge:[252] So ist in einem ersten Schritt zu prüfen, ob sich die Übermittlung an den außereuropäischen Partner, säße dieser innerhalb des EWR, von einem Erlaubnistatbestand gedeckt ist. Ist dies zu bejahen, ist in einem zweiten Schritt festzustellen, ob die aus §§ 4b Abs. 2 bis 6, 4c BDSG folgenden besonderen Anforderungen für einen Drittstaatentransfer gegeben sind. Nur wenn sich beides bejahen lässt, ist die Übermittlung an den Partner außerhalb des EWR datenschutzrechtlich erlaubt.

Abweichende Risiken zu den Grundkonstellationen 1a) und 1b) können damit nur aus der zweiten Prüfungsstufe, den zusätzlichen Anforderungen für einen Drittstaatentransfer, folgen. Zur Erfüllung dieser Anforderungen kommen mit Filip[253] folgende Varianten in Betracht:

- Beim Datenempfänger ist ein angemessenes Datenschutzniveau gewährleistet (§ 4b Abs. 2, Abs. 3 BDSG),
- es liegt der Ausnahmetatbestand nach § 4c Abs. 1 BDSG vor oder
- die Übermittlung wird von der Aufsichtsbehörde gem. § 4c Abs. 2 S. 1 BDSG genehmigt.

Insoweit gilt es Folgendes zu beachten:

- Datenempfänger mit angemessenem Datenschutzniveau

Nach den Entscheidungen der EU-Kommission gemäß Art. 25 Abs. 6 der Europäischen Datenschutzrichtlinie 95/46/EG (im Folgenden „EU-DatenschutzRL“) ist derzeit ein angemessenes Datenschutzniveau grundsätzlich in den folgenden Ländern gewährleistet:[254]

- Andorra (ABl. EU v. 21. 10. 2010, Nr. L 277/27),
- Argentinien (ABl. EU v. 5. 7. 2003, Nr. L 168/19),

251 Behling/Abel/Behling, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 1 Rn. 5.
252 Behling/Abel/Filip, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 5 Rn. 78.
253 In: Behling/Abel, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 5 Rn. 79.
254 Gola/Schomerus, BDSG, 11. Aufl. 2012, § 4b Rn. 14.

- Australien (ABl. EU v. 8. 8. 2008, Nr. L 213/47),
- Färöer (ABl. EU v. 9. 3. 2010, Nr. L 58/17),
- Guernsey (ABl. EU v. 25. 11. 2003, Nr. L 308/27),
- Isle of Man (ABl. EU v. 30. 4. 2004, Nr. L 151/51 sowie Berichtigung in ABl. EU v. 10. 6. 2004, Nr. L 208/47),
- Israel (ABl. EU v. 1. 2. 2011, Nr. L 27/39),
- Jersey (ABl. EU v. 28. 5. 2008, Nr. L 138/21),
- Kanada (ABl. EG v. 4. 1. 2000, Nr. L 2/13),
- Schweiz (ABl. EG v. 25. 8. 2000, Nr. L 215/1),
- USA: Sonderfall Safe Harbor (ABl. EG v. 25. 8. 2000, Nr. L 215/7).

Gerade der Sonderfall der Safe Harbor-Zertifizierung in den USA führt derzeit zu massiven praktischen Problemen und daraus resultieren Rechtsrisiken. Im Einzelnen:

- Sonderfall: Partner mit Sitz in den USA

Gerade der Fall, dass ein Partner in der Produktionskette in den USA sitzt, stellt sich derzeit als äußerst problematisch dar.

So darf ein Datenexporteur – in unserem Fall also ein Partner in Deutschland, der personenbezogene Daten an einen anderen, in den USA gelegenen Partner übermittelt – grundsätzlich von der Angemessenheit des Datenschutzniveaus ausgehen, wenn letzterer Safe Harbor-zertifiziert ist. Aufgrund des Umstandes allerdings, dass es sich bei Safe Harbor-Zertifizierung um ein Selbstzertifizierungsverfahren handelt, gehen die deutschen Aufsichtsbehörden bereits seit Längerem davon aus, dass jedenfalls allein die behauptete Existenz einer solchen Zertifizierung nicht genügt, um als Datenexporteur ein angemessenes Datenschutzniveau beim Datenempfänger unterstellen zu können. Nach den offenkundig gewordenen Spionageaktivitäten der USA hat sich diese Kritik noch weiter verschärft und wurde auch von der EU-Kommission sowie vom Europäischen Parlament aufgegriffen.[255] Überdies ist mit Beschluss des Irischen High Court vom 18. Juni 2014 (Az. 2013 765 JR) nunmehr auch dem *Europäischen Gerichtshof* die Frage nach der Verbindlichkeit des Safe Harbor-Beschlusses der EU-Kommission vorgelegt worden, sodass die Zukunft von Safe Harbor insgesamt ungewiss ist.

In jedem Falle fordern die Aufsichtsbehörden bereits seit dem Jahre 2010, dass der Datenexporteur vor der Übermittlung seiner Daten an einen Safe Harbor-zertifizierten Empfänger in den USA Folgendes überprüft:[256]

> *„Das die Daten exportierende Unternehmen muss sich nachweisen lassen, dass die Safe Harbor-Selbstzertifizierungen vorliegen und deren Grundsätze auch eingehalten werden. Mindestens muss das exportierende Unternehmen klären, ob die Safe Harbor-Zertifizierung des Importeurs noch gültig ist.*
>
> *Weiter muss sich das Daten exportierende Unternehmen nachweisen lassen, wie das importierende Unternehmen seinen Informationspflichten nach Safe Harbor gegenüber den von der Datenverarbeitung Betroffenen nachkommt. [...]*
>
> *Diese Mindestprüfung müssen die exportierenden Unternehmen dokumentieren und auf Nachfrage der Aufsichtsbehörden nachweisen können.*
>
> *Sollten nach der Prüfung Zweifel an der Einhaltung der Safe Harbor-Kriterien durch das US-Unternehmen bestehen, empfehlen die Aufsichtsbehörden, der Verwendung von Standard-Vertragsklauseln oder bindenden Unternehmensrichtlinien zur Gewährleistung eines angemessenen Datenschutzniveaus beim Datenimporteur den Vorzug zu geben.“*

Da an eine solche Überprüfung mitunter sehr hohe Anforderungen gestellt werden, ist ein alleiniger Rückgriff auf Safe Harbor zur Sicherstellung/Annahme eines angemessenen Datenschutzniveaus risikofrei bereits seit dem Jahre 2010 kaum noch möglich.

So sollen die Aufsichtsbehörden folgende Prüfungsmaßnahmen voraussetzen:[257]

255 Vgl. hierzu Behling/Abel/Filip, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 5 Rn. 86.

256 Vgl. Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich in der Ausgangsfassung vom 28./28.4.2010 mit Überarbeitungen vom 23.8.2010, abrufbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile

257 Vgl. Datenschutz WIKI, Safe Harbor, abrufbar unter http://www.bfdi.bund.de/bfdi_wiki/index.php/Safe_Harbor

- *„Prüfung des Status' der Eintragung auf der Safe Harbor-Liste: Das Unternehmen muss als „current" geführt sein. Zudem sollte das US-Unternehmen der Zusammenarbeit mit europäischen Datenschutzbehörden zugestimmt haben. Dies gilt jedenfalls dann, wenn Beschäftigtendaten übermittelt werden (vgl. Anhang II, FAQ 9, Frage 4 der Entscheidung der Kommission vom 26. Juli 2000 gemäß der RL 95/46/EG über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, 2000/520/EG [20]);*

- *Prüfung der „privacy policy" des Importeurs: Soweit hier Unklarheiten bestehen, z. B. in Bezug auf Konflikte mit den Safe-Harbor-Grundsätzen oder in Bezug auf die in der policy genannten Verarbeitungszwecke, müssen diese aufgeklärt werden;*

- *Prüfung, ob die Informationen für die Betroffenen hinreichend sind (siehe oben Informationspflicht);*

- *Prüfung und Test des in der policy beschriebenen Systems zur Durchsetzung von Betroffenenrechten auf Plausibilität und Funktionsfähigkeit;*

- *Kontaktaufnahme mit Personen, die als Ansprechpartner genannt werden und Befragung zu den entsprechenden Aufgaben;*

- *Im Falle der Auftragsdatenverarbeitung: Sicherstellung, dass Informationen für die Beantwortung z. B. von Auskunftsersuchen in annehmbarer Zeit an den Auftraggeber weitergeleitet werden;*

- *Prüfung, wie im Falle von Weiterübermittlungen der Daten („onward transfers") durch den Importeur verfahren wird, d. h. insbesondere die Frage nach existierenden Vertragsmustern für die Weitergabe in Form der Auftragsdatenverarbeitung, Einräumung eines Widerspruchsrechts/Einholung der Einwilligung der Betroffenen."*

Zwar existieren keinerlei gesetzliche Grundlagen für diese Prüfungsanforderungen, es muss jedoch damit gerechnet werden, dass die Aufsichtsbehörden Bußgelder verhängen, wenn diese Anforderungen vor einem Export von personenbezogenen Daten an einen Partner in den USA nicht erfüllt werden und die Angemessenheit des Datenschutzniveaus allein auf Safe Harbor gestützt werden soll. Gerade die seitens der Datenschutzaufsicht geforderte Prüfung und der Test des in der Datenschutzrichtlinie des Datenempfängers beschriebenen Systems zur Durchsetzung von Betroffenenrechten auf Plausibilität und Funktionsfähigkeit erzeugt in aller Regel einen Aufwand, der sich durch den datenexportierenden Partner kaum in angemessener Zeit und mit angemessenem finanziellem Aufwand realisieren lässt. Auch wenn diese Anforderung damit unverhältnismäßig sein und auch mit Art. 25 Abs. 6 EU-DatenschutzRL kollidieren dürfte, verbleibt bei Unterlassen dieser Prüfungshandlungen gleichwohl das abstrakte Rechtswidrigkeitsrisiko bei dem die Daten übermittelnden Partner. Die Übermittlung von personenbezogenen Daten an einen Partner, der in den USA belegen ist, wird bei bloßer Safe Harbor-Zertifizierung daher in aller Regel mit erheblichem Bußgeldrisiken verbunden sein; überdies kann die Aufsichtsbehörde unter bestimmten Voraussetzungen auch die Untersagung des Datentransfers anordnen, wenn sie der Auffassung ist, die vorgelagerten – angeblichen – Prüfungspflichten seien nicht erfüllt worden, § 38 Abs. 5 S. 2 BDSG.

Will man diesem Risiko angemessen begegnen, verbliebe nach der zuvor erläuterten Ausgangsentscheidung der Aufsichtsbehörden aus dem Jahre 2010 in aller Regel nur der Rückgriff auf Standard-Vertragsklauseln oder bindende Unternehmensrichtlinien. Die zweite Alternative der bindenden Unternehmensrichtlinien (sog. „Binding Corporate Rules", kurz „BCL") scheiden in aller Regel aus, da diese bloß den konzerninternen Datenaustausch im Fokus haben, woran sich auch nichts mit der vor kurzem erfolgten Einführung sog. Processor Binding Corporate Rules („PBCR")[258] geändert haben dürfte.[259] Bei I4.0 steht aber vor allem die Produktions- und damit Verarbeitungskette zwischen verschiedenen externen Partnern in Frage.

Letztlich verblieben nach der aufsichtsbehördlichen Entscheidung aus dem Jahre 2010 daher nur noch EU-Standardvertragsklauseln, um ein angemessenes Datenschutzniveau bei einem Produktionsbezug zu den USA herzustellen. Diese existieren in drei verschiedenen Fassungen (aus den Jahren 2001[260], 2004[261] und 2010[262]), wobei die Wahl der zutreffenden Fassung in erster Linie abhängig davon ist,

258 Vgl. Artikel-29-Datenschutzgruppe, WP 195 vom 6.6.2012 (00930/12/DE), WP 195a vom 17.09.2012 und WP 204 vom 19.4.2013 (00658/13/DE).
259 Behling/Abel/Filip, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 5 Rn. 205; Filip, ZD 2013, 51, 59.
260 Sog. Set I, Abl. EG Nr. L 181/19.
261 Sog. Set II, Abl. EG Nr. L 385/74.
262 ABl. EG v. 12.2.2010, Nr. L 39/5.

welche Verarbeitungssituation gegeben ist („Controller to Controller“ oder „Controller to Processor“). Wie bereits im Zusammenhang mit der Auftragsdatenverarbeitung ausgeführt, dürfte die Auftragsdatenverarbeitungssituation, die der Fallgruppe „Controller to Processor“ entspricht, bei dem Datenaustausch im Rahmen von I4.0 nur im Ausnahmefall gegeben sein. Deshalb dürften in erster Linie die Standardvertragsklauseln aus den Jahren 2001 und 2004 zu verwenden sein, wobei die zutreffende Wahl nach Auffassung der Aufsichtsbehörden u. a. auch davon abhängig sein soll, ob Beschäftigtendaten von der Übermittlung betroffen sind oder nicht. Falls Beschäftigtendaten betroffen sind, sei die Verwendung der EU-Standardvertragsklauseln aus dem Jahre 2001 geboten[263], die allerdings – wenig interessengerecht – eine gesamtschuldnerische Haftung von Datenexporteur und -importeur vorsehen.[264]

Aber unabhängig davon, welche Fassung der EU-Standardvertragsklauseln für die Datenübermittlung an Partner in den USA verwendet würden, gehen die Aufsichtsbehörden aufgrund der offenkundig gewordenen Spionageaktivitäten der NSA nunmehr davon aus, dass auch bei Vereinbarung von EU-Standardvertragsklauseln ein sicheres Datenschutzniveau von Datenempfängern in den USA nicht mehr unterstellt werden könne.[265] Da man bis zur Klärung des Sachverhaltes – die bis heute noch nicht erfolgt sein dürfte – seitens der Aufsichtsbehörden überdies auch keine Genehmigungen mehr für Übermittlungen personenbezogener Daten in die USA aussprechen wolle[266], haben Unternehmen – mit Ausnahme von ggfs. Einwilligungserklärungen und Betriebsvereinbarungen – de facto keine Möglichkeit mehr, rechtssicher Daten in die USA zu übermitteln.

Damit verbleibt zum jetzigen Zeitpunkt nur festzustellen, dass eine Weitergabe von personenbezogenen Daten in der Produktionskette sich in aller Regel nur mit rechtlichen Risiken realisieren lässt, wenn ein Partner in den USA belegen ist.

- Partner in anderen unsicheren Drittstaaten

Haben Partner ihren Sitz in anderen nicht sicheren Drittstaaten, stellen insbesondere EU-Standardvertragsklauseln probate Mittel dar, um ein angemessenes Datenschutzniveau bei den Partnern herzustellen. Allerdings empfiehlt es sich, von den außereuropäischen Partnern überprüfen zu lassen, ob die europäischen Muster einschließlich der getroffenen Festlegungen mit den nationalen Datenschutzanforderungen korrespondieren, da anderenfalls Rechtswidrigkeitsrisiken nach deren nationalen Datenschutzgesetzen drohen können.[267]

Flankierend können gemäß § 4c Abs. 1 S. 1 Nr. 1 BDSG auch Einwilligungserklärungen von den Betroffenen zwecks Legitimation des Drittstaatentransfers eingeholt werden, wenngleich aus der hierbei herzustellenden Transparenz folgt, *„dass die betroffene Person über das konkrete Risiko der Übermittlung der Daten in ein Land ohne angemessenes Schutzniveau ordnungsgemäß [zu informieren] ist. Damit besteht die Pflicht zu einer umfassenden Aufklärung, die Informationen darüber beinhalten muss, auf welche personenbezogenen Daten und auf welche Verarbeitungsvorgänge sich die Zustimmung bezieht; insbesondere bedarf es der Angabe des Empfängers und des Zielortes [...]. Der Betroffene muss auch auf die dortigen Verarbeitungsvoraussetzungen, insbesondere auf etwaige Auswertungen, Überwachungen und sonstige Nutzungen hingewiesen werden.“*[268]

Die flankierende Einwilligungseinholung kann sich trotz der dezidierten Informationspflichten empfehlen, wenn eine Einwilligung ohnehin eingeholt wird. Gerade im Endkundenbereich wird dies – wie auch im Zusammenhang mit unserem Beispiel (1) ausgeführt – nicht selten der Fall sein, sodass die Einwilligungseinholung insoweit praxisrelevant auch bezüglich der Legitimation von Drittstaatentransfers sein kann.

In Bezug auf Beschäftigtendaten kommt auch der Abschluss von Betriebsvereinbarungen zwecks Legitimation des Drittstaatentransfers in Betracht, dies allerdings

263 Behling/Abel/Filip, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 4 Rn. 148.
264 Vgl. Behling/Abel/Filip, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 4 Rn. 148.
265 Vgl. Pressemitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24.7.2013, abrufbar unter https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen236.c.9283.de
266 Vgl. Pressemitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24.7.2013, abrufbar unter https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen236.c.9283.de
267 So ist etwa in der Türkei die Aufzeichnung und damit denkgesetzlich auch der Export von sensitiven Daten i.S.v. § 3 Abs. 9 BDSG unter Strafe gestellt und muss folglich ausgeschlossen werden, vgl. Art. 135 Abs. 2 des Türkischen Strafgesetzbuches (Gesetz Nr. 5237 v. 26.09.2004).
268 Gola/Schomerus, BDSG, 11. Aufl. 2012, § 4c Rn. 5.

nur dann, wenn diese hinreichende Garantien für die Betroffenenrechte vorsieht und sich die datenempfangenden Partner in den Drittstaaten diesen Garantien per vertraglicher Vereinbarung mit dem datenübermittelnden Partner unterwerfen.[269]

4.4.4.3.2 Bestehende Risiken unter Zugrundelegung des DS-GVO-E

Bei Zugrundelegung des DS-GVO-E ist im Zusammenhang mit der Grundkonstellation 1c) festzustellen, dass auch nach dem DS-GVO-E die Weitergabe von personenbezogenen Daten an einen Partner in einem Drittstaat ohne die vorherige Sicherstellung eines angemessenen Datenschutzniveaus mit erheblichen Bußgeldern, die deutlich über den derzeit möglichen liegen, geahndet werden kann.[270] Die bereits erwähnten Kommissionsentscheidungen sollen nach dem DS-GVO-E gestärkt werden, indem bspw. auch negative Feststellungsentscheidungen bezüglich der Angemessenheit eines Datenschutzniveaus ergehen können sollen.

Schließlich wird aber auch bei Verarbeitungssachverhalten, die sich ausschließlich auf Drittstaaten beziehen, stets zu klären sein, ob nicht ebenfalls die Regelungen des DS-GVO-E Anwendung finden, da der Anwendungsbereich der DS-GVO nach dem Entwurf unter bestimmten Voraussetzungen auf Drittstaaten ausgeweitet wird.[271]

Im Übrigen ergeben sich keine wesentlichen Änderungen zu den zuvor im Zusammenhang mit dem BDSG erläuterten Risiken.

4.4.4.4 Grundkonstellation 2a):

Bei der Grundkonstellation 2a) handelt es sich um eine netzförmige Kooperationsstruktur mit Partnern ausschließlich mit Sitz im Inland. Zwischen den unterschiedlichen Partnern werden personenbezogene Daten ausgetauscht.

Hinsichtlich der Risiken möchten wir auf die unter Ziff. 4.4.4.1.1 und 4.4.4.1.2 getroffenen Feststellungen verweisen. Es ergibt sich insofern nur eine Änderung im Hinblick darauf, dass die die Erfüllbarkeit der materiellen Tatbestandsvoraussetzungen für eine ADV-Vereinbarung mangels eines zentralen Partners noch unwahrscheinlicher erscheint.

4.4.4.5 Grundkonstellation 2b):

Bei der Grundkonstellation 2b) handelt es sich um eine netzförmige Kooperationsstruktur mit Partnern im Inland sowie mit Sitz im EWR-Ausland. Zwischen den verschiedenen Partnern werden personenbezogene Daten ausgetauscht.

Bezüglich der hier bestehenden Risiken möchten wir auf die oben (Ziff. 4.4.4.2.1 und 4.4.4.2.2) gemachten Ausführungen verweisen. Im Übrigen besteht darüber hinaus bei der derzeit geltenden Rechtslage das erhöhte Risiko, dass ausländische Datenschutzgesetze durch den Datenaustausch verletzt werden, da bei dieser Konstellation personenbezogene Daten auch unmittelbar zwischen im Ausland ansässigen Partnern ausgetauscht werden können, sodass in diesen Fällen auch mehrere ausländische Datenschutzgesetze gleichzeitig tangiert sein können. Nach Inkrafttreten des DS-GVO-E, würde dieses Risiko aufgrund der Vereinheitlichungswirkung indes wieder geringer ausfallen (siehe Ziff. 4.4.4.2.2).

4.4.4.6 Grundkonstellation 2c)

Bei der Grundkonstellation 2c) handelt es sich um eine netzförmige Kooperationsstruktur mit Partnern im Inland sowie mit Sitz im EWR- und Nicht-EWR-Ausland. Zwischen den unterschiedlichen Partnern werden personenbezogene Daten ausgetauscht.

Schließlich ergeben sich auch mit Blick auf die Grundkonstellation 2c) keine wesentlichen Änderungen zu den bereits unter Ziff. 4.4.4.3.1 und 4.4.4.3.2 aufgeführten Risiken. Im Übrigen besteht darüber hinaus sowohl bei der derzeit geltenden Rechtslage als auch nach Inkrafttreten des DS-GVO-E das Risiko, dass, weil personenbezogene Daten auch mit Partnern im (Nicht-EWR-)Ausland ausgetauscht werden, mehrere verschiedene ausländische Rechtsordnungen betroffen sein und entsprechend verletzt werden können.

Nach dem Inkrafttreten des DS-GVO-E werden überdies die Partner außerhalb des EWR prüfen müssen, inwieweit sie auch in den Anwendungsbereich der Datenschutz-Grundverordnung fallen, um die danach drohenden, immens hohen Bußgelder zu vermeiden.

269 Vgl. Gola/Schomerus, BDSG, 11. Aufl. 2012, § 4c Rn. 10.
270 Bis zu 100.000.000 EUR oder fünf Prozent des weltweiten Umsatzes, je nachdem, was höher ist.
271 Vgl. Art. 3 DS-GVO-E.

4.4.5 WTO-Recht

In einem nächsten Schritt ist mit Blick auf die zwei Grundkonstellationen zu prüfen, welche rechtlichen Risiken aus dem WTO-Recht für die Partner erwachsen können:

4.4.5.1 GATS

Das GATS kann insoweit nur anwendbar sein, wenn im Rahmen von I4.0 eine Dienstleistungserbringung erfolgt, also bspw. die Fernwartung durch einen Partner auf den Systemen eines anderen Partners in der Produktionskette erfolgt.

4.4.5.1.1 Grundkonstellationen 1a) und 2a)

Bei diesen rein innerdeutschen Konstellationen ist das GATS nicht anwendbar, da kein „grenzüberscheitender" Handel mit Dienstleistungen stattfinden kann. Für die Grundkonstellationen 1a) und 2a) erwachsen aus dem GATS folglich keine weiteren Risiken.

4.4.5.1.2 Grundkonstellationen 1b), 1c), 2b) und 2c)

Sofern in den vorliegenden Grundkonstellationen 1b), 1c), 2b) und 2c) eine Dienstleistung in einem WTO-Staat erbracht wird und in einem anderen WTO-Staat empfangen wird, können die Regelungen des GATS indes vom Grundsatz her anwendbar sein. Dabei zielt das GATS auf den Abbau von Hemmnissen im internationalen Dienstleistungshandel ab, also auf die Erweiterung, die Transparenz und die fortschreitende Liberalisierung zur Förderung des Wirtschaftswachstums aller Handelspartner.[272] Insofern werden den WTO-Mitgliedsstaaten Regelungen auferlegt, dass bspw. Dienstleistungserbringern aus allen WTO-Mitgliedsstaaten grundsätzlich unter gleichen Voraussetzungen die Dienstleistungserbringung in einem WTO-Mitgliedsstaat ermöglicht werden muss.

Es heißt bspw. in Art. 2 Abs. 1 GATS: *„Jedes Mitglied gewährt hinsichtlich aller Maßnahmen, die unter dieses Abkommen fallen, den Dienstleistungen und Dienstleistungserbringern eines anderen Mitglieds unverzüglich und bedingungslos eine Behandlung, die nicht weniger günstig ist als die, die es den gleichen Dienstleistungen oder Dienstleistungserbringern eines anderen Landes gewährt."*

Von diesem Grundsatz können jedoch unter bestimmten Voraussetzungen Ausnahmen zugelassen werden, vgl. Art. 2 Abs. 2 GATS.

Unmittelbare Risiken für Akteure im Rahmen von I4.0 birgt ein etwaiger Verstoß gegen die Regelungen des GATS nicht, vielmehr handelt es sich dabei um ein multilaterales völkerrechtliches Übereinkommen, welches zunächst nur in hierfür eingerichteten Streitbeilegungsverfahren von den Mitgliedsstaaten durchgesetzt werden kann.[273] Es kann jedoch ggf. als Auslegungshilfe herangezogen werden, wenn dahingehende Streitigkeiten zwischen den Partnern erwachsen.

4.4.5.2 TRIPS Abkommen

Es stellt sich allerdings die Frage, ob etwas anderes in Bezug auf die Normen des TRIPS gilt.

Auch bei dem TRIPS handelt es sich um ein multilaterales zwischenstaatliches Abkommen, welches grundsätzlich nur bei einer Grenzüberschreitung Anwendung finden kann, sodass es im Hinblick auf die Grundkonstellationen 1a) und 2a) bereits an einer Anwendbarkeit des TRIPS fehlt.

Spezifische Risiken für die Akteure von I4.0 unmittelbar aus dem TRIPS, erwachsen aber auch in den übrigen Fallkonstellationen nicht, da dieses keine unmittelbaren Rechtswirkungen für diese entfaltet.[274] Vielmehr sind die hieraus resultierenden Rechte auch allein von den Mitgliedsstaaten im Verfahren der Streitbeilegung geltend zu machen.[275] Umstritten ist, ob die Wertungen des TRIPS in die Auslegung der zu erläuternden lauterkeitsrechtlichen Tatbestände miteinbezogen werden müssen.[276] Daher ist allein fraglich, ob durch das TRIPS als Auslegungshilfe Risiken für die beteiligten Parteien aufkommen können; hierauf wird an anderer Stelle[277] noch näher eingegangen.

272 Vgl. Einleitung zum GATS.
273 Grabitz/Hilf/Vedder/Lorenzmeier, Das Recht der Europäischen Union, 40. Aufl. 2009, Art. 133 EGV Rn. 148 ff; hierzu auch EuGH, Urteil vom 1. 3. 2005 – C-377/02 Léon Van Parys NV/Belgisch Interventie – en Restitutiebureau BIRB, EuZW 2005, 214.
274 Vgl. hierzu Mcquire/Joachim/Künzel/Weber, GRUR Int. 2010, 829, 831.
275 Vgl. Art. 64 TRIPS.
276 Ohly, GRUR 2014, 1,3.
277 Hierzu unten Ziff. 4.4.6.

4.4.6 Gesetzlicher Geheimnisschutz in Deutschland

Der Schutz von Betriebs- und Geschäftsgeheimnissen des TRIPS ist in Deutschland über die §§ 17, 18 UWG umgesetzt worden. Damit sind gemäß der Ausgangsfrage Betriebs- und Geschäftsgeheimnisse in Deutschland geschützt. Insbesondere in Bezug auf § 17 UWG ist allerdings fraglich, ob sein Schutzziel tatsächlich dazu beitragen kann, den Datenaustausch im Rahmen von I4.0 zu fördern. Im Einzelnen:

In allen beschriebenen Grundkonstellationen ist es möglich, dass aufgrund der übergreifenden Vernetzung von elektronischen Systemen ein Partner bzw. ein Mitarbeiter eines Partners Zugriff auf Informationen erhält, die ein Geschäfts- oder Betriebsgeheimnis i.S.d. § 17 UWG eines anderen Partners in der Produktionskette darstellen.

Denn ein *„Geschäfts- oder Betriebsgeheimnis ist jede im Zusammenhang mit einem Geschäftsbetrieb stehende nicht offenkundige, sondern nur einem begrenzten Personenkreis bekannte Tatsache, an deren Geheimhaltung der Unternehmensinhaber ein berechtigtes wirtschaftliches Interesse hat und die nach seinem bekundeten oder doch erkennbaren Willen auch geheim bleiben soll.“*[278]

Sofern hierzu keine weitere Vereinbarungen zwischen den in Rede stehenden Partnern getroffen werden, besteht deshalb das Risiko, dass die Datenweitergabe in der Produktionskette als ein unbefugtes Offenbaren von Betriebs- und Geschäftsgeheimnissen zu qualifizieren sein könnte (§ 17 Abs. 1 UWG), die sich der empfangende Partner durch Anwendung technischer Mittel unbefugt verschafft (§ 17 Abs. 2 Nr. 1a UWG). Dies wiederum kann zu lauterkeitsrechtlichen Ansprüchen der Partner untereinander führen, wenn diese – was sich häufig kaum ausschließen lassen wird – Mitbewerber sind[279]. Überdies kommen strafrechtliche Sanktionen auch gegen die verantwortlich handelnden Mitarbeiter auf allen Seiten der Produktionskette in Betracht[280], darüber hinaus auch zivilrechtliche Ansprüche.[281] Diese Risiken stehen der Förderung des Informationsaustausches ggfs. entgegen.

Hinzu kommt, dass § 17 Abs. 1 UWG in seinem persönlichen Anwendungsbereich hinter den Anforderungen des TRIPS zurückbleibt. So kann nach § 17 Abs. 1 UWG nur Täter eines Geheimnisverrates sein, wer Beschäftigter des Geheimnisinhabers ist, während Art. 39 Abs. 2 TRIPS allgemein darauf abstellt, ob ein Geheimnis dem „Empfänger“ anvertraut worden ist; auf die Beschäftigteneigenschaft kommt es also nach TRIPS nicht an.[282] Entsprechend stellen auch die Vorschriften anderer WTO-Mitgliedstaaten nach dem Vorbild des Art. 39 Abs. 2 TRIPS allgemein darauf ab, ob das Geheimnis dem Empfänger anvertraut wurde. Da der persönliche Anwendungsbereich des § 17 Abs. 1 UWG hinter dem Schutz des Völkerrechts und der korrespondierenden nationalen Vorschriften der anderen WTO-Mitgliedstaaten zurückbleibt, kann dies zu weiteren Problemen zwischen den Partnern führen.

Zwar kann im bestimmten Umfang § 823 Abs. 1 BGB diese Lücke ggfs. schließen, da die Rechtsprechung Betriebs- und Geschäftsgeheimnisse bereits als sonstige Rechte im Sinne dieser Vorschrift anerkannt hat, aber nur soweit diese den eingerichteten und ausgeübten Gewerbebetrieb betreffen.[283] Da deshalb Schutzlücken im Vergleich zum TRIPS auch unter Heranziehung von § 823 Abs. 1 BGB verbleiben dürften, sind die Partner der Produktionskette gut beraten, sich über ein einheitliches Schutzniveau bezüglich des Austauschs und der Nutzung von Betriebs- und Geschäftsgeheimnissen zu verständigen. Dies kann über flankierende „Non Disclosure Agreements“ (NDA) oder ähnliche Vereinbarungen erfolgen, wobei diese sich auch dazu äußern sollten, in welchem Umfang der Umgang mit Betriebs- und Geschäftsgeheimnissen der jeweils anderen Partner erlaubt ist, um die eingangs erläuterten Rechtswidrigkeitsrisiken bei deren Übermittlung und Empfang zu vermeiden.

Allerdings ist auch in Bezug auf den Geheimnisschutz eine weitere Rechtsentwicklung zu beachten. Die EU-Kommission hat am 28. November 2013 einen Vorschlag für eine Verordnung zum Schutz von Geschäftsgeheimnissen[284] vorgestellt. Damit soll der bisherige Schutz über § 17 f. UWG durch einen einheitlichen EU-weit gültigen Schutzstandard ersetzt werden. Unmittelbar anwendbar in den einzelnen

278 Köhler/Bornkamm/Köhler, UWG, 32. Aufl. 2014, § 17
279 Köhler/Bornkamm/Köhler, UWG, 32. Aufl. 2014, § 17 Rn. 51.
280 Köhler/Bornkamm/Köhler, UWG, 32. Aufl. 2014, § 17 Rn. 66 ff.
281 Köhler/Bornkamm/Köhler, UWG, 32. Aufl. 2014, § 17 Rn. 52 ff.
282 Ohly, GRUR 2014, 1, 5.
283 MüKoBGB/Wagner, 6. Aufl. 2013, § 823 Rn. 228 mit Verweis auf BGHZ 16, 172, 175 = NJW 1955, 628, 629, und BGHZ 17, 41, 50 f. = NJW 1955, 829, 830.
284 Vorschlag für eine RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung /* COM/2013/0813 final - 2013/0402 (COD) */.

Mitgliedsstaaten kann dieser jedoch erst durch die jeweilige nationalstaatliche Umsetzung werden. Diesbezügliche Entwürfe liegen derzeit noch nicht vor und können daher nicht in die hiesige Betrachtung einbezogen werden.

4.4.7 Grundsätze zur Exportkontrolle

Schließlich kann die Nutzung von I4.0 exportkontrollrechtlichen Beschränkungen unterliegen, und zwar in zweierlei Hinsicht: Zum einen fällt bereits jedes spezifische Wissen, das für die Entwicklung, Herstellung oder Verwendung eines der Exportkontrolle unterliegenden Produktes nötig ist, unter dieselbe Exportbeschränkung wie das Produkt selbst. Zum anderen können insbes. Verschlüsselungstechnologien, deren Verwendung vor allem bei einer Fernübertragung von vertraulichen Informationen im Rahmen der Nutzung von I4.0 über das Internet zumindest zweckmäßig sein dürfte, einer eigenständigen Exportbeschränkung unterliegen, welche bspw. gegen eine die Dual-Use-Verordnung der Europäischen Union (EU/428/2009), das Außenwirtschaftsgesetz und die Außenwirtschaftsverordnung verstoßen kann.

Wie bereits unter 3.3.6 dargestellt regelt das deutsche Außenwirtschaftsrechts primär die Ausfuhr von Gütern, die ihrer Natur nach militärischen Zwecken dienen (Waffen und andere Rüstungsgüter), während die Dual-Use-Verordnung (EU/428/2009) die Aus- und Durchfuhr von Gütern reguliert, die sowohl zu zivilen als auch potentiell zu militärischen Zwecken verwendet werden könnten (dual-use).

Der Begriff der Güter umfasst nach Artikel 1 der Dual-Use-Verordnung (EU/428/2009) insbesondere auch Datenverarbeitungsprogramme und Technologien.

Unter einer Ausfuhr versteht die Dual-Use-Verordnung (EU/428/2009) unter anderem auch die Übertragung von Software oder Technologien mittels elektronischer Medien, sowie bereits das Bereitstellen solcher Software oder Technologie in elektronischer Form.

Auch die Bereitstellung etwa von Hochleistungsrechnen kann u. U. in den Anwendungsbereich der Exportkontrolle fallen[285].

Eine Vernachlässigung der unternehmensinternen Exportkontrolle kann sehr ernste Risiken sowohl für das Unternehmen selbst als auch für die in der Unternehmensleitung verantwortlichen Personen nach sich ziehen.[286]

Solche Verstöße können möglicherweise strafrechtlich geahndet werden (§ 34 AWG) oder Bußgelder nach sich ziehen (§ 33 AWG bis zu 500.000 Euro oder gemäß § 130 des Gesetzes über Ordnungswidrigkeiten (OWiG) sogar bis zu 1.000.000 Euro). Diese Geldbußen können auch gegen das Unternehmen selbst verhängt werden, § 30 OWiG.[287] Auch das Risiko von Imageschäden besteht.[288]

Entsprechend ist es unumgänglich, dass sich die Partner vor Beginn des wechselseitigen Datenaustauschs darüber in Kenntnis setzen, welche Technologien sie verwenden und welche Informationen sie austauschen dürfen, ohne der Ausfuhrgenehmigung zu unterliegen.

Auch kann es in Zweifelsfällen geboten sein, sich bei Unklarheiten vorab bei dem Bundesamt für Wirtschaft und Ausfuhrkontrolle zu erkundigen, dies insbesondere was Fragen der Unterrichtungspflicht und Genehmigungspflichtigkeit oder -fähigkeit betrifft.

4.4.8 Rechtliche Ableitungen für die konkret betrachteten Fallbeispiele

Für die in der Gesamtuntersuchung im Fokus stehenden Fallbeispiele lassen sich daraus die folgenden Risiken ableiten. Exemplarisch soll dies am Fallbeispiel Fernwartung (Maschinenbau) erläutert werden:

4.4.8.1 Betreiber-zentrierte Lösung[289]

Servicetechniker der einzelnen Herstellerunternehmen von Maschinen in einer Produktionskette erhalten Fernzugriff auf eine Plattform des Unternehmens, welches die Maschinen in seiner Produktionskette verwendet (im Folgenden „Anwender“ oder „Anwendungsunternehmen“). Für die Dauer der Wartung wird auf Servern des Anwendungsunternehmens für jede Maschine oder Komponente, die gewartet werden soll, eine virtuelle Maschine (VM) eingerichtet. Auf

285 Hoeren, MMR 2012, 715,
286 Umnuß/Schlegel/Cammerer, Corporate Compliance Checklisten, 2. Aufl. 2012, Kapitel 4 Rn. 9-16.
287 Umnuß/Schlegel/Cammerer, Corporate Compliance Checklisten, 2. Aufl. 2012, Kapitel 4 Rn. 10.
288 Umnuß/Schlegel/Cammerer, Corporate Compliance Checklisten, 2. Aufl. 2012, Kapitel 4 Rn. 16.
289 Sehen Sie zu den Einzelheiten die Erläuterungen im Fallbeispiel.

diese VM erhält der Service-Techniker eines Herstellers per Terminal-Emulation einen Zugriff. Daten aus der Maschine, die auf deren Abbild in der VM zur Verfügung stehen, können vom Anwender gefiltert werden.

Datenschutzrechtliche Risiken

Datenschutzrechtliche Risiken bestehen, sofern sich nicht ausschließen lässt, dass Servicetechniker bei Vornahme ihrer Wartungstätigkeit auch auf personenbezogene Daten zugreifen können. Dies halten wir in erster Linie für Beschäftigtendaten wahrscheinlich, da solche bereits heute nicht selten auch auf den zu wartenden Maschinen gespeichert sind. Entsprechend gehen wir in unserer nachfolgenden Betrachtung davon aus, dass nur Beschäftigtendaten betroffen sein werden. Deutlich machen soll dies nachfolgendes

Beispiel (3):

In den anwenderspezifischen Konfigurationsdaten einer Maschine ist hinterlegt, welche Mitarbeiter bei dem Anwender Anpassungen an der Konfiguration der Maschine vorgenommen haben (Hans Müller hat am 2. Februar 2015 die Farbcodierung der Lackiermaschine derart verändert, dass nur noch die genau bezeichneten Farbtöne A, B und C bei dem zu wartenden Lackierroboter verfügbar sind). Bei der Wartung der Maschine durch einen Servicetechniker des Herstellers besteht die Möglichkeit, dass dieser die genannten Daten einsieht.

Sofern kein datenschutzrechtlicher Erlaubnistatbestand für den in Beispiel (3) beschriebenen Vorgang gegeben ist, wäre dieser als *„unbefugte Erhebung oder Verarbeitung personenbezogener Daten“* i. S. v. § 43 Abs. 2 Nr. 1 BDSG zu qualifizieren. Die zuständige Datenschutzaufsichtsbehörde kann dies mit einem Bußgeld von grundsätzlich bis zu 300.000 EUR ahnden. Nach Inkrafttreten der DS-GVO-E kann dieses Bußgeld nach dem jetzigen Gesetzgebungsstand 100.000.000 Euro oder fünf Prozent des weltweiten Umsatzes betragen, je nachdem, was höher ist.

Datenschutzrechtliche Erlaubnistatbestände

Für die insoweit in Betracht kommenden Erlaubnistatbestände[290] gilt Folgendes:

Die Einholung von Einwilligungserklärungen von den in dem Beispiel (3) betroffenen Beschäftigten unterliegt nicht unerheblichen rechtlichen Hürden. Dies zum einen vor dem Hintergrund, dass die Möglichkeit zur Einholung rechtssicherer Einwilligungserklärungen im Beschäftigungsverhältnis aufgrund Besonderheiten des bestehenden Ober-Unter-Ordnungsverhältnisses im Einzelfall umstritten sein kann,[291] wenngleich mit den Erwägungen des BAG im Urteil vom 11. Dezember 2014, AZ: 8 AZR 1010/13 davon auszugehen ist, dass ein „faktischer Zwang“ im Beschäftigtenverhältnis nicht generell zu unterstellen ist.

Zum anderen aus dem Grunde, weil der Einwilligungstext eine hinreichende Transparenz über die möglichen Datenverarbeitungen herstellen muss[292], was sich aber nicht immer leicht realisieren lassen wird. So muss etwa sichergestellt sein, dass der betroffene Beschäftigte bereits vor Erteilung der Einwilligung über die Hersteller informiert wird, bei denen seine Daten dann infolge der Wartung ggfs. verarbeitet oder genutzt werden, über den Zweck der Verarbeitung und über weitere Empfänger auf Seiten des wartenden Herstellers (z. B. konzerninterne IT-Dienstleister).

Dies alles wird sich bei einer Einwilligungseinholung durch das Anwendungsunternehmen aber nicht immer rechtssicher realisieren lassen, zumal für jede Wartungsart ggfs. eine andere Einwilligung benötigt wird. Da ohnehin generell umstritten ist, ob eine Einwilligungserklärung im Beschäftigungsverhältnis legitimieren kann, erscheint ein Rückgriff (allein) auf diesen Erlaubnistatbestand eher risikobehaftet.Der Abschluss einer Betriebsvereinbarung kommt, wie bereits im Zusammenhang mit unseren allgemeinen Ausführungen erläutert, grundsätzlich nur in Betracht, sofern das wartende Herstellerunternehmen und das Anwenderunternehmen einem Konzern angehören, was regelmäßig nicht der Fall sein dürfte. Aus der praktischen Erfahrung lässt sich ferner ableiten, dass das wartende Unternehmen i. d. R. auch nicht bereit sein wird, sich entsprechenden Betriebsvereinbarungen des Anwendungsunternehmens zu unter-

290 Hierzu ausführlich oben Ziff. 4.4.4.1.1.1.

291 Ob eine freiwillige Einwilligungserklärung eines Beschäftigten an seinen Arbeitgeber aufgrund des im Arbeitsverhältnisses bestehenden faktischen Zwangs möglich ist, ist umstritten, vgl hierzu Behling/Abel/Gola, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 8 Rn. 10; Däubler/Hjort/Schubert/Wolmerath/Hilbrans, Arbeitsrecht, 3. Aufl. 2013, BDSG § 4a, Rn. 3.

292 Hierzu Behling/Abel/Ringel, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 10 Rn. 118.

293 Hierzu oben Ziff. 4.4..4.1.1.1., Betriebsvereinbarungen und Tarifverträge.

werfen[293], was umso mehr gilt, wenn das wartende Unternehmen nicht in Deutschland sitzt. Betriebsvereinbarungen erscheinen deshalb ebenfalls allenfalls beschränkt geeignet, die im Zuge der Fernwartung erfolgenden Verarbeitungen zu legitimieren.

Das Eingreifen gesetzlicher Erlaubnistatbestände erscheint dagegen zumindest möglich. Lässt sich die Fernwartung nur realisieren, wenn auch beschäftigtenbezogene Daten eingesehen werden, spricht vieles für ein Eingreifen des Erlaubnistatbestandes des § 32 Abs. 1 S. 1 BDSG. Ist der Zugriff auf Beschäftigtendaten indes nicht zwingend erforderlich, aber nützlich, ist dieser, wie im Zuge der allgemeinen Ausführungen bereits erläutert, an § 28 Abs. 1 S. 1 Nr. 2 BDSG zu messen, was mit den bereits erläuterten Risiken verbunden ist.[294] Denn, wie ausgeführt, ist es umstritten, ob § 28 Abs. 1 BDSG neben § 32 BDSG anwendbar ist. Dabei dürfte zu unterstellen sein, dass im Zuge der Fernwartung nicht immer nur zwingend erforderliche (Protokollierungs-)Daten mit Beschäftigtenbezug ausgelesen werden, sondern auch lediglich nützliche. Es wird deshalb auch immer ein Rückgriff auf § 28 Abs. 1 S. 1 Nr. 2 BDSG erforderlich sein, dessen Legitimationswirkung im Beschäftigungsverhältnis aber fraglich ist.

In jedem Falle ist der Abschluss einer ADV-ähnlichen[295] Vereinbarung nach § 11 Abs. 5 BDSG erforderlich. So heißt es in § 11 Abs. 5 BDSG, dass die Absätze 1 bis 4 des § 11 BDSG (Datenverarbeitung im Auftrag) entsprechend gelten, *„wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei eine Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.“* So liegt es gerade im Falle einer Fernwartung.

Aus § 11 Abs. 5 BDSG folgt, dass die Regelungsdichte der danach zu schließenden Vereinbarung mit der einer ADV-Vereinbarung vergleichbar sein dürfte, aber an die Besonderheiten der Wartung angepasst werden muss.[296] Festzulegen sind beispielsweise die von der externen Stelle, also hier dem Herstellerunternehmen, vorzunehmenden Arten und ggf. Beschränkungen des Zugriffs, genaue Aussagen zu Art und Umfang der Wartung[297] sowie Art und Umfang der Protokollierung der (erlaubten) Zugriffe von Servicetechnikern auf die Plattform. In diesem Zusammenhang gilt es daher auch Umfang und Art des per Terminal-Emulation durchgeführten Zugriffs dezidiert zu erläutern.

Weiter ist zu beachten, dass zusätzlich bzw. ergänzend auch sicherzustellen ist, dass ein angemessenes Datenschutzniveau bei dem fernwartenden Unternehmen besteht, wenn dieses in Drittstaaten, z. B. in China oder in den USA, belegen ist. In diesem Falle sind EU-Standardverträge als Mittel der Wahl zu qualifizieren, die nach Auffassung der deutschen Aufsichtsbehörden allerdings um die Aspekte des § 11 (Abs. 5) BDSG zu ergänzen sind.[298] In Bezug auf ein wartendes Unternehmen in den USA besteht jedoch, wie ausgeführt, auch dann das Risiko, dass deutsche Datenschutzaufsichtsbehörden unterstellen würden, dass ein angemessenes Datenschutzniveau nicht sichergestellt worden ist und könnten deshalb ein Bußgeld gegen das Anwendungsunternehmen verhängen. Der Einsatz US-amerikanischer Fernwartungsunternehmen wird daher ohne eine Abstimmung mit der zuständigen Datenschutzaufsicht stets risikobehaftet sein.

Überdies gilt es bei bestehendem Auslandsbezug in jedem Falle auch die nationalen datenschutzrechtlichen Anforderungen zu beachten.

Technische und organisatorische Maßnahmen

Es besteht weiterhin das Risiko, dass bei der Fernwartung keine angemessenen technischen und organisatorischen Maßnahmen getroffen werden (bspw. Verzicht auf eine vorherige Freischaltung des Servicetechnikers durch einen Mitarbeiter des Anwenderunternehmens vor dem Zugriff auf die virtuelle Maschine), was insbesondere das erhöhte Risiko eines unerlaubten Datenabflusses begründet. Dies insbesondere kann den Verlust von Betriebs- und Geschäftsgeheimnissen zur Folge haben, was entsprechende Schäden auf Seiten des Anwendungsunternehmens auslösen kann.

DS-GVO-E

Die aus der DS-GVO-E für die Fernwartung folgenden Risiken entsprechen der unter Ziff. 4.4.4.1.2, 4.4.4.2.2 und 4.4.4.3.2 erläuterten Risikolage.

294 Vgl. auch Gola/Schomerus, BDSG, 11. Aufl. 2012, § 32 Rn. 12.
295 Nach überwiegender Auffassung liegt in einem solchen Fall keine unmittelbare ADV-Situation vor, da (Haupt-)Zweck eines Wartungsauftrages nicht die Datenverarbeitung ist (Gola/Schomerus, BDSG, 11. Aufl. 2012, § 11 Rn. 14 m. w. N.).
296 Simitis/Petri, BDSG, 8. Aufl. 2014, § 11 Rn. 102.
297 Gola/Schomerus, BDSG,11. Aufl. 2012, § 11 Rn. 14.
298 Behling/Abel/Filip, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 4 Rn. 153.

Risiken nach WTO-Recht

Unmittelbare Risiken für Akteure im Rahmen der Fernwartung und von I4.0 insgesamt birgt ein etwaiger Verstoß gegen die Regelungen des GATS oder TRIPS nicht, vielmehr handelt es sich hierbei um multilaterale völkerrechtliche Übereinkommen, welche zunächst nur in hierfür eingerichteten Streitbeilegungsverfahren von den Mitgliedsstaaten durchgesetzt werden können.[299]

Risiken nach Geheimnisschutzrecht

Sofern die bestimmte anwenderspezifische Konfiguration der Maschine in Beispiel (3) ein Betriebs- oder Geschäftsgeheimnis[300] darstellt, besteht das Risiko, dass die Zulassung des Datenzugriffs durch den Servicetechniker des Herstellerunternehmens als ein unbefugtes Offenbaren von Betriebs- und Geschäftsgeheimnissen zu qualifizieren ist (§ 17 Abs. 1 UWG). Tathandlung könnte durch Aufschaltung des Servicetechnikers des Herstellers auf die Anwender-Plattform bspw. ein „unbefugtes Verschaffen durch Anwendung technischer Mittel“ sein (vgl. § 17 Abs. 2 Nr. 1a UWG).

Dies kann zu lauterkeitsrechtlichen Ansprüchen des Anwenderunternehmens gegen das Herstellerunternehmen führen, wenn es sich bei Letzterem um einen Mitbewerber des Anwenderunternehmens handelt[301]. Überdies kommen strafrechtliche Sanktionen auch gegen die verantwortlich Handelnden Mitarbeiter auf allen Seiten in Betracht[302], darüber hinaus auch zivilrechtliche Ansprüche.[303]

Daher sollte in einem NDA geregelt werden, in welchem Umfang der Umgang mit Betriebs- und Geschäftsgeheimnissen der jeweils anderen Partner erlaubt ist, um die erläuterten Rechtswidrigkeitsrisiken bei deren Übermittlung und Empfang zu vermeiden.

Risiken nach Exportkontrollrecht

Risiken aus dem Exportkontrollrecht können sich in Beispiel (3) etwa dann ergeben, wenn spezielle Verschlüsselungstechniken bei Durchführung der Wartung angewandt werden, die unter die Dual-Use-Verordnung der Europäischen Union (EU/428/2009), das Außenwirtschaftsgesetz oder die Außenwirtschaftsverordnung fallen, was es entsprechend im Vorfeld der Implementierung einer Verschlüsselungstechnologie zu eruieren ist.

Solche Verstöße können möglicherweise strafrechtlich geahndet werden oder Bußgelder nach sich ziehen.[304] Diese Geldbußen können auch gegen das Unternehmen selbst verhängt werden, § 30 OWiG.[305] Überdies besteht das Risiko von Imageschäden.[306]

4.4.8.2 Hersteller-zentrierte Lösung[307]

Diese Lösung stellt sich im Wesentlichen wie die Betreiber-zentrierte Lösung dar. Der einzige Unterschied besteht darin, dass die virtuelle Maschine auf den Servern des Herstellers eingerichtet wird und der Zugriff der Servicetechniker daher über eine vom Hersteller betriebene Plattform erfolgt. Deshalb stellt sich die rechtliche Risikolage weitestgehend identisch mit der der Betreiber-zentrierten Lösung dar. Die hierzu gemachten Ausführungen gelten daher entsprechend.

Ergänzend hierzu ist anzumerken, dass neben der Vereinbarung nach § 11 Abs. 5 BDSG bezüglich der Fernwartungsdienstleistungen ggfs. zusätzlich eine ADV-Vereinbarung nach § 11 Abs. 1 BDSG zwischen Anwender und Hersteller abzuschließen ist, und zwar bezogen auf das Hosting der Plattform selbst. Werden hierbei anderweitige personenbezogene Daten des Anwendungsunternehmens verarbeitet, z. B. personenbezogene Zugangsdaten von dessen Beschäftigten, stellt dies eine „klassische“ Auftragsdatenverarbeitungssituation dar, die es entsprechend zusätzlich i.S.v. § 11 Abs. 1 bis 4 BDSG vertraglich abzubilden gilt.

299 Grabitz/Hilf/Vedder/Lorenzmeier, Das Recht der Europäischen Union, 40. Aufl. 2009, Art. 133 EGV Rn. 148 ff; hierzu auch EuGH, Urteil vom 1. 3. 2005 - C-377/02 Léon Van Parys NV/Belgisch Interventie - en Restitutiebureau BIRB, EuZW 2005, 214; vgl. hierzu auch Mcquire/Joachim/Künzel/Weber, GRUR Int. 2010, 829, 831.
300 Hierzu im Einzelnen oben Ziff. 4.4.6.
301 Köhler/Bornkamm/Köhler, UWG, 32. Aufl. 2014, § 17 Rn. 51.
302 Köhler/Bornkamm/Köhler, UWG, 32. Aufl. 2014, § 17 Rn. 66 ff.
303 Köhler/Bornkamm/Köhler, UWG, 32. Aufl. 2014, § 17 Rn. 52 ff.
304 Hierzu oben Ziff. 4.4.7 ausführlich.
305 Umnuß/Schlegel/Cammerer, Corporate Compliance Checklisten, 2. Aufl. 2012, Kapitel 4 Rn. 10.
306 Umnuß/Schlegel/Cammerer, Corporate Compliance Checklisten, 2. Aufl. 2012, Kapitel 4 Rn. 16.
307 Sehen Sie zu den Einzelheiten die Erläuterungen im Fallbeispiel.

4.4.8.3 Dienstleister-basierte Lösung

In rechtlicher Hinsicht stellen sich die Risiken dieser Lösung als eine Kombination der Risiken von anwender- und herstellerzentrierter Lösung dar.

So besteht der tatsächliche Unterschied zu den zuvor genannten Lösungen lediglich darin, dass die virtuelle Maschine auf den Servern eines dritten Dienstleisters eingerichtet wird und der Zugriff der Servicetechniker daher über eine vom Dienstleister betriebene Plattform erfolgt. Der Dienstleister stellt diesen Service auch grenzübergreifend verschiedenen Herstellern und Anwendern als Service zur Verfügung.

Bei dieser Lösung vereinigen sich die Risiken der Anwendungs- und der Hersteller-zentrierten Lösung deshalb mit der Abweichung, dass eine weitere Partei, der Dienstleister, in den Daten- und Informationsaustausch involviert ist. Da dieser nicht selbst die Fernwartung vornimmt, ist mit diesem eine „klassische" ADV-Vereinbarung nach § 11 Abs. 1 BDSG zu schließen, wobei hierzu entweder der Anwender oder der Hersteller angehalten ist, je nachdem von welcher Seite der Dienstleister eingesetzt wird. Zwischen Anwender und Hersteller ist indes ein Vertrag nach § 11 Abs. 5 BDSG abzuschließen.

Da der Dienstleister aber auch mit den bei der Fernwartung ausgetauschten Daten in Berührung kommen dürfte, sollten mit ihm auch Regelungen (NDA) zu dem Umgang mit Betriebs- und Geschäftsgeheimnissen getroffen werden.

4.5 Anwendung der Fallbeispiele auf das Referenzmodell

4.5.1 Bedrohungs- und Risikoeinschätzung

Eine Bedrohungs- und Risikoeinschätzung deckt vorhandene Probleme auf und zeigt damit, an welchen Stellen Handlungsbedarf besteht.

4.5.1.1 Modellierung des Fallbeispiels aus der Automobilindustrie

Das Fallbeispiel aus der Automobilindustrie trifft im Wesentlichen eine Aussage über eine sinnvolle Segmentierung und Abschottung von Produktionsnetzwerken über verschiedene Produktionsstandorte mittels Firewalls und deren Auswirkung auf eine reibungslose Inbetriebnahme von Produktionsanlagen. Im Entwurf des zugehörigen Datenflussdiagramms wurden deshalb Wartungsarbeiten als Prozess modelliert, der auf entsprechende Datenspeicher für die Konfiguration der im Fallbeispiel angeführten Leittechnik und Firewall-Systeme zugreift. Die Produktionsanlagen werden im Fallbeispiel abstrakt als Prozesse dargestellt, nur das Vorhandensein von OPC-UA-Servern in jeder Produktionsanlage wurde explizit genannt. Sowohl der Prozess für Wartungsarbeiten als auch der Prozess für die Firewall werden nicht in das Gesamtmodell übernommen. Zum einen stört ein zentraler Prozess, über den scheinbar alle Datenflüsse zwischen Vertrauensgrenzen abgewickelt werden die Semantik des Datenflussdiagramms erheblich. Praktisch werden Firewall-System schließlich auch als transparente Netzwerkkomponenten verstanden, deren Vorhandensein für jede IP-basierte Netzwerkinfrastruktur selbstverständlich sein sollte. In Bezug auf die speziellen Wartungsarbeiten an Firewall und Leitsystem, trifft auch das später behandelte Fallbeispiel zur Fernwartung gute Aussagen, die sich zur Übernahme in das Gesamtmodell eignen.

4.5.1.2 Modellierung des Fallbeispiels aus der chemischen Industrie

Das Fallbeispiel der chemischen Produktion weist auf die zunehmende Komplexität bei der Vernetzung einer Vielzahl von PLS- und MES-Systemen über mehrere Produktionsstandorte und Unternehmensgrenzen hinweg. Gegenüber dem Fallbeispiel aus der Automobilbranche wird hier auch auf das Vorhandensein einer Vielzahl von MES- und PLS-Systemen hingewiesen, welche die untergeordneten Systeme, wie z. B. FDI und PAT, auch innerhalb eines Produktionsnetzwerkes zusätzlich in separaten Sicherheits-Zellen betreiben. Insbesondere der isolierte Betrieb einzelner Systeme, wie z. B. einer Sicherheits-SPS wird einzig in diesem Fallbeispiel dargestellt.

4.5.1.3 Modellierung des Fallbeispiels zur Logistik

Das Fallbeispiel Logistik rückt sehr anschaulich die Bedeutung von Vertrauensnetzwerken im Fall einer Auslagerung unternehmenskritischer Logistik-Prozesse in Rechenzentren außerhalb der unternehmenseigenen IT-Systeme in den Vordergrund. Für die Modellierung des Fallbeispiels wurde angenommen, dass die Logistik-Systemlösung in einem Rechenzentrum außerhalb des Unternehmensnetzwerkes betrieben wird. Dies deckt sich sehr gut mit den Szenarien aus I4.0 in denen auch gerade solche Branchen-

lösungen als Software-as-a-Service (SaaS) aus der Cloud zugekauft werden. Die ebenfalls beschriebene Variante des lokalen Betriebs innerhalb des Unternehmens wurde deshalb außen vor gelassen.

Das Fallbeispiel geht bezüglich der verschiedenen Software-Prozesse und ausgetauschten Daten deutlich mehr ins Detail als die anderen Fallbeispiele. Neben der Einbeziehung einer Vielzahl externer Entitäten, wie z. B. Transportbörsen, Spediteure und Telematik-Anbieter, ist für die Modellierung von Vertrauensgrenzen insbesondere der Umstand interessant, dass innerhalb des Unternehmensnetzwerks des Anwenders praktisch nur noch Produktion und Transport als Prozesse betrachtet werden. Sämtliche für die Logistik relevanten Prozesse, wie Verkauf, Produktions- und Transportplanung, sowie der Lagerhaltung, laufen innerhalb des Rechenzentrums, welches auch die zentrale Datenbank für alle Prozesse betreibt.

4.5.1.4 Modellierung des Fallbeispiels zur Fernwartung

Das Fallbeispiel zur Fernwartung greift die Problematik der unterschiedlichen Vertrauensstellungen beim Fernzugriff von Maschinenherstellern auf beim Kunden aufgestellte Produktionssysteme und Maschinennetzwerke durch Servicetechniker auf. Das Fallbeispiel wird in drei unterschiedlichen Varianten ausgeführt, die sich im Wesentlichen durch den Standort der Portallösung beim Hersteller, Betreiber oder einem dritten externen Dienstleister unterscheiden. Letzteres wurde aufgrund seiner größeren Komplexität und damit besseren Eignung für zukünftige Fernwartungskonzepte in der dienstleisterzentrierten Variante für die Einbettung in das Teilnehmer- und Kommunikationsmodell ausgewählt. Aus der Extrapolation der Beschreibung des Fallbeispiels heraus wurden explizit VPN-Clients bzw. -Concentrator, sowie DMZ modelliert. Es wird davon ausgegangen, dass ein Servicetechniker grundsätzlich über eine Remote-Desktop-ähnliche Verbindung von einer virtualisierten Wartungsmaschine aus operiert. Diese wird dynamisch durch VPN-Technologie in das jeweilige Zielnetzwerk, beispielsweise das der zu wartenden Maschine, eingeklinkt. Das wäre im Idealfall ein vom restlichen Produktionsnetzwerk durch Security-Zellen oder als maschineneigenes Netzwerk abgeschottetes Netzwerk. Innerhalb einer Produktionsanlage wird prinzipiell immer das Vorhandensein von mindestens drei expliziten Prozessen angenommen, die auch Zugriff auf unterschiedliche Daten innerhalb der Produktion haben:

- Ein **„Produktions-PC“** ist eine PC-basierte, möglicherweise auch als Embedded-System ausgeführte, Komponente innerhalb einer Produktionsanlage/Maschine, welche im Vergleich zu den industriellen Steuerungskomponenten höherwertige Software-Prozesse innerhalb einer Betriebssystemumgebung ausführen kann. Mögliche Anwendungsfälle sind HMI oder das Speichern von für die Produktion relevanten Daten (Fabrikationsdaten) sowie anwenderspezifische Maschinenkonfigurationen.

- Als VPN-Client kann eine separate Hardware-Komponente dienen, die bei Bedarf eine VPN-Verbindung zum Service-Portal von innen nach außen aufbauen kann. Diese Komponente besitzt auch den exklusiven Zugriff auf einen Passwortspeicher zur Authentisierung von VPN-Verbindungen.

- Unter der Maschinensteuerung werden eine oder mehre industrielle Steuerungskomponenten, wie z. B. SPS mitsamt allen nachgelagerten Feldbussystemen verstanden. Wichtig ist hierbei vor allem, dass zunächst nur dieser Maschinensteuerung der unmittelbarere Zugriff auf das jeweilige Steuerprogramm einer Anlage bzw. deren Grundkonfiguration möglich ist. Ein indirekter Zugriff wird bspw. durch entsprechende Software auf dem Produktions-PC möglich.

4.5.1.5 Komposition eines Gesamtmodells

Aus der Summe der einzelnen Datenflüsse ergibt sich ein großes zusammenhängendes Modell mit den in den nachfolgenden Abschnitten vorgestellten Entitäten. Dabei ist noch zu erwähnen, dass in diesem Zuge auch eine Vereinheitlichung der in den Fallbeispielen verwendeten Begrifflichkeiten aus verschiedenen Industriesektoren im Sinne einer verwirrungsfreien Beleuchtung der IT-technisch relevanten Aspekte angestrebt wurde. Diese werden im Folgenden erläutert.

4.5.1.5.1 Rollen und Akteure

Rollen und Akteure können Unternehmen, Personen oder ext. Systeme sein, deren innere Funktion nicht modelliert wird. Im Teilnehmer- und Kommunikationsmodell werden sie daher nur neutral als Teilnehmer bezeichnet. Allen gemein ist, dass sie Daten mit Prozessen austauschen:

- **Auftraggeber (Kunde)/Auftragnehmer/Zulieferer:** Hierbei ist anzumerken, dass in den I4.0-Szenarien jedes produzierende Unternehmen in den Wertschöpfungsnetzwerken gleichermaßen Auftraggeber und Auftragnehmer ist. Die klassische Trennung zwischen Auftraggeber, Auftragnehmer und Zulieferer hat auch aus der Sicherheitsperspektive keine Bedeutung und dient nur noch bei der Betrachtung einer konkreten Wertschöpfungskette zur Unterscheidung der für diesen einen Betrachtungsfall relevanten Interessensparteien. Für die Darstellung im Teilnehmer- und Kommunikationsmodell könnten diese Begriffe deshalb streng genommen synonym verwendet werden. Sie werden hier aber dennoch im Sinne einer besseren Verständlichkeit des Modells und Abgrenzung verschiedener Kommunikationsschwerpunkte bei den Datenflüssen von und zu externen Entitäten auch einzeln dargestellt.

- **Hersteller/Betreiber (von Maschinen):** Diese Unterscheidung verschiedener Unternehmensrollen dient der Darstellung von Aspekten und unterschiedlichen Interessen sowie den damit einhergehenden Vertrauensgrenzen aus dem Fallbeispiel zur Fernwartung.

- **Anwender/Betreiber** (Auftragnehmer und Betreiber von Maschinen) im Sinne von Personen innerhalb eines produzierenden Unternehmens, welche über die Verteilung der Produktionskapazitäten zur Auftragserfüllung entscheiden.

- **Sonstige Dienstleister**, wie z. B. Spediteure oder Anbieter von Telematikdiensten für Fahrzeugflotten, Transporttauschbörsen, stellen im Rahmen des Gesamtmodells tatsächlich reine Dienstleistungsunternehmen dar, deren Geschäftsmodell keine Produktion beinhaltet.

- **Service-Techniker** für die Wartung einer Produktionsmaschine über in geeigneter Weise abgesicherte Netzwerkverbindungen aus der Ferne.

- **Bediener** im Sinne von Personal für das Führen von Produktionsanlagen (Maschinen) vor Ort.

- **ERP- und SAP-Systeme** als externe Entitäten ohne weitere Berücksichtigung oder Modellierung innerhalb des Teilnehmer- und Kommunikationsmodells.

4.5.1.5.2 System- und Vertrauensgrenzen

Im Sinne einer vollständigen Vernetzung aller Partner in den Szenarien von I4.0 können Vertrauensgrenzen und Netzwerkgrenzen im Nachfolgenden praktisch synonym verwendet werden, da jede Segmentierung/Trennung von Netzwerken primär aus den Fragestellungen zur Vertrauen und Kontrolle resultiert bzw. davon ausgegangen wird, dass auch in Zukunft jedes eigenständige Unternehmen auch über die Kontrolle über ihre jeweiligen Netzwerke behalten wird.

- **Überbetriebliche Netzwerkgrenzen (Perimeter Schutz):** resultieren zum einen aus der techn. Notwendigkeit zur hierarchischen Trennung von IP-basierten Netzwerk. Zum andern stellt diese technische Notwendigkeit auch die hoheitliche Kontrolle über den Datenaustausch innerhalb eines Unternehmens und über die Unternehmensgrenzen hinweg sicher. Bei der Modellierung werden
  folgende Grenzen unterschieden:

  - Unternehmen, das einen Auftrag vergibt (Kunde)
  - Unternehmen, das einen Auftrag annimmt (Auftragnehmer)
  - Maschinenhersteller
  - Rechenzentren
  - verschiedene Dienstleister, insbesondere für den Betrieb von Fernwartungsportalen

- **Innerbetriebliche Netzwerkgrenzen:** Innerhalb eines Unternehmens werden häufig in Form von technischer Netzwerksegmentierung weitere Vertrauenszonen eingerichtet, die klassischerweise in erster Linie dem Schutz von industriellen Anlagen und Komponenten ohne nennenswerte Sicherheitseigenschaften mittels Auftrennung durch Firewalls dienen.

  - **Office-IT-Netzwerk:** Hier werden typischerweise Arbeitsplatz-PC und Serversysteme mit entsprechenden Diensten, wie bspw. ERP und SAP, verortet.
  - **Produktionsnetzwerke** an verschiedenen Standorten trennen in erster Linie Produktionsanlagen von Office-IT gegen unbefugte Zugriffe. Mit zunehmender Vernetzung von Systemen hat zusätzlich auch die Absicherung schutzwürdiger Daten innerhalb der Produktion eine starke Bedeutung gewonnen.
  - **Security-Zellen** (Demilitarisierte Zonen) stellen eine zusätzliche vertikale Ebene in der expliziten Segmentierung von Produktionsnetzwerk dar, welche über gesonderte Firewalls mit restriktiven Filterregeln vom übrigen Produktionsnetzwerk getrennt werden

- **Maschinennetzwerke** repräsentieren eine implizite Segmentierung von Produktionsnetzwerken durch die technische Eigenschaft moderner Produktionsanlagen: Sie erfordern typischerweise bereits zur Erfüllung ihrer Funktion nur für die Komponenten der Anlage selbst ein eigenes Netzwerk. Damit einhergehende vom übrigen Produktionsnetzwerk abweichende und ggf. auch vom Hersteller der Anlage vorgegebenen Adressierungsschemata ist ein dedizierter Netzwerkübergangspunkt (z. B. Firewall/Router) unabdingbar.

4.5.1.5.3 Kommunikationsprozesse und Datenflüsse

Die im Teilnehmer- und Kommunikationsmodell dargestellten Prozesse repräsentieren unterschiedlichste Aufgaben im jeweiligen Kontext, wie bspw. Anwendungsprozesse oder Komponenten, welche Daten verarbeiten oder Aktionen auf Basis dieser Daten ausführen. Im Teilnehmer- und Kommunikationsmodell dargestellte Prozesse sind:

- **Produktionssysteme** – sind typischerweise PC-basierte, möglicherweise auch als Embedded-System ausgeführte, Komponenten innerhalb einer Produktionsanlage/Maschine, welche im Vergleich zu den industriellen Steuerungskomponenten höherwertige Software-Prozesse innerhalb einer Betriebssystemumgebung ausführen kann. Mögliche Anwendungsfälle sind HMI oder das Speichern von für die Produktion relevanten Daten (Fabrikationsdaten) sowie anwenderspezifische Maschinenkonfigurationen.

- **Maschinensteuerungen** SPS und SSPS – ist ein Gerät, das zur Steuerung oder Regelung einer Maschine oder Anlage eingesetzt und auf digitaler Basis programmiert wird. Eine Sicherheits-Steuerung (SSPS) dient darüber hinaus ausschließlich dem Zweck zur Gewährleistung und Überwachung der Betriebssicherheit und wird deshalb häufig getrennt von SPS ausgeführt.

- **OPC-UA-Server** – bietet durch Standardisierung von Protokollen und Datenformaten (OPC) einen einheitlichen Zugriff auf unterschiedlichste Komponenten von Produktionssystemen.

- **MES** (Manufacturing Execution System) – Systemlösung zur effizienten Steuerung der Fertigung. Ein MES zeichnet sich gegenüber ähnlich wirksamen Systemen zur Produktionsplanung, den sog. ERP-Systemen (Enterprise Ressource Planning), durch die direkte Anbindung an die verteilten Systeme der Prozessautomatisierung aus und ermöglicht die Führung, Lenkung, Steuerung oder Kontrolle der Produktion in Echtzeit.

- **PLS** (Prozessleitsystem) – dient zum Führen einer verfahrenstechnischen Anlage. Es besteht typischerweise aus so genannten prozessnahen Komponenten und Bedien- und Beobachtungsstationen und Engineering-Komponenten

- **FDI** (Field Device Integration) – Technik zur Einbindung intelligenter Feldgeräte in Leitsysteme

- **PAT** (Process Analytical Technology) – dient der Optimierung, der Analyse und Kontrolle von Herstellungsprozessen in der chemischen Industrie mit dem Ziel der Erhöhung der Produktqualität durch standardisierte Kontrollen und der Dokumentation kritischer Größen während der Produktion (Inprozesskontrollen)

- **VPN-Client/VPN-Concentrator** – sind die als Prozesse dargestellten Komponenten, welche zur Realisierung einer VPN-Verbindung notwendig sind. Als VPN-Client kann eine separate Hardware-Komponente dienen, die bei Bedarf eine VPN-Verbindung zu einem so genannten VPN-Concentrator, bspw. beim Betreiber eines Service-Portal) aufbaut. Beide Komponenten besitzen jeweils einen exklusiven Zugriff auf eine Art Passwortspeicher zur Authentisierung der VPN-Verbindungen.

- **Virtualisierungslösungen** – dienen dem virtualisierten Betrieb von Anwendungsdiensten, bspw. einer Portal-Lösung für Fernwartungssysteme oder Cloud-Diensten allgemein, die bspw. Software-as-a-Service anbieten.

- **Verkauf** – Anwendungsprozess im Rahmen einer Logistik-Lösung

- **Produktionsplanung** – Anwendungsprozess im Rahmen einer Logistik-Lösung

- **Transportplanung** - Anwendungsprozess im Rahmen einer Logistik-Lösung

- **Finished Goods Management** – Anwendungsprozess im Rahmen einer Logistik-Lösung

Datenflüsse im Teilnehmer- und Kommunikationsmodell repräsentieren die Übertragung von Daten zwischen Prozessen, externen Entitäten und Datenspeichern. Eine evtl. graphisch dargestellte Kommunikationsrichtung ist für die

weitere Betrachtung gegenstandslos, da für die Betrachtung von Sicherheitseigenschaften jedweder Kommunikation grundsätzlich beide Richtungen untersucht werden müssen. Im Teilnehmer- und Kommunikationsmodell dargestellte Datenflüsse sind:

- **Aufträge** – Auftragsdaten zwischen Auftraggeber und Auftragnehmer
- **Auftrags**- und **Transportplanung** – Planungsdaten aus den zugehörigen Logistikprozessen an Produktions- oder Transport-Prozesse
- **Fertigungs**- und **Transportaufträge** – Austausch von Datensätzen innerhalb der Logistikprozesse
- **Finished Goods** und **Stock offerings** – Austausch von Datensätze mit dem Logisitk-Anwedungsprozess für die Verwaltung von Lagerbeständen
- **Zustände, Auslastung** und **Mengenzähler** – Leistungsdaten von Produktionsanlagen zur Auswertung durch bspw. ERP-Systeme
- **Produktions- und Fabrikationsdaten** – unterscheiden die für die Produktion grundsätzlich notwendigen Daten in zwei Gruppen: Produktionsdaten fallen bereits bei der Planung von Produktion an, wie z. B. CAD-Konstruktionszeichnungen. Von Fabrikationsdaten spricht man, sobald eine Transformation der Produktionsdaten in für die tatsächlichen Produktionsmaschinen verständliche Anweisungen (z. B. CNC-Steuerprogramme) vorgenommen wurde. Diese müssen dann auch vor Ort auf den Produktionsmaschinen vorliegen.
- **Maschinenprogramm** und **Grundkonfiguration** – Im Datenspeicher einer SPS befinden sich neben dem eigentlich Anwendungsprogramm, welche die SPS ausführen soll, auch entsprechende Konfigurationsdaten, wie sie vom Hersteller der Anlage eingerichtet wurden.
- **Anwenderspezifische Konfiguration** – Produktionssysteme lassen sich selbstverständlich durch den Anwender oder Bediener an die Anforderungen vor Ort anpassen. Solche anwenderspezifischen Konfigurationsdaten werden typischerweise vor Ort in den Produktionssystemen der jeweiligen Anlagen gespeichert, um dort zur Verfügung zu stehen.
- **Virtuelle Protokolle** – zur Übertragung virtueller Konsolen (z. B. RDP) für die Fernwartung von Produktionssystemen
- **VPN-Tunnel** – zur Absicherung von Datenübertragungen in virtuellen Netzwerken
- **Anmeldedaten/Passwörter** – stellen Geheimnisse dar, die in ihrer jeweiligen Entsprechung auf jedem Kommunikationspartner bekannt sein müssen.
- **Firmware-Updates, Konfiguration & Projektierungsdaten** – sind typische Daten, die ein Service-Techniker auf seinem Wartungs-PC vorliegen haben muss, um Wartungsarbeiten an einer Produktionsanlage durchführen zu können.

4.5.1.5.4 Konkrete Bedrohungen

Durch Anwendung des SDL Threat Modeling Tools[308] (vgl. Abschnitt 4.2.2.13) auf das Teilnehmer- und Kommunikationsmodell wurden automatisch 289 potentielle Gefährdungen generiert. Diese große Zahl resultiert aus der systematischen Anwendung aller jeweils zutreffenden Bedrohungsarten auf alle modellierten Elemente im Datenflussdiagramm. Im Falle einer vollständigen Bedrohungsmodellierung ist eine manuelle Durcharbeitung aller potentiellen Gefährdungen notwendig. Dies würde jedoch im Rahmen dieser Studie für die weitestgehend universelle Modellierung des Teilnehmer- und Kommunikationsmodells keinen Sinn ergeben. Stattdessen wurde eine Gruppierung der Fundstellen vorgenommen und für die Gruppe jeweils repräsentative und realistische Gefährdungen exemplarisch ausgewählt, um hier vorgestellt zu werden.

Für alle Prozesse im Rechenzentrum:

- Rechteausweitung: Ein Angreifer könnte Datenflüsse zwischen Prozessen verändern, um die Programmausführung zu beeinflussen, bspw. Ausführung von Schadcode im Prozesskontext.
- Rechteausweitung: Ein Anwender könnte aus der Ferne Schadcode im Kontext eines Anwendungsprozesses ausführen.
- Rechteausweitung: Ein Angreifer könnte sich durch Übernahme eines Anwendungsprozesses als Kunde ausgeben und in dessen Namen Käufe tätigen.

308 http://msdn.microsoft.com/en-us/magazine/cc163519.aspx

- Enthüllung: Ein Angreifer könnte durch Spoofing Zugriff auf vertrauliche Informationen erhalten.
- DoS: Crash, Stopp oder langsame Ausführung von Anwendungsprozessen.
- Leugnung: Anwendungsprozesse könnten abstreiten, z. B. Auftragsdaten von außerhalb der Vertrauensgrenze erhalten zu haben.
- Manipulation: durch mangelnde Validierung von Eingabedaten durch Anwendungsprozesse. Datenflüsse über die Vertrauensgrenze zu Anwendungsprozessen können durch Angreifer manipuliert werden und zu DoS, Rechteausweitung und Enthüllung vertraulicher Information durch Anwendungsprozesse führen.
- Verfügbarkeit: Ein Angreifer könnte mittels DoS-Angriff auf die zentrale Datenbank im Rechenzentrum die gesamte Logistik zum Erliegen bringen.
- Vertraulichkeit: Ein Angreifer könnte Zugriff auf vertrauliche Daten in der zentralen Datenbank erlangen.
- Integrität: Ein Angreifer könnte durch Manipulation an der zentralen Datenbank Einfluss auf sämtliche Logistikprozesse einschl. nachgelagerte Systeme wie PLS und MES nehmen.

Kommunikation über das Internet:

- Unterbrechung von Datenflüssen über Unternehmensgrenzen und Internet. Bspw. Verhinderung der Übermittlung von Aufträgen.
- Datenübertragungen (z. B. Auftragsdaten) könnten abgehört oder manipuliert und dadurch zu Compliance-Verletzungen führen. (Sollte durch Annahme verschlüsselter Verbindungen abgesichert sein.)
- Mittels Spoofing von Anwendungsprozessen, wie z. B. Verkauf, könnte ein Angreifer Zugriff auf vertrauliche Informationen erhalten.
- Mittels Spoofing externer Akteure, wie z. B. Kunden, könnte ein Angreifer bspw. unautorisierten Zugriff auf Anwendungsprozesse erlangen.

Produktion/Maschinenbetreiber:

- Verfügbarkeit: Angreifer könnten MES- oder PLS-Systeme mittels DoS-Angriffen zum Absturz oder verlangsamter Ausführung bringen.
- Datenübertragungen zu MES- & PLS-Systemen (z. B. Auftragsplanung) könnten abgehört oder manipuliert und dadurch zu Compliance-Verletzungen führen.
- Leugnung: MES des Auftragnehmers könnte behaupten, über Vertrauensgrenzen gesendeten Fertigungsauftrag nicht erhalten zu haben.
- Leugnung: PLS des Auftragnehmers könnte behaupten, über Vertrauensgrenzen gesendete Prozessdaten nicht erhalten zu haben.
- Angreifer könnte Zugriff auf Passwörter für Fernwartungsportal erlangen.
- Angreifer könnte Zugriff auf Fabrikationsdaten im Produktionssystem erlangen (Verlust von Know-how) oder diese manipulieren (Sabotage der Produktion).
- Auslesen und Ändern von Datenspeichern in Produktionsanlagen und Steuerungskomponenten: Verlust von Know-how, internem Wissen oder Sabotage der Produktion.

Dienstleister für Fernwartung:

- Accounting: Passwörter könnten an unberechtigte Personen gelangen.
- DoS gegen VPN-Concentrator möglich.
- Zugriff auf oder Manipulation von Images für Wartungs-PC: von Firmwareupdates, Ausspähen von Anlagendetails über Konfiguration und Projektierungsdaten, Sabotage von Anlagen über das Fernwartungsportal.
- Auslesen/Ändern von Fabrikationsdaten via Fernwartung: Verlust von Know-how oder Sabotage der Produktion.

Maschinenhersteller:

- Passwörter für Fernwartungsportal könnten an unberechtigte Personen gelangen.

4.5.1.5.5 Risikoeinschätzung der Bedrohungen

Die nachfolgende Tabelle 4–13 dient der Risikoeinschätzung der Bedrohungen. Sie enthält neben der Beschreibung der Bedrohung die wichtigsten Informationen, unter anderem zu Angreifertypen, deren potentielle Motivation sowie den notwendigen Fähigkeiten.

Tabelle 4–13: Risikoeinschätzung der Bedrohungen

Wo	Ziel	Bedrohungs-typ	Bedrohung	Angreifertypen (Motivation)	Fähigkeiten
Maschinen-hersteller	Daten-speicher für Passwörter	Enthüllung	Passwörter für Fernwartungsportal könnten an unberechtigte Personen gelangen.	Böswillige Angestell-te (Rache, unerlaubte Aktivitäten), Cyber-crime	Niedrig
Rechen-zentrum	alle Logistik-prozesse	Manipulation, DoS	Durch mangelnde Validierung von Eingabedaten durch Anwendungsprozesse. Datenflüsse über die Vertrauensgrenze zu Anwendungsprozessen können durch Angreifer manipuliert werden und zu DoS, Rechteausweitung und Enthüllung vertraulicher Information durch Anwendungsprozesse führen.	Cybercrime	Niedrig/ Mittel
Produktion	Daten-speicher für Passwörter	Enthüllung	Angreifer könnte Zugriff auf Passwörter für Fernwartungsportal erlangen.	Böswillige Angestell-te (Rache, unerlaubte Aktivitäten), Cyber-crime	Niedrig/ Mittel
Dienstleister für Fern-wartung	VPN-Con-centrator	DoS	DoS gegen VPN-Concentrator möglich	Kleinkriminelle, Hacktivists	Mittel
Rechen-zentrum	alle Logistik-prozesse	Rechteaus-weitung	Ein Angreifer könnte Datenflüsse zwischen Prozessen verändern, um die Programmausführung zu be-einflussen, bspw. Ausführung von Schadcode im Prozesskontext.	Konkurrent (Spionage, Sabotage)	Mittel/ Hoch
Rechen-zentrum	alle Logistik-prozesse	Rechteaus-weitung	Ein Anwender könnte aus der Ferne Schadcode im Kontext eines Anwendungprozesses ausführen.	Konkurrent (Spionage, Sabotage)	Mittel/ Hoch
Rechen-zentrum	alle Logistik-prozesse	Rechteaus-weitung	Ein Angreifer könnte sich durch Übernahme eines Anwendungsprozesses als Kunde ausgeben und in dessen Namen Käufe tätigen.	Konkurrent (Spionage, Sabotage)	Mittel/ Hoch
Rechen-zentrum	alle Logistik-prozesse	Enthüllung	Ein Angreifer könnte durch Spoofing und dadurch Zugriff auf vertrauliche Informationen erhalten.	Konkurrent (Spionage, Sabotage)	Mittel/ Hoch
Rechen-zentrum	alle Logistik-prozesse	DoS	Crash, Stopp oder langsame Ausführung von Anwendungsprozessen.	Konkurrent (Spionage, Sabotage)	Mittel/ Hoch
Rechen-zentrum	alle Logistik-prozesse	Leugnung	Anwendungsprozesse könnten abstreiten, z. B. Auftragsdaten von außerhalb der Vertrauensgrenze erhalten zu haben.	Konkurrent (Spionage, Sabotage)	Mittel/ Hoch
Rechen-zentrum	alle Logistik-prozesse	DoS	Ein Angreifer könnte mittels DoS-Angriff auf die zentrale Datenbank im Rechenzentrum die gesamte Logistik zum Erliegen bringen.	Konkurrent (Spionage, Sabotage)	Mittel/ Hoch
Rechen-zentrum	alle Logistik-prozesse	Enthüllung	Ein Angreifer könnte Zugriff auf vertrauliche Daten in der zentralen Datenbank erlangen.	Konkurrent (Spionage, Sabotage), Geheimdienste (Spionage)	Mittel/ Hoch
Kommunika-tion über das Internet	alle Logistik-prozesse	Täuschung	Mittels Spoofing externer Akteure, wie z. B. Kunden, könnte ein Angreifer bspw. unautorisierten Zugriff auf Anwendungsprozesse erlangen.	Konkurrent (Piona-ge, Sabotage), Orga-nisiertes Verbrechen (Erpressung), Geheimdienste (Spionage)	Mittel/ Hoch
Dienstleister für Fern-wartung	Daten-speicher für Passwörter	Enthüllung	Accounting: Passwörter könnten an unberechtigte Personen gelangen.	Böswillige Angestell-te (Rache, unerlaubte Aktivitäten)	Niedrig/ Mittel

→

Tabelle 4–13: Risikoeinschätzung der Bedrohungen (Fortsetzung)

Wo	Ziel	Bedrohungs-typ	Bedrohung	Angreifertypen (Motivation)	Fähigkeiten
Rechen-zentrum	alle Logistik-prozesse	Manipulation	Ein Angreifer könnte durch Manipulation an der zentralen Datenbank Einfluss auf sämtliche Logistik-prozesse einschl. nachgelagerte Systeme wie PLS und MES nehmen.	Geheimdienste (Sabotage)	Hoch
Kommuni-kation über das Internet	ext. Daten-flüsse, z. B. Auftragsda-ten	DoS	Unterbrechung von Datenflüssen über Unterneh-mensgrenzen und Internet. Bspw. Verhinderung der Übermittlung von Aufträgen.	Organisiertes Verbre-chen (Erpressung), Geheimdienste (Sabotage)	Hoch
Kommunika-tion über das Internet	ext. Daten-flüsse, z. B. Auftrags-daten	Enthüllung	Datenübertragungen (z. B. Auftragsdaten) könnten abgehört oder manipuliert und dadurch zu Compliance-Verletzungen führen.	Geheimdienste (Spionage)	Hoch
Kommunika-tion über das Internet	alle Logistik-prozesse	Täuschung	Mittels Spoofing von Anwendungsprozessen, wie z. B. Verkauf, könnte ein Angreifer Zugriff auf ver-trauliche Informationen erhalten.	Geheimdienste (Spionage)	Hoch
Produktion	MES/PLS	DoS	Angreifer könnten MES- oder PLS-Systeme mittels DoS-Angriffe zum Absturz oder verlangsamter Ausführung bringen.	Konkurrent (Sabota-ge), Geheimdienste (Sabotage)	Hoch
Produktion	MES/PLS	Enthüllung/ DoS	Datenübertragungen zu MES- & PLS-Systemen (z. B. Auftragsplanung) könnten abgehört oder manipuliert und dadurch zu Compliance-Verletzungen führen.	Konkurrent (Spionage), Geheimdienste (Spio-nage, Sabotage)	Hoch
Produktion	MES	Leugnung	MES des Auftragnehmers könnte behaupten, einen über Vertrauensgrenzen gesendeten Fertigungsauf-trag nicht erhalten zu haben.	Konkurrent (Sabotage)	Hoch
Produktion	PLS	Leugnung	PLS des Auftragnehmers könnte behaupten, über Vertrauensgrenzen gesendete Prozessdaten nicht erhalten zu haben.	Konkurrent (Sabotage)	Hoch
Produktion	Produktions-systeme	Enthüllung, Manipulation	Angreifer könnte Zugriff auf Fabrikationsdaten im Produktionssystem erlangen (Verlust von Know-how) oder diese manipulieren (Sabotage der Produktion).	Konkurrent (Siona-ge), Geheimdienste (Spionage, Sabotage)	Hoch
Produktion	Steuerungs-komponen-ten	Enthüllung, Manipulation	Auslesen und Ändern von Datenspeichern in Produk-tionsanlagen und Steuerungskomponenten: Verlust von Know-how, internem Wissen oder Sabotage der Produktion).	Konkurrent (Siona-ge), Geheimdienste (Spionage, Sabotage)	Hoch
Produktion	Datenspei-chern von Produktions-systemen	Enthüllung	Zugriff auf oder Manipulation von Images für War-tungs-PC: von Firmwareupdates, Ausspähen von Anlagendetails über Konfiguration und Projektie-rungsdaten, Sabotage von Anlagen über das Fern-wartungsportal.	Konkurrent (Siona-ge), Geheimdienste (Sabotage)	Hoch
Dienstleister für Fern-wartung	Datenspei-cher Fabrika-tionsdaten	Enthüllung, Manipulation	Auslesen/Ändern von Fabrikationsdaten via Fern-wartung: Verlust von Know-how oder Sabotage der Produktion.	Organisiertes Verbre-chen (Erpressung), Geheimdienste (Spionage)	Hoch

4.6 Zusammenfassung und Zwischenfazit

Schon die Ausgangssituation für I4.0 weist erhebliche Defizite in der IT-Sicherheit auf, auf die in den vorhergehenden Kapiteln hingewiesen wurde. Es muss daher bei allen weiteren Betrachtungen immer im Auge behalten werden, dass für die Lösung von durch I4.0 neu entstehenden Herausforderungen, Bedrohungen und Risiken zunächst ein sicheres Fundament durch die Adressierung dieser alten Probleme erforderlich ist.

Für I4.0 werden sich nun aber, wie in den Fallbeispielen illustriert wird, zusätzliche Herausforderungen ergeben, die in der gegenwärtigen Situation noch nicht diese prominente Rolle spielen.

Es sind im Wesentlichen drei Entwicklungen, aus denen hier neue Herausforderungen entstehen:

1. Die Vernetzung von Industrieanlagen und deren Komponenten wird künftig nicht nur organisations- und jurisdiktionsübergreifender, sondern vor allem auch dynamischer stattfinden als bisher. Die konkreten Teilnehmer an einem IT-Prozess in einer I4.0-Wertschöpfungskette sind nicht mehr alle lange im Voraus fest planbar. Um die IT-Sicherheit in einem solchen Szenario zu gewährleisten, muss eine belastbare Grundlage von Vertrauen und Verlässlichkeit geschaffen werden, die sich über alle Teilnehmer der Wertschöpfungskette erstreckt. Die Herstellung solcher Vertrauensbeziehungen kann nicht erst in dem Moment in Angriff genommen werden, indem sich aufgrund dynamischer Abläufe eine neue Kommunikationsbeziehung über Unternehmens- und Ländergrenzen hinweg ergibt. Die Herausforderung besteht hier vor allem in der Definition von Mindestsicherheitsstandards, denen alle potentiellen Teilnehmer an den I4.0-Prozessen genügen müssen, beziehungsweise zu deren Einhaltung diese sich verbindlich verpflichten. Da diese Standards für Teilnehmer jeder Größe, also auch für KMU mit zumutbarem Aufwand umsetzbar sein müssen und ihre Einhaltung nachweisbar sein muss, ergibt sich als weitere Herausforderung, hier auf internationaler Ebene ein schlankes, auf das Wesentliche beschränkte Rahmenwerk aus technischen und organisatorischen Maßnahmen zu konzipieren, das diesen Zweck erfüllt.

2. Die Menge an Daten, die von einem Teilnehmer einem anderen Teilnehmer aus funktionalen Gründen absichtlich mitgeteilt oder zugänglich gemacht werden, nimmt zu. Darunter befinden sich insbesondere auch solche Daten, die nicht nur aus Sicht eines einzelnen Unternehmens als Geschäftsgeheimnis gelten, sondern an die aufgrund staatlicher Gesetze eine besonders hohe Anforderung an die Vertraulichkeit besteht (z. B. Schutz von Personendaten). Verschärfend kommt hinzu, dass derjenige, der solche Daten anderen bereitstellt, oft nicht wissen kann, wer die Teilnehmer im weiteren Verlauf der Wertschöpfungskette genau sein werden, denen diese Daten bekannt gegeben werden müssen, um ihre Funktion in einem I4.0-Prozess zu erfüllen. Jeder Teilnehmer trägt damit nicht nur eine Verantwortung für die Sicherheit seiner eigenen Daten, sondern auch für die Sicherheit der Daten seiner Prozesspartner. Umgekehrt muss jeder Teilnehmer darauf vertrauen können, dass Daten, die er im Verlauf von I4.0-Prozessen im Rahmen eines Wertschöpfungsnetzwerkes seinen Kommunikationspartnern überlässt, von diesen angemessen geschützt werden.

3. Entscheidungen werden bei I4.0 zunehmend autonom von Maschinen (das heißt von Software-Programmen) getroffen. Diese Entscheidungen und die daraus resultierenden Änderungen von Abläufen und Teilnehmer-Konfigurationen können sich aufgrund von Ereignissen aus unterschiedlichsten Domänen und Partnersystemen ergeben sowie aus der Analyse von Daten aus unterschiedlichsten Quellen. Erfolgsentscheidend für diesen Aspekt von I4.0 ist sowohl die Integrität als auch die Authentizität der verwendeten Daten und Datenquellen.

Welche Schritte nun konkret unternommen werden müssen, um diesen Herausforderungen zu begegnen, ist Thema der nachfolgenden Kapitel.

5. IT-Sicherheitsmaßnahmen sowie Implementierungshindernisse

Nachdem im Kapitel 4 anhand von für die Industrie 4.0 (I4.0) relevanten Fallbeispielen ein Referenzmodell und darüber abgeleitete Bedrohungen (siehe auch weiter unten) beschrieben wurden, wird in diesem Kapitel nun auf existierende IT-Sicherheitsmaßnahmen (Security) und deren Eignung zur Abwendung bzw. Abschwächung dieser Bedrohungen für die IT-Systeme der I4.0 gemäß dem Stand der Technik eingegangen. Es wird aufgezeigt und diskutiert, welche Hindernisse es bereits heute bei einer Implementierung gibt oder zukünftig geben kann, mit dem Ziel hierauf aufbauend vorhandene IT-Security-Konzepte zu prüfen und als notwendig erachtete neuartige Konzepte beschreiben zu können (Kapitel 6).

Bevor der Stand der Technik thematisiert wird, soll an dieser Stelle kurz die für die nachfolgende Untersuchung relevante Ausgangsbasis reflektiert werden. Auf Basis der praxisnahen Fallbeispiele in Kapitel 4.1, des Referenz- und des Bedrohungsmodells in Kapitel 4.2 sowie den TOP10 Bedrohungen in Kapitel 4.3 wurden 26 konkrete und im Kontext von I4.0 relevante Bedrohungen identifiziert (vgl. Abschnitt 4.5.1.5.4 und Anhang 8.1). Auf Grund der zur Identifizierung verwendeten Methode, lassen sich diese Bedrohungen einer von sechs allgemeinen Bedrohungsklassen zuordnen:

1. Täuschung (Identitätsdiebstahl),
2. Manipulation (von Daten),
3. Leugnung (Abstreiten von Aktionen),
4. Enthüllung (unberechtigte Informationsweitergabe),
5. Dienstblockade (Denial-of-Service (DoS)) oder
6. Rechteausweitung.

Im Hinblick auf den Ort der Bedrohung betreffen die identifizierten Bedrohungen das vom Maschinenbetreiber für seine IT-Systeme verwendete Rechenzentrum, die Produktion beim Maschinenbetreiber, die Kommunikation über das Internet, den Dienstleister für Fernwartungen und den Maschinenhersteller (vgl. Kapitel 4.5.1.5.4). Der Fokus bei der Beschreibung der Bedrohungen liegt primär auf dem sicherheitsrelevanten Ereignis selbst (z. B. unberechtigter Zugriff auf vertrauliche Daten), weniger auf den Gegebenheiten, die das Ereignis ermöglichen oder verursachen. Da für die Untersuchung von IT-Sicherheitsmaßnahmen und Implementierungshindernissen ein Verständnis der Ursachen von sicherheitsrelevanten Ereignissen unerlässlich ist, wird im Folgenden auch direkt auf die Fallbeispiele verwiesen. Um die Untersuchung vor dem Hintergrund einer möglichst umfassenden, über die Fallbeispiele hinausgehenden Darstellung der Bedrohungslage durchführen zu können, wird auch auf eine vom BSI erstellte Liste von zentralen Bedrohungen für Systeme zur Fertigungs- und Prozessautomatisierung Bezug genommen (siehe Kapitel 4.3).

Das Kapitel 5.1 fasst den Stand der Technik und die Eignung und Implementierungshindernisse hinsichtlich der relevanten technischen Aspekte zusammen. Im folgenden Kapitel 5.2 werden dann die organisatorischen und rechtlichen Umsetzungsaspekte von IT-Sicherheitsmaßnahmen, deren Eignung sowie in den Kapiteln 5.3 und 5.4 deren Implementierungshindernisse beschrieben.

5.1 Stand der Technik, Technische Aspekte der Umsetzung, Eignung der Maßnahmen und Implementierungshindernisse

Im Folgenden wird der Stand der Technik hinsichtlich IT-Sicherheit im Industriekontext beschrieben. Dazu werden die in existierenden Standards und Leitfäden genannten Maßnahmen im Kontext der in Kapitel 4 eingeführten Fallbeispiele und der identifizierten Bedrohungen (siehe oben) diskutiert, um die grundsätzliche Eignung der Maßnahmen für die I4.0 zu ermitteln und Hemmnisse sowie erste Handlungsvorschläge aufzuzeigen. Im Hinblick auf Standards und Leitfäden wird nach einer Literaturanalyse vorrangig das ICS-Security-Kompendium[309] des BSI als Basisrahmenwerk betrachtet und verwendet, da es auf vielen weiteren Standards und Leitfäden beruht bzw. diese referenziert und den eigenen Maßnahmen zuordnet (IEC 62443, VDI/VDE 2182, NERC CIP, DHS Best Practices, ISO/IEC 27001 und IT-Grundschutz; vgl. ICS-Security-Kompendium Kapitel 5.7, Seiten 78 bis 101). Berücksichtigt wurden in der Literaturanalyse aktuelle Studien, Leitfäden, Normen und Standards zu den Themen IT-Sicherheit und I4.0, sofern dort explizit technische Aspekte adressiert wurden, unter anderem die folgenden Werke:

309 BSI (2013): ICS-Security-Kompendium, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile

- die Richtlinie VDI/VDE 2182[310],
- die Normenreihe ISA/IEC 62443[311],
- der Standard ISO/IEC 27001[312] und Weitere (270xy),
- der Leitfaden des US National Institute of Standards and Technology (NIST) zu ICS-Sicherheit[313],
- die Umsetzungsstrategie Industrie 4.0 – Ergebnisbericht der Plattform Industrie 4.0, Kapitel 7 „Sicherheit vernetzter Systeme“[314],
- die Operational Guidelines für Industrial Security[315] von Siemens,
- die Sicherheitsspezifischen Empfehlungen für Maschinenbauer und Integratoren[316] des BSI (BSI-CS 106).

Am Rande wurden auch die folgenden Standards bzw. Leitfäden betrachtet:

- der IT-Grundschutz sowie das Anwendungsbeispiel für IT-Grundschutz im produzierenden Gewerbe[317] des BSI
- und die VDMA-Studie zum Status quo der Security in Produktion und Automation[318].

Die Betrachtung orientiert sich aufgrund der Fallbeispiele aus der industriellen Praxis (siehe Kapitel 4.1) und der darauf aufbauenden Analyse (siehe Kapitel 4.2f) über das Referenzmodell an zehn zentral relevanten Maßnahmenpakten:

- Inbetriebnahme in sicherer Konfiguration
- Fernwartung durch Hersteller und Integrator
- Absicherung von Feldgeräten
- Absicherung der Netze
- Datensicherung
- Schutz vor Schadsoftware (Malware)
- Härtung der IT-Systeme
- Patchmanagement
- Authentisierung, Zugriffskontrolle, Protokollierung und Auswertung
- Mobile Datenträger

Diese zehn Pakete und die damit verbundenen Aspekte wurden als relevant betrachtet, nachdem ein Mapping der Bedrohungen (vgl. Abschnitt 4.5.1.5.4) mit den Maßnahmenpaketen des ICS-Security-Kompendium stattgefunden hat (vgl. Anhang 8.1). Das methodische Vorgehen an dieser Stelle umfasst eine

- Beschreibung des relevanten Maßnahmenpakets aus dem als maßgeblich relevant erachteten ICS-Security-Kompendium des BSI (Zusammenfassung), unter Einbeziehung zusätzlicher, relevanter IT-Sicherheitsmaßnahmen aus den genannten weiteren Werken,
- Beschreibung der damit adressierten Bedrohungen (siehe Kapitel 4 bzw. Anhang),
- Beschreibung der Wirkungsweise gegen bereits identifizierte Bedrohungen.

Bei der Beschreibung hinsichtlich der Eignung der Maßnahmen, möglichen Hindernissen bei deren Implementierung sowie diesbezüglich ersten, technisch detaillierteren Handlungsvorschlägen wurde wie folgt vorgegangen:

310 VDI-Richtlinie Informationssicherheit in der industriellen Automatisierung, VDI/VDE 2182.
311 IT-Sicherheit für industrielle Steuerungssysteme, ISA/IEC 62443.
312 Informationssicherheitsmanagement, ISO/IEC 27001.
313 NIST (2011): Guide to Industrial Control Systems (ICS) Security, SP 800-82, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
314 Plattform Industrie 4.0 (2014): Umsetzungsstrategie Industrie 4.0 – Ergebnisbericht der Plattform Industrie 4.0, http://www.plattform-i40.de/sites/default/files/150410_Umsetzungsstrategie_0.pdf
315 Siemens (2013): Operational Guidelines für Industrial Security, http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_de.pdf und http://www.industry.siemens.com/topics/global/de/industrial-security/Seiten/default.aspx
316 BSI (2014) BSI-CS 106, Version 1.00 vom 10.10.2014: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_106.html
317 BSI (2008): IT-Grundschutz-Profile – Anwendungsbeispiel für IT-Grundschutz im Produzierenden Gewerbe, http://www.edvq.de/downloads/IT-Sicherheit/IT-Grundschutzprofil%20produzierendes%20Gewerbe.pdf
318 VDMA (2013): VDMA-Studie: Status Quo der Security in Produktion und Automation 2013/2014, http://www.vdma.org/documents/105969/142443/VDMA%20Studie%20Security/82324cfa-2df6-4c4e-ae21-490a26e30d0c

- Die technischen Maßnahmen aus dem ICS-Security-Kompendium werden referenziert. Hier werden zur Vereinfachung die Nummerierung der BSI-Maßnahmennummern aus dem Kapitel 5 des ICS-Security-Kompendiums verwendet. Siehe Kreuztabelle im Anhang.

- Beschreibung und Diskussion der Eignung dieser Maßnahmen und der möglichen Hindernisse, welche bei der Umsetzung der referenzierten technischen Maßnahmen im I40-Kontext unter Einbeziehung der berücksichtigten Fallbeispiele bestehen oder zukünftig bestehen können.

- Wo sinnvoll, Beschreibung von möglichen technischen Handlungsvorschlägen, als Grundlage für neuartige Konzepte (Kapitel 6) und die Handlungsvorschläge in Kapitel 7.

Zum Verständnis der folgenden Kapitel ist die nummerierte Liste der in der Bedrohungsanalyse extrahierten Bedrohungen (vgl. Kapitel 4) notwendig, da auf sie im Folgenden Bezug genommen wird. Diese befindet sich im Anhang 8.1 unter Bedrohungen und Mapping auf Maßnahmen.

5.1.1 Inbetriebnahme in sicherer Konfiguration

Für eine Inbetriebnahme von Anlagen und Komponenten in einer sicheren Konfiguration sollten bestimmte Voraussetzungen bereits durch die Hersteller geschaffen sein. So können beispielsweise für eine sichere Konfiguration erforderliche Funktionen, wie Log-Datenerfassung oder Schutzmaßnahmen für Konfigurationsschnittstellen, nur durch den Hersteller implementiert werden (vgl. Kapitel 5.1.7). Zum Zeitpunkt der Inbetriebnahme müssen jedoch weitere Maßnahmen getroffen werden, um die Konfiguration an die Erfordernisse vor Ort anzupassen. Diese Anpassungsmaßnahmen betreffen im Wesentlichen die Konfiguration von Komponenten, aber auch die Aktualisierung von Software und die Dokumentation aller Maßnahmen und Einstellungen. Im Rahmen der Konfigurationsmöglichkeiten der jeweiligen Komponenten oder Systeme sollten typischerweise zunächst alle nicht benötigten Dienste oder Schnittstellen deaktiviert oder ganz entfernt werden. Alle verfügbaren IT-Sicherheitsfunktionen sollten dagegen aktiviert werden, falls dies in der jeweiligen Umgebung möglich ist. Dabei sollten sicherheitsrelevante Konfigurationsoptionen grundsätzlich so restriktiv wie möglich gewählt werden. Ein besonderes Augenmerk gilt dabei der Wahl von Zugangsdaten. Diese sollten immer individuell und idealerweise pro Gerät und Verwendungszweck festgelegt werden.

Bezüglich der Software wird im Sinne einer sicheren Inbetriebnahme die jeweils aktuellste Version aufgespielt. Eine abschließende Dokumentation aller Änderungsmaßnahmen ermöglicht eine zukünftige Fortsetzung des Sicherheitsmanagements von Anlagen auch über Personalwechsel oder Anlagenerweiterungen hinweg.

Eine Inbetriebnahme in sicherer Konfiguration adressiert praktisch alle Bedrohungen aus Kapitel 4 (vgl. „Kreuztabelle der Bedrohungen und Maßnahmen des ICS-Security-Kompendiums“ im Anhang Bedrohungen und Mapping auf Maßnahmen), da entsprechende Maßnahmen implizit auch eine Verbesserung der Sicherheitssituation für die meisten denkbaren Bedrohungen bedeutet – Ausnahme 0-day-Exploits.

So verhindert bspw. die Deaktivierung nicht benötigter Funktionalität die Ausnutzung von potentiellen Schwachstellen in Software-Modulen, die überhaupt nicht für den Betrieb einer Anlage notwendig sind. Die Aktivierung aller möglichen Sicherheitsfunktionen mit maximal restriktiven Einstellungen gewährleistet dagegen das höchstmögliche Maß an Sicherheit, welches durch die Komponenten selbst möglich ist. Die Verwendung von aktueller Software soll sicherstellen, dass möglichst alle bereits aus der Vergangenheit bekannten Schwachstellen zum Zeitpunkt der Inbetriebnahme behoben sind. Die explizite Konfiguration ausschließlich erforderlicher Berechtigungen für Benutzer stellt sicher, dass nur solche Daten oder Dienste für den Zugriff durch Benutzer freigegeben werden, die unbedingt für Betrieb und Wartung einer Produktionsanlage notwendig sind. Erforderliche Freigaben von Benutzerzugriffen sollten idealerweise nur durch explizite Konfiguration möglich sein.

Entsprechende Maßnahmen des ICS-Security-Kompendiums des BSI finden sich dort in Kapitel 5.4.4 (die dortige Nummerierung wurde beibehalten):

- 24. Verzicht auf überflüssige Produktfunktionen

- 25. Individuelle Zugangsdaten

- 26. Aktivierte Sicherheitsmechanismen und aktueller Patchstand

- 27. Langfristige Gewährleistung der IT-Security

- 28. Unterstützung von Virenschutz-Lösungen

Hindernisse bei der Umsetzung

Die Realität im industriellen Kontext kann in diesem Punkt erheblich von der Situation in der Office-IT abweichen. Das Fallbeispiel Automobilbau (vgl. Abschnitt 4.1.1) zeigt anschaulich, welche praktischen Schwierigkeiten bspw. bei der Inbetriebnahme von Anlagen auftreten können. Im Folgenden werden die praktischen Hindernisse in zwei Gruppen unterschieden: fehlende Funktionalität und unsichere Konfiguration.

Zur ersten Gruppe zählt der Umstand, dass oftmals schlicht keine aktuellere Softwareversion verfügbar ist, als die Version, welche mit den Komponenten oder einer Anlage ausgeliefert wurde. Anlagen können dann nur mit der ursprünglich ausgelieferten Software betrieben werden. Eine Aktualisierung ist nicht möglich oder aus wirtschaftlichen Gründen nicht sinnvoll. Oft fehlen sicherheitsrelevante Konfigurationsmöglichkeiten. So können bspw. Funktionen mit potenziellem Sicherheitsrisiko nicht deaktiviert werden, weil dies im Rahmen der Konfigurationsmöglichkeiten nicht vorgesehen wurde. Mögliche Gründe dafür sind etwa mangelndes Risikobewusstsein seitens der Hersteller oder Kostendruck bei der Softwareentwicklung.

Praktische Erfordernisse in der Produktion können eine individuelle Konfiguration von Zugriffsberechtigungen, die an einzelne Personen/Maschinen gebunden ist, unmöglich machen bzw. würden einen erheblichen organisatorischen Mehraufwand bedeuten oder sogar ein schnelles Einschreiten im Fehlerfall unnötig erschweren. Diese praktischen Zwänge resultieren daher oftmals in einer unsicheren Konfiguration. So werden beispielsweise Benutzerkonten und Kennwörter mit anderen Mitarbeitern geteilt oder für verschiedene Maschinen dieselben Standardkennwörter verwendet, um bei Personalwechseln oder in Vertretungsfällen keine Störung des Betriebes zu riskieren.

Handlungsvorschlag

Auch eine sichere Konfiguration von Produktionssystemen geht oft mit Kompromissen und Zugeständnissen an die Erfordernisse anderer Systeme einher. Werden mit einer Anlage zusammenwirkende Systeme verbunden, sollten die oben genannten Maßnahmen zur Konfiguration im Rahmen der jeweiligen Möglichkeiten maximal ausgenutzt werden. Ferner müssen die notwendigen Möglichkeiten zur Absicherung der Produktionssysteme bereits bei der Entwicklung durch die Hersteller berücksichtigt und den Maschinenbauern und Integratoren zur Verfügungen gestellt werden. Diese müssen die Funktionen entsprechend bei Inbetriebnahmen konsequent nutzen. Eine Einschränkung der Konfigurierbarkeit und verbleibende Risiken sind zu dokumentieren.

5.1.2 Fernwartung durch Hersteller oder Integrator

Auch 2015 wiederholen sich Berichte in den Medien, dass Industriesteuerungen (SCADA-Systeme (Supervisory Control and Data Acquisition)) mit Fernwartungszugang manipuliert wurden[319]. Häufig wiederkehrende Gründe sind bis heute immer noch die Verwendung von Standardpasswörtern oder sogar auch völlig ungesicherte Zugänge. Nicht nur im Hinblick auf die Eignung für I4.0-Szenarien sind hier zukünftig höhere Anforderungen an die Sicherheit zu stellen. Waren auf Virtualisierung basierende Portal-Lösungen zur Fernwartung bis vor kurzem noch Eigenentwicklungen von besonders für die IT-Sicherheit engagierten Herstellern oder Betreibern von Maschinen, finden sich heute bereits erste kommerzielle Anbieter für derartige Lösungen am Markt. Diese stellen gegenüber konventionellen Direktverbindungen vom Hersteller direkt zur Produktionsanlage/Maschine vorbei am Produktionsnetzwerk des Betreibers eine signifikante Verbesserung diverser Sicherheitsaspekte in diesem Problemkreis dar.

Das BSI empfiehlt, dass Verbindungen zur Fernwartung erst von einem Techniker vor Ort bei Bedarf aktiviert werden. Direkte Verbindungen zur Produktionsanlage über Telefon- oder Mobilfunknetze sollten vermieden werden. Stattdessen ist ein Verbindungsaufbau von extern über einen Sprungserver innerhalb der Unternehmens-DMZ zu bevorzugen. Alternativ kann der Verbindungsaufbau auch zu Portalservern externer Dienstleister oder des Herstellers erfolgen. Wichtig ist, dass entsprechende Netzwerkverbindungen zur Fernwartung innerhalb des Unternehmens durch geeignete technische Lösungen zur Netzwerksicherheit auf die Kommunikation zwischen Sprungserver und Produktionsanlage eingeschränkt wird.

319 Siehe http://www.computerworld.com/article/2475789/cybercrime-hacking/hackers-exploit-scada-holes-to-take-full-control-of-critical-infrastructure.html

Allgemein sind verschiedene Modi für Fernwartungsverbindungen möglich:

- Verbindung auf Anfrage: Eine Verbindung kann nur nach vorheriger Absprache mit dem Betreiber aufgebaut werden.
- Beaufsichtigter Zugriff: Der Zugriff auf das Produktionssystem kann durch einen Techniker von Betreiberseite live mitverfolgt werden.
- Voller Zugriff: Der Servicetechniker erhält uneingeschränkten Zugriff auf das Produktionssystem
- Nur ausgehende Kommunikation: In diesem Modus wird bspw. lediglich die Übertragung von Leistungs- oder Statusdaten in Intervallen oder Echtzeit an ein externes System zu Monitoring-Zwecken erlaubt.

Besondere Aufmerksamkeit gilt auch der Authentisierung sowie den Möglichkeiten zur Auditierung. Zur Authentisierung gilt heute die so genannte Zwei-Faktor-Authentisierung als Standard. Funktionen zur Auditierung ermöglichen auch im Nachhinein Einsicht in die Vorgänge während einer Fernwartungs-Verbindung.

Die Maßnahmen zur sicheren Fernwartung adressieren folgende Bedrohungen aus Kapitel 4 und „Kreuztabelle der Bedrohungen und Maßnahmen des ICS-Security-Kompendiums“ im Anhang Bedrohungen und Mapping auf Maßnahmen:

- 3.5
- 4.1, 4.2, 4.3, 4.4

Eine im Regelfall deaktivierte Fernzugriffsmöglichkeit stellt grundsätzlich sicher, dass von dieser Zugriffsmöglichkeit nur Gebrauch gemacht werden kann, wenn dies auch wirklich erforderlich ist. Die Einschränkung des Kommunikationspfades auf einen Sprungserver innerhalb der DMZ und der Produktionsanlage stellt sicher, dass durch die Fernwartungsverbindung kein Zugriff auf andere Systeme außer dem betreffenden Produktionssystem möglich ist und außerdem eine Aufzeichnung bzw. Filterung der Datenflüsse möglich ist. Eine Zwei-Faktor-Authentifizierung stellt sicher, dass Unbefugte durch den Besitz eines ausgespähten Kennwortes allein keinen Zugriff auf Produktionsmaschinen erhalten.

Entsprechende Maßnahmen aus dem ICS-Security-Kompendium des BSI finden sich dort in Kapitel 5.4.6 (Fernwartung durch Hersteller und Integrator, Seite 61):

- 29. Sichere Fernwartung

Sowie in

- 54. Technische Authentisierungsmaßnahmen
- 58. Einsatz geeigneter kryptographischer Algorithmen

Hindernisse bei der Umsetzung

Auch moderne Lösungsansätze zur Fernwartung stellen prinzipiell nur Lösungen zur effektiven Absicherung der Netzwerke bei Zugriff von außen dar. Prinzipiell ungelöst bleiben auch damit die Probleme rund um Vertrauensbeziehungen im Fernwartungsfall. So sind beispielsweise keine Lösungen bekannt, um einem Servicetechniker den Zugriff auf die Firmen-Know-how tragenden Fabrikationsdaten zu verwehren, welche auf einer Produktionsmaschine gespeichert sind, auf die zu Wartungszwecken voller Zugriff besteht. Das Fallbeispiel Anlagen-/Maschinenbau (vgl. Abschnitt 4.1.2) zeigt zwar verschiedene technische Lösungsansätze zur Durchsetzung technischer Sicherheitsbarrieren. Allerdings wirft die Vielzahl der unterschiedlichen Interessensparteien – Hersteller einer Maschine, Betreiber einer Maschine, Zulieferer von VPN-Lösungen für den industriellen Einsatz und nicht zuletzt der Betreiber einer Portallösung – die Frage auf, wer letztlich die Hoheit über die Daten in einer Produktionsanlage behält. Auch ist oftmals die Kontrolle über die in der Kommunikationsstrecke befindlichen Firewalls fraglich, wenn entsprechende Firewall-Regeln vom Maschinen-Hersteller definiert werden. Eine sinnvolle Lösung müsste es erlauben, Schreib- und Leserechte auf die unterschiedlichen Daten und Komponenten innerhalb eines Produktionssystems auch im Wartungsfall durchzusetzen.

Handlungsvorschlag

Zur technischen Durchsetzung der Netzwerkhoheit im eigenen Unternehmen ist der Einsatz einer zweiten mit der Produktionsanlage in Reihe geschalteten Firewall empfehlenswert. Diese steht ausschließlich unter der Kontrolle des Anlagenbetreibers, um einen missbräuchlichen Zugriff auf weitere Netzwerksegmente im Fernwartungsfall zu verhindern.

Da praktisch keine technischen Maßnahmen bekannt sind, welche für alle Parteien ausschließlich die ihnen zustehenden Rechte durchsetzen kann, sollten Vertrauensbeziehungen heute mindestens durch entsprechende vertragliche Regelungen festgelegt werden. Ferner sollte eine Standardisierung von Fernzugriffkonzepten angestrebt werden. Dies würde die Integration in Unternehmen mit vielen angeschlossenen Partnern vereinfachen sowie die Kosten und Aufwände reduzieren.

5.1.3 Absicherung von Feldgeräten

Im Unterschied zu Systemen auf der Unternehmens-, Produktions- und Prozessleitebene sind Geräte auf der Feldebene unmittelbar in technische Prozesse integriert. Daher betreffen Angriffe diese Prozesse und die darin verarbeiteten Daten direkt. Die Feldebene kann von einem Angreifer dabei über zwei Wege erreicht werden. Zum einen sind durch die zunehmende vertikale Vernetzung der höheren Ebenen mit der Feldebene indirekte Angriffe von höher gelegenen Ebenen aus möglich. Diesen Angriffen muss durch die beschriebenen Maßnahmen auf der Unternehmens-, Produktions- und Prozessleitebene begegnet werden. Zum anderen können Angreifer mittels direktem physischen Zugriff auf Feldgeräte, wie beispielsweise durch Ankoppelung eines mobilen Endgerätes an den Feldbus oder Zugriff über die Programmierschnittstelle, den Versuch unternehmen, die Funktionalität oder die Kommunikation zu manipulieren.

Der direkte physische Zugriff durch einen Angreifer kann am besten durch physische Zugangsbarrieren verhindert werden. Wegen der oft weiten, lokalen Verteilung von Feldgeräten innerhalb eines Automatisierungssystems und der Exponiertheit der Systeme muss prinzipiell davon ausgegangen werden, dass ein Angreifer sich an beliebiger Stelle an die Feldebene ankoppeln kann. Maßnahmen für eine vollständige physische Zugangsbegrenzung sind daher in vielen Fällen mit hohen Kosten verbunden und aus diesem Grunde ungeeignet. Die Verwendung von Drahtloskommunikation kann ebenfalls gegen den Einsatz derartiger Maßnahmen sprechen.

Kommen Internet-Kommunikationsprotokolle bzw. Industrial Ethernet zum Einsatz, können zur Absicherung von Automatisierungssystemen Firewalls mit spezifischen Regeln für IP-basierte Kommunikationsprotokolle der Automatisierungstechnik eingesetzt werden. Diese Absicherung greift jedoch nicht, wenn ein Angreifer sich direkt, physisch mit einem Gerät der Feldebene verbindet. Basiert die Kommunikation, wie in den meisten Fällen, nicht auf Internet-basierten Protokollen, können konventionelle Firewalls nicht ohne Weiteres eingesetzt werden, da sie für das IP-Adress-/Port-Schema konzipiert sind. Allerdings können hier entsprechend geeignete Application Layer Gateways eingesetzt werden.

Kryptografische Maßnahmen zur Absicherung von Funktionalität, Kommunikation und Daten sind aus sicherheitstechnischer Sicht auch für die Feldebene geeignet. Wegen der hohen Echtzeitanforderungen und den geringen Ressourcen der meisten Systemelemente der Feldebene ist die Durchführung kryptografischer Operationen direkt auf den Komponenten in der Regel jedoch nicht möglich.

Ähnliches gilt für den Einsatz von Systemen zur Anomalie-Erkennung (z. B. Intrusion Detection Systeme (IDS)). Zum einen sind derartige Systeme für bestimmte Betriebssysteme konzipiert und somit für den Einsatz in den heterogenen Landschaften der Automatisierungstechnik schlecht geeignet. Zum anderen benötigen auch sie eine nicht unerhebliche Rechenleistung der Systeme auf denen sie laufen. Feldgeräte können diese Ressourcen in der Regel nicht zur Verfügung stellen.

Sowohl kryptografische Maßnahmen als auch Systeme zur Anomalie-Erkennung können auf der Feldebene in Form von zusätzlichen speziellen Hard- und Softwarekomponenten mit Sicherheitsfunktionalität (Security Appliances) eingebracht werden. Diese Appliances werden direkt vor die Geräte der Feldebene geschaltet und übernehmen z. B. die Durchführung kryptografischer Operationen. Die Anzahl der benötigten Appliances kann je nach Größe eines Automatisierungssystems jedoch sehr hoch werden, so dass ihr Einsatz mit hohem Aufwand und Kosten verbunden sein kann. Während das notwendige Schutzniveau durch Security Appliances durchaus erreicht werden kann, ist ihr Einsatz aus wirtschaftlicher Sicht dann oft nicht möglich.

Kryptografische Maßnahmen, Firewalls und Systeme zur Anomalie-Erkennung sind aus Sicherheitsperspektive geeignet, ein adäquates Schutzniveau auf der Feldebene zu erreichen. Sowohl Manipulation der Funktionalität (Ausfälle, Veränderung der Verhaltensweise usw.) und Kommunikation als auch der unbefugte Informationsgewinn (Abgreifen vertraulicher Informationen) können durch diese Maßnahmen wirksam verhindert werden.

Entsprechende Maßnahmen aus dem ICS-Security-Kompendium finden sich dort in Kapitel 5.4.7 (Absicherung von Feldgeräten, Seite 61):

- 30. Anforderungen an Feldgeräte

Hindernisse bei der Umsetzung

Das Fallbeispiel aus der chemischen Industrie (vgl. Abschnitt 4.1.3) zeigt, in welchem Maße die Vernetzung von Anlagen über Standortgrenzen bereits heute Wirklichkeit ist. Die damit verbundene große Angriffsfläche unterstreicht die Wichtigkeit des Ansatzes, Sicherheit bereits auf der Feldebene zu adressieren. Hauptsächliche Hinderungsgründe für die Integration der erwähnten Maßnahmen in die Feldgeräte selbst sind die hohen Anforderungen der Feldebene an Echtzeitfähigkeit und Verfügbarkeit. Gleichwohl haben vergangene Arbeiten gezeigt, dass die Integration von beispielsweise Kryptografie mit entsprechend gewählten Algorithmen und deren Parametern auch in Systemkomponenten der Feldebene möglich ist, ohne dabei die Echtzeitanforderung oder Verfügbarkeit einzuschränken.[320] Ein weiterer Hinderungsgrund ist die Heterogenität der Systemkomponenten auch innerhalb einer Automatisierungsumgebung.

Die Kompatibilität eines bestimmten Feldgerätes oder Feldbusses kann ein weiteres Hindernis bei der technischen Umsetzung einer Schutzmaßnahme sein, wenn diese bestimmte Anforderungen voraussetzt, welche nicht durchgängig in allen Geräten gegeben ist. Dies ist beispielsweise der Fall, wenn Feldgeräte nicht alle Funktionen eines Protokolls vollständig implementieren, welche zur effektiven Umsetzung einer bestimmen Sicherheitsmaßnahme erforderlich wären.

Handlungsvorschlag

Es ist zu prüfen, wie hoch der Schutzbedarf ist und entsprechend auch, ob das identifizierte Niveau erreicht werden kann, ohne dabei Eigenschaften, wie Verfügbarkeit und Echtzeit einzuschränken. Es sollten Maßnahmen zum physischen Zugriffsschutz für die schutzbedürftigsten Komponenten ergriffen werden.

Die Erkenntnis, dass Sicherheitsfunktionalität auf Feldebene möglich ist, ohne Echtzeitfähigkeit und Verfügbarkeit zu gefährden, muss vor allem Herstellern von Systemkomponenten für die Feldebene bewusst gemacht werden. Hersteller sollten diese Funktionalität in künftige Produkte integrieren.

Hersteller sollten im Rahmen von geförderten Forschungsprojekten motiviert werden, zusammen mit Forschungseinrichtungen Systemkomponenten für die Feldebene mit integrierter Sicherheitsfunktionalität zu entwickeln.

Firewalls sollten grundsätzlich eingesetzt werden, wenn Systeme auf Basis von Industrial-Ethernet vernetzt werden.

5.1.4 Absicherung der Netze

Zur Absicherung von IP-Netzwerken eigenen sich diverse Technologien, die sich seit vielen Jahren bereits in der Office-IT etabliert haben, jedoch in der Industrie-IT kaum bis gar nicht Verwendung finden. Im Wesentlichen fallen unter diese Technologien diverse Firewall-Lösungen, Proxy-Lösungen, Netzwerksegmentierung, Intrusion Detection Systeme (IDS) und die Verwendung von sicheren Protokollen. Bevor allerdings der Einsatz von Sicherheits-Appliances erfolgt, sollte zunächst einmal die Angriffsfläche auf die beteiligten Netzwerkteilnehmer reduziert werden, indem z. B. nicht benötigte Schnittstellen (sowohl Netzwerkschnittstellen, als auch andere) deaktiviert und ggf. unzugänglich gemacht werden. Mittels Netzwerksegmentierung und VLAN können dann Netzwerksegmente unterschiedlicher Schutzklassen realisiert werden. Diese Segmente können dann mit Firewall-Technologien, Proxies, und Datendioden geschützt werden. Um die Angriffsfläche für Angreifer weiter zu verringern, können automatische Netzwerkkonfigurationen zu Gunsten Statischer deaktiviert werden. In besonderem Maße müssen dabei funkbasierte Netzwerke konfiguriert und geschützt werden, da hierbei kein direkter physikalischer Zugriff auf Netzwerkkomponenten für einen Angriff notwendig ist. Funknetzwerke sollten demnach immer das höchstmögliche Maß an Sicherheitsmaßnahmen verwenden, welches die beteiligten Netzwerkteilnehmer unterstützen. Ist das Netzwerk im Betrieb und so sicher wie möglich konfiguriert, sollte sichergestellt werden, dass die Netzwerkteilnehmer sichere Protokolle nutzen, z. B. HTTPS gegenüber HTTP, SSH gegenüber TELNET.

320 Vgl. Felix Gutbrodt, „Effizienter Schutz der IT-Sicherheit auf der Feldebene von Automatisierungssystemen“, Fakultät Informatik, Elektrotechnik und Informationstechnik der Universität Stuttgart, 2009.

Neben diesen Technologien ist auch der zusätzliche Betrieb von Intrusion-Detection-Systemen (IDS) möglich, welche im Wesentlichen den Netzwerkverkehr des Unternehmens analysieren, um bekannte Angriffsmuster zu detektieren und entsprechende Gegenmaßnahmen einzuleiten.

Entsprechende Maßnahmen aus dem ICS-Security-Kompendium finden sich dort in Kapitel 5.6.1 (Seite 61ff):

- 32. Netzsegmentierung
- 33. Absichern der elektronischen, externen Schnittstellen
- 34. statische Netzkonfiguration
- 35. Gleiche Sicherheitsmaßnahmen für ICS in einer Netzsegmentierung
- 36. Unabhängiger Betrieb der Netzsegmente
- 37. Absichern der Funktechnologien
- 38. Einsatz von Firewalls
- 39. Host-based Firewalls
- 40. Datendiode (One-Way-Gateway)
- 41. Geeignete logische Trennung und VLAN
- 42. Implementierung von Intrusion-Detection- bzw. Intrusion-Prevention-Systemen
- 43. Nutzung von sicheren Protokollen

Hindernisse bei der Umsetzung

Am Fallbeispiel aus der chemischen Industrie (vgl. Abschnitt 4.1.3) lässt sich die Bedeutung der Vernetzung von Anlagen erläutern. Hier steht der gewachsene Bedarf nach Querverbindungen durch alle Ebenen zu dedizierten Anwendungen auf der Leit- oder Office-IT-Ebene einer konsequenten Segmentierung der Netzwerke sowie Einführung eines Zellschutzkonzeptes, wie im Fallbeispiel aus der chemischen Industrie beschrieben („Defense In Depth"-Ansatz, vgl. Abschnitt 4.1.3), entgegen. Offene elektronische Datenschnittstellen, wie z. B. USB, sind in fast allen IT-Systemen vorhanden und deren flächendeckende Einschränkung nur schwer umzusetzen, da diese auch physisch in unterschiedliche Zuständigkeitsbereiche fallen. So sind beispielsweise innenliegende Schnittstellen, die nicht nach außen geführt wurden oder Schnittstellen, deren Nutzbarkeit im Regelfall durch Schaltschränke/-kästen physisch eingeschränkt werden, dennoch kleineren Personenkreisen, wie z. B. Herstellern oder Servicepersonal, zugänglich. Werden solche Schnittstellen nicht ebenfalls konsequent blockiert oder kontrolliert, können darüber ggf. Kommunikationspfade geöffnet werden, welche nicht durch ein Zellschutzkonzept vorgesehen waren.

Ein unabhängiger Betrieb von Netzwerksegmenten ist bereits bei der Verwobenheit heutiger Produktions- und IT-Prozesse nur theoretisch möglich, wenn zwar die Netzwerkkomponenten für den unabhängigen Betrieb ausgelegt, jedoch die Produktionsprozesse von übergeordneten IT-Prozessen abhängig sind.

Der konsequente Einsatz von IDS- und IPS-Systemen ist schwierig, da betroffene Komponenten in der Praxis schlecht isoliert werden können, um die Produktion nicht zu gefährden.

Handlungsvorschlag

Es wird die Schaffung dezidierter Übergabepunkte für Daten zwischen den Ebenen und auch Unternehmensgrenzen und die konsequente Blockierung/Sperrung aller übrigen Verbindungsmöglichkeiten empfohlen.

Der Einsatz von Funktechnologien in neuen Anlagen sollte vertraglich abgesichert und dokumentiert werden, um der unkontrollierten Einbringung weiterer nicht dokumentierten Funknetzwerke entgegenzuwirken. Für die Konfiguration von Funknetzwerken sollte zwingend die höchstmögliche Sicherheitsstufe gewählt werden und Datenübertragungen sollten nur über verschlüsselte Funkverbindungen und Protokolle einsetzen. Nach Möglichkeit sollte Whitelisting für zulässige Geräte und Verbindungen verwendet werden.

5.1.5 Datensicherung

Um Datenverluste möglichst zu vermeiden, muss in regelmäßigen Intervallen eine Datensicherung (Backup) aller relevanten Daten erfolgen. Ein zugrundeliegendes Datensicherungskonzept sollte folgende Aspekte berücksichtigen bzw. regeln:

1. Zeitintervall: Wird eine Sicherung bspw. täglich, wöchentlich oder monatlich durchgeführt?

2. Zeitpunkt: Wird eine Sicherung bspw. nachts oder sonntags durchgeführt?

3. Umfang der zu sichernden Daten: Werden vollständige Sicherungen und/oder inkrementelle Sicherungen durchgeführt?

4. Anzahl der aufzubewahrenden Generationen: Werden bspw. Tagessicherungen nach sieben tagen gelöscht, während Wochensicherungen mehrere Monate lang aufbewahrt werden?

5. Speichermedium: Abhängig von der Datenmenge muss ein geeignetes Medium gewählt werden, bspw. DVDs, Bänder oder Festplatten.

6. Sicherstellung der Integrität: Zusätzlich zu den eigentlichen Daten sollten Metadaten gesichert werden, mit deren Hilfe Veränderungen an den Stammdaten festgestellt werden können.

7. Zuständigkeit für die Durchführung und Überwachung der Sicherung.

Die Datensicherung sollte mindestens alle Daten umfassen, die nicht ohne Weiteres aus anderen Daten wieder gewonnen werden können oder deren Erstellung viel Zeit in Anspruch nehmen würde. Dazu zählen:

- Betriebssysteme und Firmware,
- Konfigurationen (z. B. Switches, Firewalls etc.)
- Anwendungsprogramme
- Datenbanken, Produktionsdaten, sonstige Daten

Insbesondere die Punkte 1-3 betreffen u. U. die Performanz und Verfügbarkeit betroffener Systeme. Um bspw. Produktionsstillstände durch überlastete Komponenten zu vermeiden, muss je nach Szenario eine passende Backup-Strategie gewählt werden.

Punkt vier betrifft den Aspekt der Datenaufbewahrung. Unabhängig von der Dauer der Aufbewahrung gilt es zu beachten, dass die Speichermedien in einem geeigneten Umfeld aufbewahrt werden, welches zum einen Schutz vor Einflüssen wie Feuer oder Feuchtigkeit bietet und gleichzeitig einen unmittelbaren Zugriff durch ausschließlich berechtigte Personen ermöglicht.

Datensicherungsmechanismen können verwendet werden, um bestimmten Bedrohungen der Verfügbarkeit und Integrität von Daten bzw. Systemen zu begegnen. Zwar werden Angriffe durch die Maßnahmen erst einmal nicht verhindert, sie helfen jedoch nach Schadenseintritt schnell wieder in einen betriebsbereiten Zustand zu gelangen, bzw. in Form von Daten vorliegendes Know-how schnell wieder herzustellen. So könnte eine manipulierte Datenbank aus Bedrohung 1.10 auf Basis eines Backups zügig wieder hergestellt werden (sofern die Manipulation erkannt wurde), so dass die angeschlossenen Prozessleitsysteme (PLS) und Manufacturing Execution Systems (MES) wieder fehlerfrei arbeiten können. Auch die Auswirkungen eines DoS-Angriffs wie aus Bedrohung 1.8 können auf diese Art und Weise begrenzt werden. Es gilt zu beachten, dass Datensicherungsmaßnahmen lediglich als reaktive und damit nachgelagerte Maßnahme dienen können. Sie müssen durch vorgelagerte proaktive Sicherheitsmaßnahmen unterstützt werden.

Entsprechende Maßnahmen aus dem ICS-Security-Kompendium finden sich dort in Kapitel 5.6.9 (Seite 75ff):

- 71. Datensicherungen der Systeme
- 72. Aufbewahrung der Datensicherungen

Hindernisse bei der Umsetzung

Die Verfügbarkeit und Echtzeitfähigkeit von Produktionskomponenten dürfen durch die Datensicherungsmaßnahmen nicht beeinträchtigt werden. Es ist daher nicht immer möglich, Datensicherungen in der gewünschten Frequenz und dem gewünschten Umfang durchzuführen. Insbesondere spielen diesbezüglich die Faktoren Datensicherungsfrequenz, Datensicherungsmenge und Datensicherungszeitpunkt eine Rolle. Um eine optimale Strategie zu erreichen, müssen diese Parameter von Fall zu Fall variiert werden.

Auch die Verschlüsselung von Daten kann ein Problem darstellen. Sensitive Daten werden unter Umständen in verschlüsselter Form an Produktionsmaschinen oder andere angeschlossene Systeme übermittelt. Werden diese Daten durch Datensicherungskonzepte erfasst, so muss sichergestellt werden, dass die Daten entweder in unverschlüsselter Form gesichert werden (in diesem Fall müsste die Sicherung an den Ursprungssystemen, auf denen die Daten unverschlüsselt vorliegen, ansetzen) oder es muss die

Möglichkeit bestehen, die Daten auch aus den Backups heraus wieder entschlüsseln zu können. Die Sicherung sensitiver Daten in verschlüsselter und integritätsgesicherter Form ist aus Sicht der IT-Security zu bevorzugen.

Handlungsvorschlag

Wegen der hohen Anforderungen an Verfügbarkeit und Echtzeitfähigkeit sollten Datensicherungskonzepte immer nur diejenigen Daten beinhalten, die auch unbedingt gesichert werden müssen. Die Datensicherungsfrequenz sollte eng am jeweiligen Kontext ausgerichtet werden. Ändern sich beispielsweise Konfigurationsdateien bestimmter Komponenten nur selten, so kann ein ereignisbasierter Sicherungsmechanismus in Betracht gezogen werden. Auch die Möglichkeit inkrementeller, intelligenter Backups sollte genutzt werden, so dass nicht bei jeder Sicherung alle vorhandenen Daten gesichert werden müssen. Unter Umständen ist es eine Option, Datensicherungszeitpunkte mit Phasen des Produktionsstillstands z. B. während durchgeführter Wartungsarbeiten abzustimmen. Liegen dieselben Daten an mehreren Orten vor (bspw. Produktionsdaten die von einem Quellsystem an Produktionsmaschinen übertragen werden), so sollte die Sicherung immer an dem Ort erfolgen, an dem die meisten Ressourcen (CPU, Hauptspeicher etc.) verfügbar sind, bzw. an dem der Anspruch an Verfügbarkeit und Echtzeitfähigkeit am geringsten ist.

Handelt es sich bei den zu sichernden Daten um verschlüsselte Daten, so ist zu prüfen, ob die Speicherung der Daten in unverschlüsselter Form ein Sicherheitsrisiko darstellt (die Speicherung von Daten in einer entfernten, unternehmensfremden Cloud-Lösung wäre bspw. ein sicherer Indikator, der für eine verschlüsselte Speicherung der Daten spricht). Möglicherweise ist eine Verschlüsselung bestimmter Daten nur sinnvoll, solange diese innerhalb der Produktion gespeichert werden und könnten an einem separaten Sicherungsort auch unverschlüsselt gespeichert werden. Alternativ müssten die Verschlüsselungsschlüssel ebenfalls (verschlüsselt) gesichert werden.

5.1.6 Schutz vor Schadsoftware (Malware)

Zur Erkennung und Vermeidung der Ausbreitung von Schadprogrammen wie Viren und Trojanern im ICS-Umfeld sollten passende Maßnahmen implementiert werden.

Prinzipiell kommen dabei Blacklisting- oder Whitelisting-Ansätze[321] in Frage. Der Blacklisting-Ansatz entspricht dem Einsatz von Virenschutzprogrammen. Antivirus-Software erkennt bösartige Software anhand von Signaturen und ist daher auf die regelmäßige Aktualisierung der Signaturdatenbank angewiesen. Erkennt ein Virenschutzprogramm bösartige Software, so kann es je nach Konfiguration auf unterschiedliche Art und Weise auf die infizierte Datei reagieren, beispielsweise Datei-Quarantäne oder Blockade bestimmter Kommunikationswege. Beim Application-Whitelisting wird ein umgekehrter Ansatz verfolgt, d. h. es wird nicht versucht, unerwünschte Software zu blockieren, sondern es wird ausschließlich die Ausführung erwünschter Programme gestattet.

Gelingt es einem Angreifer, eingeschleuste Programme auf einem kompromittierten System auszuführen, sind prinzipiell Angriffe auf sämtliche Schutzziele möglich. Die installierte Schadsoftware könnte Daten verändern, mit dem Ziel, Prozesse gänzlich lahmzulegen (Verfügbarkeit) oder Prozesse unbemerkt zu verändern (Integrität). Genauso gut könnte ein Schadprogramm unbemerkt Nutzereingaben protokollieren, um auf diese Weise an Passwörter zu gelangen oder es könnte Daten direkt ausspähen (Vertraulichkeit). Daher begegnet man durch die Anwendung von Black- und Whitelisting-Ansätzen entweder direkt oder indirekt den meisten der zu Beginn dieses Kapitels aufgeführten Bedrohungen. Da es viele weitere Angriffspfade in Bezug auf die genannten Bedrohungen gibt, dürfen die in diesem Abschnitt beschriebenen Maßnahmen jedoch nicht exklusiv verstanden werden. Black- und Whitelisting-Ansätze sind im Sinne eines Defense-in-Depth-Ansatzes immer durch weitere flankierende Sicherheitsmaßnahmen zu ergänzen.

Black- und Whitelisting-Ansätze verhindern den direkten oder indirekten Start unerwünschter Software und Skript-Dateien (Viren, Trojaner usw.) durch Benutzer und Administratoren. So können unerlaubte Zugriffe auf das System selbst oder daran angeschlossene Systeme verhindert werden. Whitelisting-Ansätze können verhindern, dass unbekannte Schadprogramme (z. B. Zero-Day-Exploits), welche unerwünschte Software und Skript-Dateien starten, zu Sicherheitslücken führen, während Virenschutzprogramme in derselben Situation versagen würden.

Entsprechende Maßnahmen aus dem ICS-Security-Kompendium des BSI finden sich dort in Kapitel 5.6.7 (Schutz vor Schadprogrammen, Seite 71ff):

321 Siehe auch Industrial Internet Reference Architecture, Version 1.7, Seite 54, http://www.iiconsortium.org/IIRA-1-7-ajs.pdf

- 59. Installation und Betrieb von Virenschutzprogrammen
- 60. Geeignete Alternativen für den Fall, dass keine Virenschutzprogramme möglich sind
- 61. Sichere Konfiguration von Virenschutzprogrammen
- 62. Zentraler Viren-Signaturen-Verteildienst
- 63. Zeitnahe Aktualisierung der Viren-Signaturen
- 64. Virenschutzprogramm auf der Firewall (Virus Wall)
- 65. Application Whitelisting

Hindernisse bei der Umsetzung

Im industriellen Umfeld hat das Schutzziel der Verfügbarkeit, bedingt durch die verbundenen Produktionsprozesse, höchste Priorität vor allen anderen Schutzzielen. Die Verwendung von Antiviren-Software und die mit ihr verbundenen möglichen Performance-Verluste durch Scan-Vorgänge stellen für viele Anwendungsfälle ein Problem dar. Gängige Maßnahmen, wie sie im Bereich der Office-IT Verwendung finden, beispielsweise Datei-Quarantäne oder das Herunterfahren eines Systems bei Infektion, sind ebenfalls so nicht umsetzbar. Weitere Gründe, die gegen den Einsatz von Antiviren-Software sprechen können, sind fehlende Freigaben einer ICS-Komponente durch den Hersteller (und damit einhergehende Service Level Agreements (SLAs)), fehlende Performance bestimmter Komponenten (z. B. SPS oder Feldgeräte) oder fehlende Produktangebote für diese Komponenten. Auch die notwendige Pflege einer Antiviren-Lösung kann unter Umständen gegen den Einsatz einer solchen sprechen, wenn beispielsweise regelmäßige Updates der Signaturdatenbank nicht möglich sind oder zur Beeinträchtigung der Verfügbarkeit führen würden.

Handlungsvorschlag

Bei der Anschaffung von ICS-Komponenten sollte auf die Möglichkeit des Einsatzes von Virenschutzprogramen Rücksicht genommen werden. Vor allem auf der Ebene der Prozessleitsysteme, die häufig auf Microsoft Windows aufsetzen, existieren am Markt befindliche Produkte mit expliziter Unterstützung und Freigabe für den Einsatz und das Management von Virenscannern.

Für bestehende Anlagen und Komponenten sollte die Möglichkeit des Einsatzes von Virensoftware und die Freigabe durch den Hersteller für konkrete Scanner in jedem Falle geprüft werden. Ist der Einsatz möglich, aber noch kein Virenschutzprogramm installiert, so sollte dies nachgeholt werden.

Wenn der Einsatz von Antivirensoftware nicht möglich ist, sollten flankierende Maßnahmen getroffen werden, beispielsweise die Auslagerung der betroffenen Komponenten in ein eigenes Netzwerksegment und Schutz dieses Segments mittels einer Firewall, welche auch eine Virenscan-Funktion implementiert. Ähnlich wie bei den Prozessleitsystemen gibt es am Markt befindliche Produkte, welche diese Funktionalität für das ICS-Umfeld implementieren.

Bei Bedenken bzgl. eingeschränkter Verfügbarkeit durch Virenschutzprogramme sollte geprüft werden, ob diese Bedenken durch eine spezifische Konfigurationen des Scanners ausgeräumt werden können (z. B. System-Scans nur während ohnehin festgelegter Wartungsfenster, während Zeitfenstern mit geringer Auslastung der Anlage oder durch ausschließliche Prüfung lokaler Medien).

Whitelisting ist bei den neueren Microsoft-Betriebssystemen Windows 7 und Windows 2008 R2 von Haus aus möglich und über Umwege auch bei Windows XP. Außerdem gibt es am Markt befindliche Produkte von Drittanbietern, die das Whitelisting ermöglichen. White- und Blacklisting-Ansätze haben jeweils eigene Vor- und Nachteile und sollten – falls möglich – im Sinne einer Defense-In-Depth-Strategie parallel betrieben werden.

Hersteller von z. B. Steuerungssystemen, SPS und Feldgeräten sollten bei Neuentwicklungen die Kompatibilität mit Virenschutzlösungen explizit berücksichtigen.

5.1.7 Härtung der IT-Systeme

Eine Härtung von IT-Systemen und -Komponenten kann Stand heute bei deren Herstellung (Hard- und Softwareentwicklung), der Integrationsphase, der Inbetriebnahme (vgl. Kapitel 5.1.1) und dem Betrieb der IT-Systeme vorgenommen werden. Hierbei kommt dem Systemhersteller eine besondere Bedeutung zu, da er bei der Entwicklung der Komponenten die Grundlage für alle Härtungsmaßnahmen schafft. Bestimmte Aufgaben können beispielsweise nur durch den Hersteller erledigt werden, wie beispielsweise Implementierung einer Logdatenerfassung oder Schutzmaßnahmen für Konfigurationsschnittstellen.

Die weitere Härtung der IT-Systeme beginnt betreiberseitig mit ersten Maßnahmen zur Härtung während der Inbetriebnahme, siehe auch Abschnitt „Inbetriebnahme in sicherer Konfiguration".

Eine Härtung von IT-Systemen bedeutet nach aktuellem Stand der Technik in Industrieanlagen und insbesondere deren Steuerungssystemen (ICS) 1) den richtigen Umgang mit Standard-Benutzerkonten und -Passwörtern, 2) die konsequente Einführung und Nutzung individueller Benutzerkonten und falls nicht möglich eine Risikoanalyse auf Basis bestehender Schutzmaßnahmen, 3) das Entfernen von unnötiger Software und unnötigen Diensten, 4) eine Anpassung der Standard-Einstellungen, 5) das Anpassen der Hardware-Konfiguration und 6) die Unterbindung eines freien Internetzugriffs innerhalb des ICS-Netzwerks.

Betreiberseitig sind üblicherweise folgende Punkte bzw. Empfehlungen bzgl. der Konfiguration für einen sicheren Betrieb (z. B. Leitfaden zur Systemhärtung), zu beachten, wie bspw. in BSI-CS 067[322] gefordert:

a) Gibt es ausreichende Hinweise für die Änderung von Standardpasswörtern und zum Deaktivieren von nicht benötigten Benutzerkonten/Accounts?

b) Sind die sicherheitsspezifischen Konsequenzen der möglichen Konfigurationsoptionen/-alternativen dokumentiert?

c) Gibt es Hinweise darauf, welche Einstellungen als kritisch zu betrachten sind und ggf. zu einer erhöhten Gefährdung führen?

d) Gibt es eine Checkliste zur Übersicht über die Konfiguration und deren sicherheitsspezifische Implikationen?

Außerdem dient das Prinzip der Zonierung der Härtung des Gesamtsystems gegenüber Angriffen und ist im Standard IEC 62443-3-2 explizit eingeführt worden. Zonen werden durch physikalische und/oder logische Trennung auf Netzwerkebene implementiert. Netzwerkzonen stellen einen Defense-in-Depth-Ansatz auf Netzwerkebene dar. Eine Anforderung kann zum Beispiel sein, dass Safety relevante Systeme in einer eigenen Zone implementiert werden müssen.[323]

Hinsichtlich einer Systemhärtung werden praktisch alle in Kapitel 4.5.1.5.4 der Studie identifizierten Bedrohungen adressiert, da insbesondere die im ICS-Security-Kompendium genannte Maßnahme 26 „Aktivierte Sicherheitsmechanismen und aktueller Patchstand" eine implizite Verbesserung der Sicherheitssituation für fast alle Bedrohungen bedeutet. Dies gilt insbesondere für die folgenden Bedrohungen (vgl. „Nummerierte Bedrohungen aus Kapitel 4" und „Kreuztabelle der Bedrohungen und Maßnahmen des ICS-Security--Kompendiums" im Anhang Bedrohungen und Mapping auf Maßnahmen):

- 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.8
- 3.1, 3.2, 3.3, 3.5, 3.6, 3.7
- 4.1, 5.1

Die Maßnahmen Standard-Benutzerkonten und -Passwörter sowie die Vergabe von individuellen Benutzerkonten schützen vor den Bedrohungen 1.1, 1.2, 1.3, 1.4, 1.6, 3.3, 3.5, 4.1, 5.1, da sie die Grundlage für klare Zugriffskontrolle und Nachvollziehbarkeit des Zugriffs auf IT-Systeme bilden.

Entsprechende Maßnahmen aus dem ICS-Security-Kompendium des BSI finden sich dort in Kapitel 5.6.3 (Härtung der IT-Systeme, Seiten 67ff):

- 46. Standard-Benutzerkonten und -Passwörter
- 47. Individuelle Benutzerkonten
- 48. Entfernen von unnötiger Software und unnötigen Diensten
- 49. Anpassen der Standard-Einstellungen
- 50. Anpassen der Hardware-Konfiguration
- 51. Zugriff auf das Internet innerhalb des ICS-Netzwerk

322 Siehe BSI-CS 067 | Version 1.20 vom 31.03.2015;
siehe https://www.bsi.bund.de/ACS/DE/_/downloads/BSI-CS_067.pdf?__blob=publicationFile&v=2

323 Siehe IT-Sicherheit auf Basis IEC 62443 für elektrische Signalanlagen, Thomas Störtkuhl, in SIGNAL und DRAHT 10/2014,
http://www.tuev-sued.de/uploads/images/1414667642244290241287/k-ds-print-iec62443-signal-draht-10-2014.pdf

Hindernisse bei der Umsetzung

Die Realität im industriellen Kontext kann, ähnlich wie im Falle der sicheren Inbetriebnahme (vgl. Kapitel 5.1.1) in diesem Punkt erheblich von der Situation in der Office-IT abweichen. Oftmals lassen sich individuelle Benutzerkonten auf IT-Systemen in Industrieumgebungen aufgrund von Verfügbarkeitsanforderungen nicht umsetzen. Praktische Erfordernisse in der Produktion oder der Prozessindustrie können eine individuelle Konfiguration von Zugriffsberechtigungen, die an einzelne Personen/Maschinen gebunden ist, unmöglich machen bzw. würden einen erheblichen organisatorischen Mehraufwand bedeuten oder sogar ein schnelles Einschreiten im Fehlerfall unnötig erschweren.

Oft fehlen zudem auch sicherheitsrelevante Konfigurationsmöglichkeiten. So können bspw. Funktionen mit potenziellem Sicherheitsrisiko nicht deaktiviert werden, weil dies im Rahmen der Konfigurationsmöglichkeiten nicht vorgesehen wurde.

Am Fallbeispiel aus der chemischen Industrie (vgl. Abschnitt 4.1.3) lassen sich die Hindernisse der Härtung des Gesamtsystems gegenüber Angriffen durch das Prinzip der Zonierung zeigen. Hier steht der gewachsene Bedarf nach Querverbindungen durch alle Ebenen zu dedizierten Anwendungen auf der Leit- oder Office-IT-Ebene einer Einführung eines Zellschutzkonzeptes wie im Fallbeispiel beschrieben („Defense In Depth“-Ansatz, vgl. Abschnitt 4.1.3) entgegen.

Handlungsvorschlag

Eine Härtung von IT-Systemen im ICS-Umfeld geht immer mit Kompromissen und Zugeständnissen an die Erfordernisse anderer Systeme einher (vgl. auch Kapitel 5.1.1). Werden mit einer Anlage zusammenwirkende Systeme verbunden, sollten die oben genannten Maßnahmen im Rahmen der jeweiligen Möglichkeiten maximal ausgenutzt werden. Betreiber von Industrieanlagen sollten moderne Benutzerkonzepte konsequent umsetzen. Dort wo individuelle Benutzerkonten nicht möglich sind, lässt sich dies in Verbindung mit organisatorischen Schutzmaßnahmen lösen (vgl. Kapitel 5.2.1.1).

Es ist zur Härtung der IT-Systeme notwendig, dass die Komponenten an zentrale Identity and Access Management (IAM)-Systeme angebunden werden können und somit eine zentrale Verwaltung der Benutzerkonten (Identitäten, Zugriffsrechte etc.) ermöglicht wird (vgl. Kapitel 5.1.9).

Gleiches gilt beispielsweise auch für das Logging und Monitoring (vgl. ebenfalls Kapitel 5.1.9). Hier sind Aktivitäten der Hersteller und Betreiber erforderlich um entsprechende Funktionen bereitzustellen bzw. einzufordern.

5.1.8 Patchmanagement

Schwachstellen in Software von ICS können es Angreifern ermöglichen, Zugriff auf das System zu erlangen oder den Ablauf der Software und damit im Extremfall des Gesamtsystems stören. Daher gilt grundsätzlich, dass die für diese IT-sicherheitsrelevanten Schwachstellen verantwortlichen Fehler behoben werden müssen.

Die Maßnahme des aus IT-Sicherheitssicht notwendigen adäquaten Umgangs mit Patches adressiert eine Vielzahl von Bedrohungen für Industrielle Systeme (Bedrohungen mit den Nummern 1.1, 1.2, 1.3, 1.4), insb. hinsichtlich Rechteausweitung und Enthüllung.

Das Maßnahmenbündel zum sicheren Umgang mit Patches und End of support (EOS) umfasst die Etablierung eines Patchprozesses mit rollenspezifischen Verantwortlichkeiten und bewirkt einen Schutz für alle Prozesse im Rechenzentrum, indem eine Rechteausweitung durch Ausnutzung von Schwachstellen in Softwareanwendungen über Patches zeitnah und nachhaltig geschlossen werden kann. Auch falls keine Patches zur Verfügung stehen, können alternative Maßnahmen nach einer Risikoanalyse für Schutz gegen diese Angriffe sorgen, z. B. durch Isolierung der betreffenden Komponenten. Außerdem bietet ein etablierter Patchprozess Möglichkeiten, um Angriffe zu verhindern, welche Schwachstellen in der Software nutzen.

Entsprechende Maßnahmen aus dem ICS-Security-Kompendium des BSI finden sich dort in Kapitel 5.6.4 (Patchmanagement, Seiten 69f):

- 52. Umgang mit Patches

Hindernisse bei der Umsetzung

Im Gegensatz zur Office-IT können ICS-Systeme nicht zu beliebigen Zeitpunkten über (Security-)Patches aktualisiert werden, da bspw. ein Bedien- und Beobachtungssystem dem Bedienpersonal jederzeit zur Verfügung stehen muss, um industrielle Automatisierungsprozesse ständig im Auge zu haben.[324]

Das unkontrollierte Einspielen von sicherheitsrelevanten Softwareaktualisierungen dient zwar der Erhöhung der Sicherheit, kann jedoch im schlimmsten Fall den Betrieb durch Nichtverfügbarkeit von betriebsrelevanten IT-Systemen gefährden, wenn bspw. durch die Softwareänderungen Integritätsprüfungen fehlschlagen oder Netzwerkzugriffe nicht mehr möglich sind.[325] Auch kann die Aktualisierung eines vermeintlich unkritischen Systems schlimmstenfalls ganze Produktionsanlagen zum Stillstand bringen.

Im ICS-Umfeld kommt erschwerend hinzu, dass die Komponenten des Herstellers oft verfügbare Patches der Plattform (z. B. Microsoft Windows-Updates) noch nicht unterstützen und deren Anwendung daher nicht erlaubt ist. In vielen Fällen erlauben Gerätezertifizierungen oder behördliche Qualifizierungen ebenfalls kein Einspielen von Patches.

Patches können häufig nur in definierten Wartungsfenstern, die tendenziell eher im Zeitraum mehrerer Jahre als Wochen liegen, durchgeführt werden. Die Behebung von Softwareschwachstellen ist dadurch eines der am schwierigsten zu lösenden Probleme der industriellen Security-Welt geworden.[326]

Der Umgang mit Patches und die Etablierung eines State-of-the-Art-Patchprozesses gemäß BSI ICS-Security-Kompendium ist daher eines der großen Probleme in heutigen langlebigen Industrieanlagen, insbesondere wenn diese eine 24/7-Laufzeit haben und Wartungsfenster für Software-Updates sehr selten sind; in der Prozessindustrie existieren Wartungsfenster z. T. nur alle paar Jahre. Sicherheitskonzepte aus der "klassischen IT", wie das Patchen von Sicherheitslücken durch Software Updates, sind demnach nicht anwendbar bei Automatisierungs-Komponenten, welche auf Standard-Produkten (Hardware, Betriebssysteme, Protokolle) basieren, um kosteneffizient zu sein. Problem dabei ist, dass diese nur untergeordnete Bausteine einer Automatisierungsanlage sind, bei denen jede Änderung die Hauptfunktion gefährdet.[327]

Handlungsvorschlag

IT-Sicherheit kann nicht durch eine einmalige Aktion erreicht werden, die Bedrohungslage verändert sich kontinuierlich mit neuen technischen Möglichkeiten für potenzielle Angreifer oder mit der Entdeckung und Veröffentlichung von Schwachstellen in Standardprodukten und -komponenten. Es ist zudem essenziell, die Abhängigkeiten zwischen Systemen zu kennen. Hersteller und Betreiber müssen darauf mit Patches und Updates reagieren können, Möglichkeiten für das Einbringen von neuen IT-Security-Versionen müssen identifiziert und prozessual eingeplant werden.[328]

Handlungsempfehlung: State-of-the-Art-Softwarewartung by Design

ICS von Industrieanlagen der I4.0 müssen bereits vom Design so gestaltet sein und betrieben werden können, dass Softwarewartung problemlos möglich ist ohne die Verfügbarkeit des Systems zu beeinträchtigen. Dies ist bei Design und Entwicklung der Systeme (Hersteller), bei Inbetriebnahme (Integrator) und bei der Beschaffung und dem Betrieb (Betreiber) zu beachten.

Handlungsempfehlung: Einführung/Umsetzung eines „Patch Management Programms"

Wie bei allen komplexen Problemen empfiehlt sich auch hier eine systematische Herangehensweise, in Form eines „Patch Management Programms". Elementare Teile davon sollten mindestens sein:

324 Softwareschwachstellen als industrielles Betriebsrisiko, 27. Dezember, 2014, https://www.limessecurity.com/de/softwareschwachstellen-als-industrielles-betriebsrisiko/index.html, abgerufen am 10.07.2015.
325 Softwareschwachstellen als industrielles Betriebsrisiko, 27. Dezember, 2014, https://www.limessecurity.com/de/softwareschwachstellen-als-industrielles-betriebsrisiko/index.html, abgerufen am 10.07.2015.
326 Softwareschwachstellen als industrielles Betriebsrisiko, 27. Dezember, 2014, https://www.limessecurity.com/de/softwareschwachstellen-als-industrielles-betriebsrisiko/index.html, abgerufen am 10.07.2015.
327 Vgl. Industrie 4.0 "Sicherheit vernetzter Systeme", Ein Lagebericht, Dr. Lutz Jänicke, Februar 2014, Folie 15.
328 Vgl. Umsetzungsstrategie Industrie 4.0, Ergebnisbericht der Plattform Industrie 4.0, Seite 84.

- Konfigurationsmanagement: Welche Komponenten existieren im Betrieb?
- Patchmanagement Plan: Nach welcher Vorgehensweise werden Softwareaktualisierungen ausgewählt, verteilt und installiert?
- Patchverifikationsmethodik: Wie werden Patches auf Verträglichkeit geprüft?
- Backup- & Desaster Recovery Plan: Wie kann im Ernstfall der Softwarestand wiederhergestellt werden?

Des Weiteren wird empfohlen, einen nachvollziehbaren Entscheidungsprozess bezüglich der Notwendigkeit und Dringlichkeit von Patches anzuwenden.[329]

5.1.9 Authentisierung, Zugriffskontrolle, Protokollierung und Auswertung

Die Bedienung von ICS, insb. aus der Ferne, sollte sowohl im nur eingeschränkt vernetzten oder durch Zonierung[330] gekapselten Umfeld und insbesondere bei einer weitreichenden Vernetzung mit anderen IT-Systemen, nur von authentifizierten Subjekten möglich sein[331]. Dazu zählen im Rahmen der zunehmenden Automatisierung, Autonomik und Vernetzung von Maschinen nicht nur deren Bediener und IT-Systemnutzer, sondern neben gewöhnlichen Industrierechnern auch nahezu alle anderen IT-Systeme eines ICS, wie Router, Switches und SPS.

Zur Authentisierung können je nach ermitteltem Risiko und Schutzbedarf unterschiedliche Verfahren und Merkmale eingesetzt werden. Mehrfaktor-Authentisierung bietet im Gegensatz zu einer 1-Faktor-Authentisierung (z. B. Passwort oder Token) ein höheres IT-Sicherheitsniveau. Hierbei müssen Merkmale aus unterschiedlichen Klassen (Wissen, Besitz und wo anwendbar Biometrie) kombiniert werden. Dies gilt sowohl für Personen als auch für Maschinen im M2M-Umfeld, es unterscheiden sich lediglich die verwendbaren Merkmale. Im Falle von M2M beispielsweise hinsichtlich eines Schlüssels im Speicher oder in einer Datei (Wissen) und eines Hardwaresicherheitsankers wie TPM (Besitz).

Laut ICS-Security-Kompendium ist bei der Auswahl der Authentisierungsmethoden eine Risikoanalyse durchzuführen. Das Ergebnis hiervon muss mit weiteren Anforderungen (z. B. Störfallverordnung) und organisatorischen Rahmenbedingungen (z. B. Zugangsrestriktionen) abgeglichen werden, um ein geeignetes Verfahren zu identifizieren.

Dort wo die Nutzung von Passwörtern zur Authentisierung auch heute noch unumgänglich ist, muss eine Passwort-Richtlinie erstellt und durchgesetzt werden. Dabei können sowohl technische Lösungen als auch organisatorische Maßnahmen (vgl. Abschnitt 5.2.1.1) festgelegt werden. Außerdem sollte ein unautorisierter Zugriff auf IT-Systeme verhindert werden.

Hinsichtlich der Möglichkeit einer Protokollierung und Auswertung von Vorgängen im System sollte zudem soweit rechtlich zulässig (z. B. BDSG) und organisatorisch abgedeckt (z. B. über Mitarbeitervereinbarungen) erkennbar und dokumentierbar sein, welcher Benutzer bzw. welche Maschine oder welcher Dienst aktiv war. Nicht zuletzt muss eine Protokollierung und Möglichkeit zur Auswertung von Logdaten umgesetzt werden, um im Falle eines, ggf. gesetzlich vorgeschriebenen, Audits auf entsprechende Audit-Logs zurückgreifen zu können.

Wenn gemäß der gewählten Sicherheitsarchitektur (basierend auf Empfehlungen der Industrial Internet Reference Architecture[332] oder der RAMI 4.0 Referenzarchitektur[333]) kryptographische Algorithmen (z. B. Hashfunktion, symmetrische und asymmetrische Verschlüsselung) zum Einsatz kommen, sollten diese wo immer möglich dem Stand der Technik (z. B. BSI TR-02102) entsprechen.

Die Protokollierungsdaten eines ICS-Betreibers sollten auf einem zentralen Server gespeichert werden. So können die Protokollierungsdaten von verteilten Systemen und Komponenten zentral gesammelt, analysiert und in Zusammenhang gebracht werden. Von dort aus können Sie über eine definierte und abgesicherte (Authentisierung, Zugriffskontrolle und zusätzliche Protokollierung) Schnittstelle abrufbar gemacht und auch authentifizierten und autorisierten Partnersystemen innerhalb eines Wertschöpfungsnetzwerkes zur Verfügung gestellt werden, wenn sich diese Anfor-

329 Vgl. Softwareschwachstellen als industrielles Betriebsrisiko, Dezember 2014, https://www.limessecurity.com/de/softwareschwachstellen-als-industrielles-betriebsrisiko/index.html
330 Zonierung nach IEC 62443-3-2, Security for industrial automation and control systems: Part 3-2: Security risk assessment and system design.
331 Vgl. BSI-Security-Kompendium Maßnahmen 46, 47.
332 Siehe Industrial Internet Reference Architecture, http://www.industrialinternetconsortium.org/IIRA.htm
333 Siehe ZVEI-Faktenblatt Industrie 4.0: Das Referenzarchitekturmodell RAMI 4.0, http://www.zvei.org/Downloads/Automation/ZVEI-Faktenblatt-Industrie4_0-RAMI-4_0.pdf

derung, z. B. im Rahmen eines Audit bei einem Wertschöpfungsnetzwerkpartner ergibt.

In einem ICS sollten mindestens die folgenden Ereignisse protokolliert und zentral gesammelt werden, soweit diese verfügbar sind:

- lokale Ereignisse, z. B. der Betriebssysteme,
- Ereignisse von Domänen-Controllern,
- Firewall-/Router-/Switch-/Server-Ereignisse,
- Ereignisse der Virenschutzprogramme,
- Ereignisse des IDS/IPS.

Außerdem ist auf die geltenden Datenschutzbestimmungen zu achten.

Entsprechende Maßnahmen aus dem ICS-Security-Kompendium des BSI finden sich dort in Kapitel 5.6.5 (Authentisierung, Seiten 70f):

- 54. Technische Authentisierungsmaßnahmen
- 55. Passwortverteilung und -management, Passwort-Richtlinie
- 56. Vermeidung von Missbrauch

In Kapitel 5.6.6 (Zugriffskontrolle, Seiten 71f):

- 57 Zugriffskontrolle
- 58. Einsatz geeigneter kryptographischer Algorithmen

Und in Kapitel 5.6.10 (Protokollierung und Auswertung, Seiten 77f):

- 73. Logging / Monitoring

Auch ist explizit auf die in der Umsetzungsstrategie Industrie 4.0 – „Ergebnisbericht der Plattform Industrie 4.0“, Kapitel 7, „Sicherheit vernetzter Systeme“, exemplarisch genannten IT-Sicherheitsmaßnahmen zu verweisen (Kapitel 7.5, Seite 85ff).

Hindernisse bei der Umsetzung

Im industriellen Umfeld hat das Schutzziel der Verfügbarkeit, bedingt durch die verbundenen Produktionsprozesse, höchste Priorität vor allen anderen Schutzzielen. Die Verwendung von Software zur Zugriffskontrolle und die mit ihnen verbundenen möglichen Performance-Verluste und Verfügbarkeitsprobleme stellen für viele Anwendungsfälle ein Problem dar. Individuelle Benutzerkonten lassen sich oft auf Systemen in Industrieumgebungen nicht umsetzen da deren Einsatz z. B. in Betriebsregelwerken untersagt ist mit dem Ziel, eine andauernde Verfügbarkeit des Systems hinsichtlich des Zugriffs durch einen Benutzer zu gewährleisten. Gängige Maßnahmen der Zugriffskontrolle, wie sie im Bereich der Office-IT Verwendung finden, beispielsweise Need-to-Know durch Mandatory Access Control (MAC) sind ebenfalls so nicht umsetzbar. Weitere Gründe, die gegen den Einsatz von etablierten Verfahren aus dem Identity and Access Management (IAM)-Umfeld sprechen können, sind fehlende Freigaben einer ICS-Komponente für die Verwendung mit IAM-Software durch den Hersteller (und damit einhergehende SLAs), fehlende Performance bestimmter Komponenten (z. B. SPS oder Feldgeräte) oder fehlende Produktangebote für diese Komponenten oder wenn diese zur Beeinträchtigung der Verfügbarkeit führen würden.

Handlungsvorschlag

Nur wenn bekannt ist, welcher Nutzer zu welchem Zeitpunkt auf welches System Zugriff hat und haben darf, können unbefugte Zugriffe identifiziert und verhindert werden. Hierzu sind elektronische Identitäten und Zugriffsrechte notwendig. Betreiber von Industrieanlagen müssen hierzu moderne Benutzerkonzepte (föderierte Identitäten, Rollen- und Zugriffskontrollkonzepte) konsequent umsetzen. Dort wo individuelle Benutzerkonten nicht möglich sind, lässt sich dies in Verbindung mit organisatorischen Schutzmaßnahmen lösen (vgl. Abschnitt 5.2.1.1). Es ist zudem hilfreich, dass die Komponenten an zentrale IAM-Systeme angebunden werden können und somit eine zentrale Verwaltung der Benutzerkonten (Identitäten, Zugriffsrechte etc.) ermöglicht wird. Gleiches gilt auch für das Logging und Monitoring. Hier sind Aktivitäten der Hersteller und Betreiber erforderlich, um entsprechende Funktionen bereitzustellen bzw. einzufordern. Bei der Anschaffung von ICS-Komponenten sollte auf die Möglichkeit einer Integration in für den I40-Kontext und die entsprechende Sicherheitsarchitektur geeigneten IAM-Systeme Rücksicht genommen werden, welche die Anforderungen von ICS in

dynamischen Ad-hoc Wertschöpfungsnetzwerken über neue Ansätze wie bspw. risikobasierte Zugriffskontrolle berücksichtigen. Da entsprechende neuartige Ansätze[334] nicht in Produkten verfügbar sind, ist eine entsprechende Förderung und/oder Produktisierung derartiger Ansätze und Konzepte notwendig. Hersteller sollten im Rahmen von geförderten Forschungsprojekten motiviert werden, zusammen mit Forschungseinrichtungen entsprechende Systemkomponenten zu entwickeln.

5.1.10 Mobile Datenträger

Notebooks als mobile Wartungsgeräte, Wechseldatenträger und mobile Datenspeichermedien, wie USB, SD-Karten und CD, DVD oder Blu-ray) stellen aufgrund von einer möglichen Infizierung mit Schadsoftware und dem möglichen Abfluss von vertraulichen Daten ein Sicherheitsproblem von IT-Systemen von der Unternehmens-, Produktions- und Prozessleitebene bis hin zur Feldebene dar.[335] Zur Erkennung und Vermeidung der Ausbreitung von Schadprogrammen im ICS-Umfeld sollten daher passende Maßnahmen zum sicheren Umgang mit diesen mobilen Datenträgern eingeführt werden. Für die Nutzung von Wechseldatenträgern greifen einerseits Regelungen für den korrekten Umgang (vgl. Kapitel 5.2, organisatorische Aspekte). Technisch sollte die Nutzung mobiler Datenträger über Funktionen des Betriebssystems oder über zusätzliche Software auf bestimmte Geräte eingeschränkt werden (Device Control – Port Control und Device Management). Eine Wechseldatenträgerschleuse (Quarantäne-PC) ist vorzusehen. Prinzipiell kommen auch Sonderregelungen für Wartungsnotebooks sowie BIOS-Härtung (sichere Konfiguration durch Abschaltung nicht benötigter Funktionen, Laufwerke und Ports, aktiviertes BIOS-Passwort und eingeschränkte Boot-Optionen) in Frage.[336] Die Autorun-Funktion sollte auf allen Systemen deaktiviert sein. Falls diese Funktion aktiviert ist, können Programme z. B. auf mobilen Datenträgern unbemerkt nach deren Erkennung durch das Betriebssystem gestartet werden. Häufig nutzen Schadprogramme diese Funktion zur Verbreitung.

Entsprechende Maßnahmen aus dem ICS-Security-Kompendium des BSI finden sich dort in Kapitel 5.6.8 (Mobile Datenträger, Seiten 75f):

- 66. Umgang mit Wechseldatenträgern
- 67. Wechseldatenträgerschleuse (Quarantäne-PC)
- 68. Einsatz von Notebooks zu Wartungszwecken
- 69. Aktiviertes BIOS-Passwort und eingeschränkte Boot-Optionen
- 70. Deaktivierung der Autorun-Funktion

Hindernisse bei der Umsetzung

Hinsichtlich der Umsetzung der Maßnahmen zum sicheren Umgang mit mobilen Datenträgern sind keine Hindernisse erkennbar. Voraussetzung hierfür ist lediglich, wie auch im Kontext Härtung (vgl. Kapitel 5.1.7), die Unterstützung durch die Hersteller. Die starke Vernetzung im Kontext der I4.0 wird in vielen Anwendungsfällen einige Maßnahmen obsolet machen, da bspw. bei einer sicheren Fernwartung keine Wartungsnotebooks und mobile Datenträger zum Einsatz kommen und ebenso wie bei einer netzwerkgestützten Datenübertragung im Betrieb kein Einsatz von Konfigurationsdateien auf mobilen Datenträgern notwendig ist.

Handlungsvorschlag

Bei dem Umgang mit mobilen Datenträgern sind die Maßnahmen des ICS-Security-Kompendiums des BSI auch unter I40-Gesichtspunkten immer anzuwenden. Hierzu sind am Markt befindliche Produkte und zugehörige Dienstleistungen vorhanden, welche Funktionalität wie Quarantäne-PC und Device Control technisch ermöglichen.

Unterstützung der Analyse und Implementierung von IT-Sicherheitsmaßnahmen

Zur Unterstützung der Analyse und Implementierung von IT-Sicherheitsmaßnahmen im ICS-Kontext wird durch das BSI das kostenfreie Werkzeug Light and Right Security ICS (LARS ICS) zur Verfügung gestellt. Dieses Werkzeug verfolgt einen leichtgewichtigen Ansatz mit dem der Einstieg in die

334 Z. B. das vom BMWi im Rahmen der Trusted Cloud Initiative geförderte SkIDentity-Projekt.
335 Siehe ICS-Security-Kompendium des BSI, Kapitel 3.2.4 Mobile Datenträger und Laptops, Seite 31) und Cyber-Bedrohungen – und was dagegen zu tun ist, Artikel in Elektroniknet, http://www.elektroniknet.de/automation/m2m/artikel/114996/1/
336 IT-Grundschutz, Maßnahme M 4.237 Sichere Grundkonfiguration eines IT-Systems, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04237.html, zuletzt abgerufen am 09.07.2015.

Cyber-Sicherheit für kleine und mittlere Unternehmen (KMU) aus dem Umfeld industrieller Steuerungsanlagen erleichtert wird. Es bietet eine fragengeleitete Selbsteinschätzung des aktuellen Stands der Cyber-Security und gibt Empfehlungen, welche Maßnahmen in welchen Bereichen als nächstes umgesetzt werden sollten.[337]

5.2 Organisatorische und rechtliche Aspekte der Umsetzung und Eignung von Maßnahmen

I4.0 beschreibt die Vision einer industriellen Produktion der Zukunft, die durch einen hohen Grad an Dynamik geprägt ist. Daher erscheint es nötig, das Thema aus verschiedenen Perspektiven zu betrachten, um geeignete Lösungsansätze zu finden. Ein rein rechtlicher Ansatz wäre wohl schon vor dem Wirksamwerden der notwendigen gesetzlichen Anpassungen veraltet, wenn er den Stand der Technik zu einem bestimmten Zeitpunkt zugrunde legt und damit die Dynamik der IT verkennt. Ein rein technischer Ansatz kann zu Entwicklungen führen, die nicht den demokratisch legitimierten Zielsetzungen der Gesellschaft entsprechen. Daher ist es wichtig, die rechtlichen, technischen und organisatorischen Maßnahmen als Maßnahmenbündel zu verstehen.[338] Es erfolgt daher ganz bewusst eine sehr breit angelegte Betrachtung, denn nur so kann den vielschichtigen Anforderungen ausreichend Rechnung getragen werden. Zudem erfordern organisatorische Maßnahmen im Kontext von I4.0 nur wenige Neuentwicklungen aber viele Anpassungen der Maßnahmen, um dynamischen Wertschöpfungsprozessen standhalten zu können. Die meisten I4.0- Prozesse sind nicht neu für Unternehmen, nur die Intensität und die Menge der Aufgaben steigt an und stellt die erprobten organisatorischen Mittel auf eine Belastungsprobe.

Im Folgenden werden daher zunächst organisatorische und rechtliche Aspekte der Umsetzung von IT-Sicherheitsmaßnahmen im I4.0-Kontext im Allgemeinen diskutiert. Der Fokus liegt dabei auf der Beschreibung von erwarteten und im Hinblick auf Sicherheitsmaßnahmen relevanten Änderungen. Von Interesse sind dabei vor allem Änderungen im Hinblick auf die Anforderungen denen Sicherheitsmaßnahmen genügen müssen. Im Anschluss daran wird die Bedeutung der identifizierten Änderungen auf die heute im industriellen Kontext gebräuchlichen Sicherheitsmaßnahmen diskutiert.

In den Kapiteln 5.3 und 5.4 stehen organisatorische und rechtliche Hindernisse im Mittelpunkt, die bei der Umsetzung von grundsätzlich geeigneten Sicherheitsmaßnahmen eine Rolle spielen können. Die folgenden Ausführungen basieren auf einer Auswertung der in Kapitel 4.1 eingeführten Fallbeispiele, ergänzt um eine Literaturanalyse, die auch die aktuellen Studien der letzten fünf Jahre zu den Themen IT-Sicherheit und I4.0 beinhaltet, sofern dort auch explizit organisatorische oder rechtliche Aspekte adressiert wurden.

5.2.1 Organisatorische Umsetzungs- und Eignungsaspekte

Im Folgenden werden erwartete und im Hinblick auf IT-Sicherheitsmaßnahmen relevante organisatorische Veränderungen in der Industrie beschrieben. Von Interesse sind dabei vor allem Änderungen im Hinblick auf die Anforderungen denen Sicherheitsmaßnahmen genügen müssen. Im Kontext von I4.0 verändern sich die Anforderungen an organisatorische IT-Sicherheitsmaßnahmen in erster Linie durch Veränderungen bei der Bedrohungslage, die zum Teil auf sich ändernde organisatorische Strukturen und Prozesse zurückgeführt werden können.

Im Rahmen einer umfassenden Untersuchung im Projekt SecurePLUGandWORK[339] wurden vom Fraunhofer ISI im Jahr 2014 Publikationen über den aktuellen Verbreitungsgrad, das Erfolgspotenzial sowie die Chancen und Gefahren von I4.0 gesammelt und ausgewertet. Von insgesamt 125 Einzelpublikationen, die in einem ersten Schritt identifiziert wurden, verblieben 65 Beiträge mit Relevanz für das verarbeitende Gewerbe, die detailliert analysiert wurden. Hinsichtlich Erscheinungsjahr und Beitragstyp ergibt sich für diese Beiträge folgendes Bild: Die Mehrheit der Beiträge, 35 Beiträge, wurde im Jahr 2014 publiziert, 25 Beiträge im Jahr 2013 und je zwei Beiträge in den Jahren 2012 und 2011. Hinsicht-

337 Siehe LARS ICS: Ein Werkzeug für den leichtgewichtigen Einstieg in industrielle Cyber-Security, https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Tools/LarsICS/LarsICS.html, zuletzt abgerufen am 19.11.2015; Michael Gröne: LARS – Leichtgewichtiges Werkzeug zum Einstieg in IT-Sicherheit, 14. Deutscher IT-Sicherheitskongress, Bonn 2015.

338 Roßnagel, Alexander (2009): Mobilität und Kontext - Zukunftsentwicklung der mobilen Kommunikation in Recht und Technik. In: Schriftenreihe des Instituts für Europäisches Medienrecht (EMR) (Band 38) Roßnagel 2009, S. 15–20; Wildemann, Horst; Ann, Christoph; Broy, Manfred; Günthner, Willibald A.; Lindemann Udo (2007): Plagiatschutz: Handlungsspielräume der produzierenden Industrie gegen Produktpiraterie. 1. Aufl. TCW Transfer-Centrum. München. Wildemann et al. 2007, S. XII.

339 Das Projekt SecurePLUGandWORK (http://www.secureplugandwork.de) wird vom Bundesministerium für Bildung und Forschung (BMBF) gefördert und vom Projektträger Karlsruhe (PTKA) betreut (Förderkennzeichen 02PJ2590 ff).

lich des Beitragstyps wurden zwei Kategorien unterschieden: 20 Beiträge enthalten quantitativ-empirische Daten zum Themengebiet I4.0, 45 Beiträge beinhalten konzeptionelle Ausführungen und/oder Fallbeispiele. Die Kernergebnisse der Untersuchung zu organisatorischen Aspekten ergänzen im Folgenden – sofern thematisch passend – die Ausführungen.

Zunächst lassen sich Schadensfälle, deren Wahrscheinlichkeit und/oder Auswirkungen durch organisatorische IT-Sicherheitsmaßnahmen beeinflusst werden können, grob in zwei Hauptgruppen und je zwei Untergruppen einteilen: Die zwei Hauptgruppen von Schadensfällen werden gebildet in Abhängigkeit davon, ob (1) Handeln aus dem Kreis der Partner einer Kooperation oder (2) Handeln Dritter oder sonstige Ereignisse zu einem Schaden führt/führen. Bei Fällen der Fallgruppe (1) kann weiter unterschieden werden, ob der Schaden (1a) mit böser Absicht (Innentäter) oder (1b) ohne böse Absicht (menschliches Fehlverhalten) herbeigeführt wurde. Dem Kreise der Partner einer Kooperation wird in der Regel besonderes Vertrauen entgegengebracht. Handelnde können dabei sowohl Personen sein, die dem Unternehmen zugeordnet werden, bei dem ein Schaden aufgetreten ist, als auch Personen aus Unternehmen die mit dem geschädigten Unternehmen kooperieren. Bei Fällen der Fallgruppe (2) kann unterschieden werden ob der Schaden (2a) zielgerichtet oder nicht zielgerichtet durch Dritte herbeigeführt wurde (Außentäter) oder ob (2b) sonstige Ereignisse für den Schaden verantwortlich waren (z. B. höhere Gewalt oder technisches Fehlverhalten). Die Eignung und Wirkungsweise bestimmter Sicherheitsmaßnahmen zur Vermeidung eines Schadens hängt zu einem gewissen Grad von der jeweiligen Fallgruppe ab. Als organisatorische IT-Sicherheitsmaßnahmen werden in erster Linie Richtlinien und Verfahren, Methoden und Werkzeuge sowie Schulungen und Sensibilisierungsmaßnahmen verstanden[340]. Während technische Maßnahmen direkt mit den Systemen zusammenhängen, betreffen organisatorische Maßnahmen das Umfeld des Systems, Strukturen, Prozesse und insbesondere die Personen, die das System nutzen.

5.2.1.1 Organisatorische Sicherheitsmaßnahmen in bestehenden Normen und Richtlinien und deren Eignung

Im Folgenden wird die Bedeutung der identifizierten Änderungen, vor allem der Bedrohungen, für die heute im industriellen Kontext gebräuchlichen organisatorischen Sicherheitsmaßnahmen diskutiert. Dazu werden die in Standards und Leitfäden genannten Maßnahmen im Kontext der Fallbeispiele, der vom BSI identifizierten Bedrohungen und der eingeführten Fallgruppen diskutiert, um die grundsätzliche Eignung der Maßnahmen für die I4.0 zu ermitteln. Es wurden die bereits zu Beginn von Kapitel 5.1 genannten Standards und Leitfäden sowie die PROFINET-Security-Richtlinie[341] betrachtet. Darüber hinaus fließen die vom BSI im Rahmen der Aufstellung der Bedrohungsliste vorgeschlagenen organisatorischen Maßnahmen in die Diskussion mit ein.

Die in den Standards und Leitfäden genannten organisatorischen Sicherheitsmaßnahmen lassen sich wie erwartet drei Gruppen zuordnen: Richtlinien und Verfahren, Methoden und Werkzeuge sowie Schulungen und Sensibilisierungsmaßnahmen. Eine Reihe von Maßnahmen wird im Zusammenhang mit verschiedenen Bedrohungen genannt.

5.2.1.1.1 Richtlinien und Verfahren

Richtlinien und Verfahren zielen meist auf konkrete Bedrohungen ab und sind im Kontext von I4.0 genauso wie bei Fragen der IT-Sicherheit im Allgemeinen von großer Bedeutung. Aufgrund der Vielzahl an Richtlinien und Verfahren in Unternehmen kann hier nur exemplarisch auf einige eingegangen werden, die im Hinblick auf die identifizierten Bedrohungen für besonders relevant gehalten werden. Im Rahmen der Standards und Leitfäden wird neben der Bedeutung von Richtlinien und Verfahren zur Durchsetzung eines einheitlichen Vorgehens meist auch explizit die Bedeutung von Sanktionen bei Nichteinhaltung von Vorgaben hervorgehoben.

Im Zusammenhang mit menschlichem Fehlverhalten und Social Engineering ist die Erstellung und Durchsetzung von Richtlinien von besonderer Bedeutung. Explizit genannt werden vom BSI im CIP-Standard bzw. im Rahmen der PROFINET-Security-Richtlinie in diesem Zusammenhang

340 Hagen, J. M., Albrechtsen, E. and Hovden, J. 2008. "Implementation and effectiveness of organisational information security measures," Information Management & Computer Security (16:4), pp. 377–397.

341 PROFIBUS (2013): PROFINET-Security-Richtlinie (Version 2.0), http://www.profibus.com/nc/download/specifications-standards/downloads/profinet-security-guideline/display/

Richtlinien zur Klassifizierung von Dokumenten, zum Umgang mit technischen Systemen, zur Aufbewahrung und Vernichtung von Daten, zum Umgang mit Passwörtern und zur Entsorgung von Datenträgern sowie Verschwiegenheits- und Datenschutzerklärungen.

Im Zusammenhang mit der Bedrohung durch Einbrüche über Fernwartungszugänge wird beispielweise betont, dass Richtlinien die Freischaltung von Zugängen durch internes Personal nur für die Dauer und den Zweck der Wartung oder den Verzicht auf Funktionszugänge fordern sollten. Personalisierte Zugänge verlangt die VDI/VDE-Richtlinie 2182 im Rahmen ihrer Ausführungen über rollen- oder personenbezogene Berechtigungen.

Alle Hard- und Softwarezugänge sollten geschlossen oder gesichert werden. Im Zusammenhang mit der Infektion mit Schadsoftware über Wechseldatenträger und externe Hardware wird auf Richtlinien zur Regelung der Verwendung von Wechseldatenträgern verwiesen. Einerseits wird die ausschließliche Verwendung unternehmenseigener (personalisierter) Wechseldatenträger nahegelegt und andererseits die Vermeidung der Verwendung von Wechseldatenträgern sowohl im Produktionsnetz als auch in anderen Netzen.

Klar definierte Verfahren werden zum Beispiel für die Neueinstellung und das Ausscheiden von Mitarbeitern für erforderlich gehalten. Der CIP-Standard fordert beispielsweise, dass Personen mit Zugriff auf sensible Systeme oder Anlagen eine persönliche Risikobewertung bestehen müssen. Berücksichtigt werden sollte dabei auch der Umgang mit externen Mitarbeitern. Im Rahmen der PROFINET-Security-Richtlinie werden Verfahren für den Umgang mit Fremdpersonal wie beispielsweise Servicetechnikern und deren Zugriffe auf das Produktionsnetz explizit adressiert. Auch ISO/IEC 27001 stellt unter anderem ein Regelwerk zur Sicherheit beim Einsatz externer Mitarbeiter zur Verfügung.

In ähnlicher Art und Weise gestaltet sich die Situation bei der Anschaffung, Abnahme und Entsorgung von IT-Komponenten, Anlagen oder Systemen. Beispielsweise sollte dem BSI zufolge im Rahmen der Abnahme sichergestellt werden, dass Standardnutzer und -passwörter gesperrt wurden. Aber auch schon bei der Auswahl von IT-Komponenten, Anlagen oder Systemen sollte darauf geachtet werden, dass bestimmte Mindestanforderungen erfüllt sind. Während der Anbieter vertrauenswürdig und zertifiziert sein sollte, sollte das Produkt robust sein. Darüber hinaus sollten Sicherheitsmechanismen vorhanden und die langfristige Verfügbarkeit von Ersatzteilen und Updates, die zeitnahe Verfügbarkeit von Patches und offene Migrationspfade geben sein. In der VDI/VDE-Richtlinie 2182 wird explizit betont, dass möglichst in der Einsatzumgebung erprobte Hard- und Software genutzt werden sollte. Verfahren für die Entsorgung von Komponenten werden unter anderem im Rahmen der PROFINET-Security-Richtlinie angesprochen.

Empfehlung: Es zeigt sich, dass zwar alle untersuchten Normen und Standards auch organisatorische Aspekte beinhalten, jedoch kann keine klare Empfehlung in Richtung der Anwendung einer speziellen Norm gegeben werden, da die aktuellen Versionen entweder zu allgemein formuliert sind, um eine konkrete Maßnahme im Unternehmen anzustoßen oder aber nur einzelne organisatorische Aspekte berücksichtigen. Einen guten, wenn auch nicht explizit produktionsbezogenen Überblick liefert in organisatorischer Hinsicht der IT-Grundschutzkatalog des BSI.

Die Durchsetzung von Richtlinien und Verfahren in Unternehmen ist unabhängig von Konzepten wie I4.0 problematisch. Etablierte Maßnahmen zur Adressierung von Durchsetzungsproblemen sollten auch im I4.0-Kontext umgesetzt werden. In der Praxis sind im Hinblick auf die Spezifizierung von Richtlinien und Verfahren Grundlagen in Form von Best-Practices-Sammlungen, Leitfäden und Standards weit verbreitet. Diese eignen sich jedoch nicht uneingeschränkt für jedes Unternehmen und müssen konkretisiert bzw. angepasst werden. Haben die Grundlagen einen Fokus auf IT-Sicherheit im Allgemeinen, ist in der Regel zunächst eine Anpassung an den I4.0-Kontext erforderlich. Bei Grundlagen, die bereits auf I4.0 abzielen, ist häufig eine Anpassung an die betrieblichen Besonderheiten notwendig. Die Entscheidung für I4.0 ist deshalb zwangsläufig mit einer Anpassung der betrieblichen Richtlinien und Verfahren verbunden. Es ist durchaus denkbar, dass durch die zunehmende Automatisierung in Unternehmen bestimmte Richtlinien und Verfahren obsolet werden. Gleichzeitig ist allerdings auch nicht auszuschließen, dass die voranschreitende Vernetzung über Standort und Unternehmensgrenzen hinweg auch eine Erweiterung sowie eine engere Abstimmung von Richtlinien und Verfahren erforderlich macht.

5.2.1.1.2 Methoden und Werkzeuge

Methoden und Werkzeuge haben meist bedrohungsübergreifende Relevanz. Aus organisatorischer Sicht spielen sie bei der Gewährleistung eines an die betrieblichen Erfordernisse angemessenen IT-Sicherheitsniveaus eine wesentliche Rolle.

Das BSI schlägt zum Beispiel vor, die frei verfügbaren Informationen in Netzen zu beschränken um den Abfluss von Informationen zu verhindern[342]. Dieser Ansatz ist auch als „Need-to-Know"-Prinzip oder, wenn es um den Zugriff auf Information oder Systeme geht, als „Least-Privileges"-Prinzip bekannt. In ähnlicher Weise verweist ISO/IEC 27001 auf die Reduktion von Datenverarbeitung auf ein Minimum. Der Standard legt Datensparsamkeit nahe. Die Umsetzung dieses Prinzips führt im Hinblick auf viele der identifizierten Bedrohungen zu einer besseren Ausgangssituation. Vor allem im Hinblick auf kritische Prozesse im Produktionsnetz wird auf das „Vier-Augen"-Prinzip verwiesen. Es wird davon ausgegangen, dass dieser Ansatz die Bedrohung durch menschliches Fehlverhalten und Sabotage, zum Beispiel im Kontext von Maßnahmen zum Sicherheits- und Konfigurationsmanagement, reduziert. Im Rahmen der Normenreihe ISA/IEC 62443 wird die Bedeutung des „Defence-in-Depth"-Ansatzes im Kontext von Systemen zur Fertigungs- und Prozessautomatisierung hervorgehoben. Der Ansatz beschreibt ein Schutzkonzept mit mehreren Schichten technischer und organisatorischer Sicherheitsmaßnahmen. In vielen Fällen kann dem BSI zufolge auch eine Abwägung von Nutzen und Risiken sinnvoll sein. Explizit erwähnt werden solche Abwägungen im Zusammenhang mit der Notwendigkeit von Zugriffsmöglichkeiten auf Anlagen von Smartphones und Tablets. Auch wenn alle der exemplarisch angeführten Methoden unabhängig von der I4.0 für die IT-Sicherheit von Bedeutung und bereits lange bekannt sind, erscheint ihre Anwendung in der I4.0, aufgrund der dort gegebenen Komplexität und Dynamik, besonders wichtig.

Empfehlung: Einsatz und systematische Weiterentwicklung der bereits bekannten Konzepte.

Im Hinblick auf Werkzeuge ist die Dokumentation ein zentrales Thema im Kontext von IT-Sicherheit. Die Dokumentation bildet die Grundlage für die Risikoanalyse sowie für die Umsetzung von Sicherheitsmaßnahmen[343]. Dokumentiert werden sollten im I4.0-Kontext unter anderem die Netzwerkverkabelung, die auf Komponenten betriebenen Dienste und die Freigaben in Firewalls. Durch die I4.0 im Allgemeinen sowie durch betriebliche Besonderheiten ergeben sich spezielle Anforderungen an die Dokumentation.

Darüber hinaus wird die Überwachung von Logfiles vom BSI vorgeschlagen.[344] Um Angriffsversuche über Internet oder Intranet zu erkennen, kann beispielsweise nach ungewöhnlichen Verbindungen oder Verbindungsversuchen gesucht werden. Das kann vor allem dann wichtig sein, wenn Zugänge zur Fernwartung angeboten werden. Damit Logfiles ausgewertet werden können, müssen sie zunächst angelegt werden. Die VDI/VDE-Richtlinie 2182 fordert, dass jeder Verursacher von Veränderungen nicht abstreitbar, überprüfbar und rechtssicher authentifiziert und erfasst wird. Dies dient insbesondere zur Vermeidung von Sabotage. Die Bedeutung der Protokollierung von Änderungen bzw. Systemereignissen wird auch in ISO/IEC 27001 sowie in der PROFINET-Security-Richtlinie hervorgehoben. Auch hier sind Maßnahmen zur Sicherstellung der Rückverfolgbarkeit und Nachweisbarkeit vorgesehen. Alle Benutzeraktivitäten werden aufgezeichnet und für einen bestimmten Zeitraum gespeichert. Darüber hinaus kann auch die Durchführung von Audits unter bestimmten Voraussetzungen oder in bestimmten Bereichen empfehlenswert sein. Im Hinblick auf die I4.0 empfiehlt das BSI Audits beispielsweise für Fernwartungszugänge. Das Aufgabenfeld für Audits ändert sich durch I4.0 erheblich. Die Möglichkeiten im Hinblick auf die Durchführung von Audits unterscheiden sich stark in Abhängigkeit vom Know-how und den Ressourcen von Unternehmen. Zertifizierungen dürften insbesondere für KMUs trotz ihrer vertrauensfördernden Wirkung nicht uneingeschränkt praktikabel sein.

Empfehlung: Alle untersuchten Richtlinien und Standards enthalten ähnliche Forderungen zur Dokumentation, so dass hier keine explizite Empfehlung hinsichtlich einer Norm ausgesprochen wird.

Im Zusammenhang mit menschlichem Fehlverhalten, Sabotage und Social Engineering wird die Bedeutung der Etablierung von Alarmierungswegen bei Vorfällen und Verdachtsfällen hervorgehoben. Der Aufbau eines Notfallmanagements erscheint auch im Hinblick auf Bedrohungen durch technisches Fehlverhalten und höhere Gewalt sinnvoll. Der Aufbau eines Notfallmanagements umfasst die Entwicklung von Gegenmaßnahmen, die Festlegung von Verfahren zur Wiederherstellung, den Aufbau von alternativen Kommunikationswegen oder die Durchführung von Übungen. Auch im Hinblick auf eine Bedrohung durch DoS-Angriffe wird eine Notfallplanung für wesentlich gehalten.

342 BSI (2014): Industrial Control System Security – Top 10 Bedrohungen und Gegenmaßnahmen 2014.
343 BSI (2013): ICS-Security-Kompendium, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile
344 BSI (2014): Industrial Control System Security – Top 10 Bedrohungen und Gegenmaßnahmen 2014.

5.2.1.1.3 Schulungen und Sensibilisierungsmaßnahmen

Schulungen und Sensibilisierungsmaßnahmen sind insbesondere im Hinblick auf menschliches Fehlverhalten und Social Engineering von Interesse. Neben dem BSI heben auch der Standard ISO/IEC 27001, die Normenreihe ISA/IEC 62443, die PROFINET-Security-Richtlinie und der CIP-Standard die Bedeutung von Schulungen im Hinblick auf ein angemessenes Sicherheitsniveau hervor. Der CIP-Standard sieht beispielsweise die Absolvierung einer jährlichen Schulung für Mitarbeiter vor. Im Hinblick auf Sensibilisierungsmaßnahmen wird meist die Fokussierung auf bestimmte Zielgruppen für wichtig gehalten.

Viele der organisatorischen Sicherheitsmaßnahmen, die heute für das industrielle Umfeld empfohlen und dort umgesetzt sind, sind auch für die I4.0 geeignet. Die Gefahren, die von einer fehlenden oder mangelhaften Umsetzung der Maßnahmen ausgehen, sind im I4.0-Kontext allerdings deutlich größer.

5.2.2 Rechtliche Umsetzungsaspekte

Im nachfolgenden Abschnitt werden rechtliche Umsetzungsaspekte in Bezug auf Anforderungen an technische und organisatorische Gegebenheiten von IT-Sicherheitsmaßnahmen mit Blick auf die I4.0 näher erläutert.

5.2.2.1 Datenschutzrechtliche Umsetzungsaspekte

Da es, wie bereits mehrfach erläutert, zu zahlreichen Verarbeitungen und Nutzungen von personenbezogenen, insbesondere Beschäftigten- und Kundendaten im Rahmen der Verbreitung von I4.0 kommen dürfte, sind datenschutzrechtliche Normen bei der Umsetzung von grundsätzlicher Bedeutung. Datenschutzrechtliche Regularien beinhalten neben materiell-rechtlichen Anforderungen an die Verarbeitung oder Nutzung von personenbezogenen Daten auch Vorgaben zur Sicherstellung der Datensicherheit. Während das materielle Datenschutzrecht reguliert, ob und welche Daten zu welchen Zwecken auf welche Weise verarbeitet werden dürfen, konkretisieren die Regelungen zur Datensicherheit die Anforderungen an in dieser Hinsicht zu treffende flankierende technisch-organisatorische Maßnahmen. Diese müssen darauf abzielen, einen unzulässigen Umgang mit personenbezogenen Daten zu verhindern und die Integrität sowie Verfügbarkeit der Daten und die zu deren Verarbeitung eingesetzten technischen Einrichtungen zu erhalten.[345]

Die Schutzziele, die hinter der Datensicherheit im Sinne des Datenschutzrechts stehen, entsprechen dabei im Wesentlichen den bereits an anderer Stelle erwähnten[346] drei Schutzzielen des CIA-Dreiecks (Vertraulichkeit, Integrität, Verfügbarkeit), an die sich die IT-Sicherheit auch im Allgemeinen orientiert. Daher schlagen die datenschutzrechtlichen Anforderungen an IT-Sicherheit unmittelbar auf die allgemeinen IT-Sicherheitsanforderungen durch und umgekehrt. Entsprechend empfiehlt es sich, im Rahmen einer vorgelagerten Schutzbedarfsanalyse zu ermitteln, welche Anforderungsrahmen (allgemeines Schutzinteresse oder datenschutzrechtliche Vorgaben) den höheren Schutzbedarf begründen.[347] Diesem folgend wären die Maßnahmen entsprechend auszugestalten. Welche Maßnahmen unter datenschutzrechtlichen Aspekten geboten sind, wird sogleich unter Ziffer 5.2.2.1.1 näher erläutert.

5.2.2.1.1 Umsetzungsaspekte aus dem derzeit geltenden datenschutzrechtlichen Rechtsrahmen

Der derzeit geltende datenschutzrechtliche Rechtsrahmen, also insbesondere das Bundesdatenschutzgesetz, statuiert verschiedene Anforderungen an die Datensicherheit, die sich überwiegend in § 9 BDSG und dessen Anlage wiederfinden. Entsprechend ist etwa nach § 9 Satz 1 BDSG jede öffentliche oder nicht-öffentliche Stelle, die selbst oder im Auftrag personenbezogene Daten erhebt, verarbeitet oder nutzt, verpflichtet, technisch-organisatorische Maßnahmen zu treffen, die erforderlich sind, um die Ausführung des Bundesdatenschutzgesetzes, insbesondere die in der Anlage zu § 9 Satz 1 BDSG genannten Anforderungen, zu gewährleisten. Der Terminus der technischen und organisatorischen Maßnahmen zielt dabei nicht auf eine Differenzierung von technischen gegenüber organisatorischen Maßnahmen ab, vielmehr ist diese rechtlich nicht relevant, so dass die Begriffe auch nicht klar voneinander abgegrenzt werden.[348]

345 Simitis/Ernestus, BDSG, § 9 Rn. 2.
346 Siehe dazu oben 4.2.2.6.
347 Behling/Abel/Brauner/Mickler und Alsbih, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 3 Rn. 67 sowie Kap. 12 Rn. 31ff.
348 Simitis/Ernestus, BDSG, § 9 Rn. 2.

Die durch das Bundesdatenschutzgesetz angeordneten Maßnahmen sind insgesamt abstrakt gehalten und definieren gerade keinen abschließenden Katalog an Einzelmaßnahmen.[349] Vielmehr werden Kontrollziele in der Anlage zu § 9 BDSG festgelegt sowie die Tatsache, dass insoweit „erforderliche" Maßnahmen zu treffen sind. § 9 Satz 2 BDSG wiederum normiert, dass Maßnahmen nur erforderlich sind, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Welche Maßnahmen daher im Einzelfall erforderlich sind, orientiert sich am Grundsatz der Verhältnismäßigkeit.[350] Dieser erfordert eine Abwägung widerstreitender Faktoren, wie einerseits der Sensibilität der jeweils verarbeiteten Daten, etwaige bestehende Risiken sowie Folgen für den Betroffenen und andererseits der Aufwand, der mit spezifischen technischen und organisatorischen Maßnahmen für das einzelne Unternehmen verbunden ist.[351] Gerade hierin zeigt sich der gedankliche Unterschied zwischen datenschutzrechtlicher Datensicherheit und IT-Sicherheit im Übrigen. Während bei nicht-personenbezogenen Daten geschäftliche Risiken Anknüpfungspunkt für die Verhältnismäßigkeitsabwägung darstellen, müssen im Falle personenbezogener Daten zusätzlich die Folgen für die Personen, auf die sich die Daten beziehen, als maßgeblicher Anknüpfungspunkt einbezogen werden.[352] Durch diese Verhältnismäßigkeitsprüfung soll – umgangssprachlich gesprochen - sichergestellt werden, dass „nicht mit Kanonen auf Spatzen geschossen wird".[353]

Die Anlage zu § 9 Satz 1 BDSG normiert also gewisse Mindeststandards, die keinen abschließenden Kriterienkatalog darstellen und als die sog. neun Gebote der Datensicherheit bezeichnet werden, die sich in der Anlage zu § 9 Satz 1 BDSG entsprechend wiederfinden.[354, 355] Dies sind die Folgenden:

1. Die **Organisationskontrolle**, die die Implementierung einer hinreichenden, auf die besonderen Anforderungen des Datenschutzes ausgerichteten Aufbau- und Ablauforganisation im Unternehmen voraussetzt.[356]

Diese Kontrolle regelt übergreifende Maßnahmen, die für **alle drei Schutzziele (Vertraulichkeit, Verfügbarkeit und Integrität)** bedeutsam sind. Sie soll dabei einerseits einem geregelten Verfahren und einer ausreichenden Konzeption zur Datensicherheit dienen und sicherstellen, dass personenbezogene Daten nur im Rahmen des datenschutzrechtlich Zulässigen gehandhabt werden.

Die Organisationskontrolle betrifft nicht nur die Fachabteilungen oder das Rechenzentrum, sondern sämtliche Bereiche, die mit personenbezogenen Daten in Berührung kommen können, also etwa auch den Bereich der Anwendungsentwicklung.[357] Im Rahmen der Organisationskontrolle sind unterschiedliche Maßnahmen denkbar[358], wobei die Wesentlichen nachfolgend kurz skizziert werden sollen.

Die Maßnahmen zur Organisationskontrolle haben insbesondere im Rahmen von I4.0 eine besondere Bedeutung, da hier eine vorausschauende und fortlaufende Sicherheitsorganisation erforderlich ist, die sich zudem auf Szenarien erstreckt, die über ein einzelnes Unternehmen hinausgehen. Hierzu zählt es auch, dass ein **IT-Sicherheitskonzept** zu entwickeln ist. Erst durch eine Gesamtanalyse lassen sich anhand der dabei festzustellenden Bedrohungs- und Risikoszenarien die weiteren technisch-organisatorischen Maßnahmen im Einzelnen bestimmen. Für übergreifende Themen enthält das in dieser Studie entwickelten Referenzmodell[359] Orientierungspunkte für das Vorgehen bei einer entsprechenden Analyse. Bei der Klassifizierung von Daten[360] ist dabei ein besonderes Augenmerk auf besondere Arten personenbezogener Daten nach § 3 Abs. 9 BDSG (Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) sowie personenbezogene Daten, die einem Berufsgeheimnis unterliegen, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den

349 Gola/Schomerus/Gola/Klug/Körffer, BDSG, §9 Rn. 2.
350 Gola/Schomerus/Gola/Klug/Körffer, BDSG, § 9 Rn. 7.
351 Gola/Schomerus/Gola/Klug/Körffer, BDSG, § 9 Rn. 9.
352 Gola/Schomerus/Gola/Klug/Körffer, BDSG, § 9 Rn. 9.
353 Gola/Schomerus/Gola/Klug/Körffer, BDSG, § 9 Rn. 7.
354 Münchener Anwaltshandbuch IT-Recht/Scheja/Haag, Teil 5E. XII, Rn. 254.
355 Münchener Anwaltshandbuch IT-Recht/Scheja/Haag, Teil 5E. XII, Rn. 254.
356 Behling/Abel/Behling, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 1 Rn. 9f.
357 Täger/Gabel/Schultze-Melling, BDSG, 2. Auflage 2013, § 9 Rn. 44.
358 Vgl. mit weiteren Bespielen Täger/Gabel/ Schultze-Melling, BDSG, 2. Auflage 2013, § 9 Rn. 48.
359 Siehe dazu oben 4.2.
360 Siehe dazu oben 4.2.2.9.

Verdacht auf solche beziehen und Bank- oder Kreditkarten zu legen, die unter anderem aufgrund der Meldepflichten nach § 42a BDSG als besonders sensibel zu betrachten sind. Praktische Relevanz dürften bei I4.0 indes allenfalls die besonderen Arten von personenbezogenen Daten haben und ggfs. noch Bank- sowie Kreditkartendaten.

In Bezug auf personenbezogene Daten, die von I4.0 betroffen sind, sollten überdies **Privacy Impact Assessments (PIAs)** durchgeführt werden, die die spezifischen Risiken für das Persönlichkeitsrecht der Betroffenen (Beschäftigte und/oder menschliche Kunden) identifizieren und daher Teil der Gesamtschutzbedarfsanalyse sind. Gerade wenn sich hierbei besondere Risiken ergeben, ist zudem eine **datenschutzrechtliche Vorabkontrolle** durch den betrieblichen Datenschutzbeauftragten geboten (§ 4d Abs. 5 BDSG). Verfahren zur Verarbeitung personenbezogener Daten sind überdies in einem **Verfahrensverzeichnis** zu dokumentieren (§§ 4g Abs. 2 S., 4e Satz 1 BDSG). Ferner sollte ein **Lösch- und Sperrkonzept** für personenbezogene Daten entwickelt werden, um die gesetzlichen Lösch- und Sperrpflichten rechtskonform umsetzen zu können. Die Möglichkeit zur Löschung und Sperrung personenbezogener Daten sollte dabei bereits während der Planungsphase systemseitig sichergestellt werden.

Zur Organisationskontrolle zählen auch **Schulungen und Sensibilisierungsmaßnahmen** gegenüber Mitarbeitern in Sachen Datenschutz.[361] Neben Schulungen sind überdies **Datenschutz-Richtlinien und -Anweisungen** für Mitarbeiter ein Mittel der Organisationskontrolle.

I.d.R. sind weitere datenschutzspezifische Organisationsmaßnahmen erforderlich. So entstehen besondere datenschutzrechtliche Risiken für Unternehmen etwa bei unterbliebenen oder nicht rechtzeitig durchgeführten Meldepflichten, falls spezifische Daten abhandenkommen, also insbesondere „gestohlen" werden (s. § 42a BDSG). Daher sollten auch **Verhaltensregeln** für den Fall von **Datenschutzvorfällen** festgelegt werden. Zudem sind alle Mitarbeiter nach § 5 BDSG auf das **Datengeheimnis zu verpflichten**.

2. Die **Zutrittskontrolle** erfordert Maßnahmen zur Verwehrung des Zutritts von Unbefugten zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden.

   Diese Kontrolle zielt primär auf das **Schutzziel der Vertraulichkeit** ab, d.h. insbesondere der Verhinderung, dass Unbefugte (hier: räumlich) die Möglichkeiten zur Kenntnisnahme von personenbezogenen Daten erhalten. Maßnahmen der Zutrittskontrolle sind etwa:[362] Kontrolle der Eingänge durch **Wachpersonal** und **Empfang**, **Schlüsselregelungen** und -vergabekonzepte zum Gebäudezutritt oder zu **verschiedenen Bereichen** (z.B. auch elektronische Schlüssel, wie Token), Führen eines **Besucherbuches**, **Begleitung von Besuchern** durch Mitarbeiter, Einrichtung einer Videoüberwachung sowie von Bewegungsmeldern. Dabei sollten zur Abwehr auch interner Angriffe – soweit erforderlich – unterschiedliche und durch entsprechende Schlüsselfunktionen abgesicherte Zutrittsberechtigungen von Mitarbeitern für unterschiedliche Bereiche differenziert werden. Insbesondere die Maßnahmen der Zutrittskontrolle wird ein Unternehmen regelmäßig nur in Bezug auf seine eigenen Betriebs- und Geschäftsräume sicherstellen können. Umso wichtiger ist es, dass entsprechende Maßnahmen auch bei den jeweiligen Partnerunternehmen etabliert sind und ein Unternehmen auf die Angemessenheit dieser Maßnahmen durch entsprechende Kontrollen vertrauen kann.

3. Mit Maßnahmen zur **Zugangskontrolle** ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

   Auch diese Maßnahme dient primär dem **Schutzziel der Vertraulichkeit**. Während die Zutrittskontrolle die räumliche Kenntnisnahmemöglichkeit betrifft, reguliert die Zugangskontrolle die tatsächliche Benutzung von Datenverarbeitungssystemen.[363] Hierzu kommen regelmäßig folgende Maßnahmen in Betracht: **Passwortverfahren** (inkl. Mindeslänge, Erneuerungsintervalle, Zugangssperre bei drei Fehlversuchen), **Bildschirmsperren** bei Verlassen des Raumes, **Zugangsprotokollierungen**, **Firewalls**[364], Anwendung des Vier-Augen-Prinzips bei Systemadministratoren, **Protokollierung und regelmäßige Kontrolle der Admin-Aktivitäten**.

361 Siehe dazu oben 5.2.1.1.3.
362 Täger/Gabel/Schultze-Melling, BDSG, 2. Auflage 2013, § 9 Rn. 53.
363 Täger/Gabel/Schultze-Melling, BDSG, 2. Auflage 2013, § 9 Rn. 54.
364 Vgl. hierzu auch das Beispiel aus der Automobilindustrie, dazu oben 4.1.1.2, und der Chemie-Industrie, dazu oben 4.1.3.2.

4. Die **Zugriffskontrolle** erfordert Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

   Die Zugriffskontrolle betrifft neben dem **Schutzziel der Vertraulichkeit** insbesondere auch die **Integrität und Verfügbarkeit** der Daten. Maßnahmen hierzu können etwa sein:[365] Ein **differenzierendes Rollen- und Berechtigungskonzept**[366], **User Identification Management** System, **Datenträgerverwaltungskonzept**[367] (Datenträger-Inventar, Ein- und Ausgangsverzeichnis, Festlegung von Befugten, Abgrenzung von Bereichen, in denen Datenträger verwendet werden dürfen etc.), ggf. **Sperrung von Schnittstellen**, z. B. von USB-Ports, **Richtlinien zur Datenträgervernichtung/-entsorgung**, ggf. Taschenverbot oder -kontrollen (sofern im Einzelfall verhältnismäßig).

5. Die **Weitergabekontrolle** setzt Maßnahmen voraus, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

   Die Weitergabekontrolle betrifft u. a. das **Schutzziel der Vertraulichkeit**. Als Maßnahmen können in Betracht kommen:[368] Verwendung **verschlossener Transportbehälter** bei Datenträgern Identitäts- und **Berechtigungsprüfung der Empfänger, Fernwartungskontrollen**[369] (z. B. in Zusammenhang mit Routern oder Gateways), verschlüsselte Verbindungen und ggf. Verschlüsselung der Daten selbst.

6. Maßnahmen zur **Eingabekontrolle** müssen gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

   Die Eingabekontrolle dient allen drei **Schutzzielen (Vertraulichkeit, Verfügbarkeit und Integrität)**. Als konkrete Maßnahmen sind insbesondere die **Protokollierung der Eingaben** (Erstellen, Verändern und/oder Löschen) und die Auswertung der Protokolle denkbar.[370] Dies setzt voraus, dass entsprechende Protokollierungsmöglichkeiten system- und anwendungsseitig überhaupt bestehen[371], was bei der Auswahl und Ausgestaltung von Systemen und Anwendungen im Kontext von I4.0 entsprechend zu berücksichtigen ist.

7. Im Rahmen der **Auftragskontrolle** sind Maßnahmen zu treffen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

   Die Auftragskontrolle soll dabei insbesondere sicherstellen, dass Auftragnehmer, die ein oder mehrere Partner im Rahmen von I4.0 einsetzen (z. B. Fernwartungsdienstleister), personenbezogene Daten nur im Rahmen der Weisungen verarbeiten, die das oder die auftragserteilenden Unternehmen in der Verarbeitungskette von I4.0 erteilt haben. Diese dient damit ebenfalls allen **drei Schutzzielen (Vertraulichkeit, Verfügbarkeit und Integrität)**, wobei hierunter z. B. folgende Maßnahmen fallen können:[372] Etablierung von Kriterien und Verfahren zur **sorgfältigen Auswahl des Auftragnehmers** (z. B. anhand wichtiger **Zertifizierungen oder Gütesiegel**), detaillierte **schriftliche Regelungen** und **Formalisierung des Auftragsablaufs**, einschließlich. eindeutiger **Abgrenzung von Zuständigkeiten und Verantwortlichkeiten**.

365 Täger/Gabel/Schultze-Melling, BDSG, 2. Auflage 2013, § 9 Rn. 62.
366 Siehe dazu oben 4.2.2.8.
367 Siehe zu den Risiken bei Verwendung von Datenträgers insbesondere oben 4.3.
368 Täger/Gabel/Schultze-Melling, BDSG, 2. Auflage 2013, § 9 Rn. 68.
369 Siehe dazu auch das Fallbeispiel aus dem Maschinenbau oben 4.1.2.2; zu den Risiken bei der Fernwartung siehe insbesondere oben 4.3 im Allgemeinen und 4.5.5.4f im Besonderen; zur Umsetzung im Rahmen der I4.0 siehe oben 5.1.2.
370 Täger/Gabel/Schultze-Melling, BDSG, 2. Auflage 2013, § 9 Rn. 72.
371 Siehe zu den Implementierungsschwierigkeiten oben 5.1.7.
372 Täger/Gabel/Schultze-Melling, BDSG, 2. Auflage 2013, § 9 Rn. 77.

8. Mit der **Verfügbarkeitskontrolle** ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

   Diese entspricht dem **Schutzziel der Verfügbarkeit**. Der Verlust von personenbezogenen Daten ist besonders gravierend, wenn der Betroffene oder die Aufsichtsbehörde um Auskunft zu Daten bittet, um die Rechtmäßigkeit einer bereits stattgefundenen Verarbeitung zu überprüfen. Aber auch im Allgemeinen kann die fehlende Verfügbarkeit relevanter personenbezogener Daten negative Folgen für die Betroffenen haben, was auch in § 35 Abs. 3 Nr. 2 BDSG zum Ausdruck kommt (keine Löschung, wenn schutzwürdige Interessen des Betroffenen entgegenstehen). Folge kann sein, dass auch bei einem Teilverlust an Daten im Einzelfall die Rechtmäßigkeit der Weiterverarbeitung der übrigen Daten in Frage gestellt werden könnte. Auch eine datenschutzrechtlich gebotene, aber nicht durchgeführte oder nicht rechtzeitig erfolgte Übermittlung von Daten kann schwere Folgen für Betroffene haben. Mögliche Maßnahmen der Verfügbarkeitskontrolle sind: **Unterbrechungsfreie Stromversorgung**, insbesondere der Server in den Rechenzentren, **Brandschutz- und Wasserschutzeinrichtungen**, **regelmäßige Back-ups** an einen **räumlich getrennten Ort**, **Notfallplan** (Wiederanlaufplan).

9. Die **Trennungskontrolle** gebietet Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Im Rahmen der Strukturen der I4.0 ist dabei insbesondere von Bedeutung, dass u. U. Daten von oder an unterschiedliche Partner zu unterschiedlichen Zwecken übermittelt werden, was durch eine hinreichende Trennung der Verarbeitungsvorgänge sicherzustellen ist, soweit personenbezogene Daten betroffen sind.

   Diese Kontrolle betrifft die Einhaltung des materiell-datenschutzrechtlichen Gebots der Zweckbindung auf technisch-organisatorischer Ebene.[373] Daneben kann sie auch dem **Schutzziel der Vertraulichkeit** dienen. Als Maßnahmen sind insbesondere zu erwägen:[374] **Physische oder logische Mandantentrennung**, **unterschiedliche Verschlüsselung** von Datensätzen je nach Zweck, Rollenkonzept (Administratoren, Revisoren, Benutzer), Verwendung **unterschiedlicher Attributs-Signaturen**.

Die aufgezeigten Kontrollen müssen sich, wie bereits erläutert, durch konkret umgesetzte Maßnahmen im Unternehmen widerspiegeln. Welche Maßnahmen hierbei im Einzelnen in Betracht kommen, wurde exemplarisch aufgezeigt.

In rechtlicher Hinsicht ist bei der Bestimmung der Maßnahmen nicht nur die Abwägung mit dem Schutzzweck sowie der Sensibilität der Daten vorzunehmen, sondern auch der Stand der Technik zu berücksichtigen.[375] Gleichwohl besteht eine wesentliche Herausforderung darin, dass mit fortschreitender technischer Entwicklung neue Risiken entstehen können, die bei der ursprünglichen Abwägung, mithin bei Entwicklung eines Verarbeitungsverfahrens nicht berücksichtigt werden konnten. Zugleich kann sich im Rahmen weiterer Entwicklungen auch der Aufwand für bestimmte präferierte technische und organisatorische Maßnahmen verringern und mithin zu einem späteren Zeitpunkt als angemessen darstellen. Entsprechend sind die technischen und organisatorischen Maßnahmen in regelmäßigen Abständen zu überprüfen und veränderten Umständen durch entsprechende Modifikationen der Maßnahmen Rechnung zu tragen.[376] Das Bundesdatenschutzgesetz verzichtet insoweit bewusst auf eine statische Regelung spezifischer technischer und organisatorischer Maßnahmen.[377] Die dynamische Regelung trägt einerseits dem Fortschritt der Technik Rechnung, ist jedoch andererseits mit einer gewissen Rechtsunsicherheit verbunden, sodass die Erfüllung der Anforderungen in der Praxis erfahrungsgemäß stets nur in enger Zusammenarbeit zwischen den jeweiligen für die (technische) Datensicherheit Verantwortlichen (bspw. CISO, CIO) sowie den für den Datenschutz Verantwortlichen (bspw. Datenschutzbeauftragter) in Unternehmen entwickelt werden kann.

Im Rahmen von I4.0 ist die Implementierung angemessener technischer und organisatorischer Maßnahmen insoweit mit besonderen Herausforderungen verbunden, als Daten in immer größeren Mengen in unterschiedlichen und sich verändernden technischen Systemen sowie Anwendungen verarbeitet und genutzt werden, sodass auch die Festlegung und regelmäßige Revision der techni-

373 Täger/Gabel/Schultze-Melling, BDSG, 2. Auflage 2013, § 9 Rn. 84.
374 Simitis/Ernestus, BDSG, § 9 Rn. 163.
375 Hierzu insgesamt BeckOK DatenSR/Karg, BDSG, § 9 Rn. 67.
376 Zu dem Vorstehenden insgesamt: BeckOK DatenSR/Karg, BDSG, § 9 Rn. 85.
377 Vgl. BeckOK DatenSR/Karg, BDSG, § 9 Rn. 70 f.

schen und organisatorischen Maßnahmen mit einem Aufwand verbunden sein dürften, der das bislang erforderliche Maß bei weitem übersteigt.

Zudem kann die jeweils verantwortliche Stelle, mithin das jeweilige Partnerunternehmen (juristische Person)[378] in der Produktionskette von I4.0, zunächst nur technisch-organisatorische Maßnahmen implementieren und kontrollieren, die sich auf ihre eigenen Datenverarbeitungen und -nutzungen beziehen. Soweit Daten innerhalb einer Produktionskette an eine andere verantwortliche Stelle, also an ein anderes Unternehmen, gelangen, besteht die Gefahr, dass diese andere oder gar weniger angemessene technische und organisatorische Maßnahmen getroffen hat, wodurch die von der einen Stelle implementierten Sicherheitsstandards unterlaufen werden könnten. Verbietet etwa die eine Stelle die Verwendung von externen Datenträgern wie USB-Sticks in ihrem eigenen Betrieb, sieht eine andere Stelle aber nur die Protokollierung der Verwendung externer Datenträger vor, so sinkt das Niveau der Datensicherheit auf das geringere Niveau, also in dem Beispielsfall auf die Protokollierung der Verwendung externer Datenträger. Dies kann im Beispielsfall das Schutzziel der Integrität beeinträchtigen. Aber auch die Schutzziele der Verfügbarkeit und Vertraulichkeit können gefährdet sein, wenn Daten in der Produktionskette ohne vorherige Festlegung und Überprüfung geeigneter technisch-organisatorischer Maßnahmen aus der Hand gegeben werden. Bei der Umsetzung ist daher zu beachten, dass die verschiedenen Akteure in Bezug auf die Umsetzung von Datensicherheitsaspekten eine einheitliche Strategie verfolgen, was umfangreiche, i. d. R. multilaterale Vereinbarungen zu Datenschutz und Datensicherheit voraussetzt. Solche Vereinbarungen sind zwar auch schon heute häufig erforderlich, wenn z. B. Auftragsdatenverarbeitungsverträge nach § 11 BDSG oder EU-Standardverträge zur Sicherstellung eines angemessenen Datenschutzniveaus nach §§ 4b, 4c BDSG geschlossen werden müssen, diese haben aber häufig keine so komplexe, weil vielschichtige Datenverarbeitungen unter Beteiligung sehr vieler Beteiligter abzubilden. Insgesamt fehlt es bislang noch an tauglichen Vertragsmustern und -vorgaben, die die komplexe Verarbeitungssituation bei I4.0 hinreichend abbilden.

5.2.2.1.2 Umsetzungsaspekte unter der EU-Datenschutzgrundverordnung

Wie bereits erläutert, sollen die nationalen Datenschutzgesetze durch eine unmittelbar anwendbare EU-Datenschutzgrundverordnung abgelöst werden, die abweichende anderslautende nationale Gesetze verdrängen soll, um eine weitgehende Einheitlichkeit des europäischen Datenschutzes zu gewährleisten.

Insoweit normieren Artikel 23 (Datenschutz durch Technik und datenschutzrechtliche Voreinstellungen) sowie Artikel 30 (Sicherheit der Verarbeitung) des Entwurfs einer EU-Datenschutzgrundverordnung (DS-GVO-E), dass der für die Verarbeitung Verantwortliche (und ggf. Auftragsdatenverarbeiter) unter Berücksichtigung des Stands der Technik und der Implementierungskosten technisch-organisatorische Maßnahmen zu treffen hat, die geeignet sind, ein Schutzniveau zu gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist. Dabei statuiert Artikel 23 des DS-GVO-E, dass der für die Verarbeitung Verantwortliche unter Berücksichtigung dieser Maßstäbe sowohl zum Zeitpunkt der Festlegung der Verarbeitungsmittel als auch zum Zeitpunkt der Verarbeitung technische und organisatorische Maßnahmen und Verfahren durchführt, durch die sichergestellt wird, dass die Verarbeitung den Anforderungen dieser Verordnung genügt und die Rechte der Betroffenen gewahrt werden. Die verantwortliche Stelle hat ihre technisch-organisatorischen Maßnahmen daher auch nach dem DS-GVO-E mithin ebenfalls nicht nur einmalig sondern fortlaufend dahingehen zu überprüfen, ob sie zur Wahrung der Datensicherheit geeignet sind.

Artikel 30 Abs. 2 des DS-GVO-E normiert zudem, dass der für die Verarbeitung Verantwortliche und ein (etwaiger) Auftragsdatenverarbeiter im Anschluss an eine Risikobewertung die technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten vor unbeabsichtigter oder widerrechtlicher Zerstörung oder vor unbeabsichtigtem Verlust sowie zur Vermeidung jedweder unrechtmäßigen Verarbeitung, insbesondere jeder unbefugten Offenlegung, Verbreitung beziehungsweise Einsichtnahme oder Veränderung treffen muss.

Nicht alle der im derzeit geltenden Bundesdatenschutzgesetz konkretisierten neun Gebote der Datensicherheit werden mithin in diesem Art. 30 DS-GVO-E ausdrücklich

378 Vgl. hierzu Gola/Schomerus/Klug/Gola/Körffer BDSG § 3 Rn. 48.

erwähnt, gleichwohl dürften die nicht benannten Gebote unter die Generalklausel „sowie zur Vermeidung jedweder unrechtmäßigen Verarbeitung“ fallen. Neu ist insbesondere der in Art. 30 Abs. 1 DS-GVO-E, enthaltene ausdrückliche Verweis auf eine vorhergehende Risikobewertung im Sinne einer Datenschutzfolgenabschätzung nach Art. 33 DS-GVO-E, die zwar praktisch bereits teilweise heute wohl schon durchgeführt wird, hier aber nun eine gesetzliche Normierung gefunden hat.

Die DS-GVO-E enthält sowohl in Artikel 23 als auch in Artikel 30 eine Ermächtigungsklausel für die Europäische Kommission, delegierende Rechtsakte zu erlassen. Entsprechend könnten die Anforderungen an angemessene technisch-organisatorische Maßnahmen durch die Kommission konkretisiert und vorgegeben werden. Hierdurch würde ein einheitlicher Rahmen für Standards getroffen, der EU-weit und – soweit im Einzelfall anwendbar – in Drittstaaten Anwendung finden würde. Hierdurch wäre die Möglichkeit der Herausbildung und rechtlichen Anerkennung internationaler Standards zur Datensicherheit im Bereich des Datenschutzes geschaffen. Allerdings bleibt abzuwarten, ob die Möglichkeit delegierender Rechtsakte der Kommission, wie er im Kommissionsentwurf vorgesehen ist, tatsächlich in dieser Form erlassen werden wird, da die Mitgliedsstaaten derartigen Ermächtigungsklauseln zugunsten der Kommission generell kritisch gegenüberstehen.[379] Zudem verfügt die Kommission anders als die Datenschutzaufsichtsbehörden wohl nicht über die grundsätzlich gebotene (politische) Unabhängigkeit für den Bereich der Datenschutzaufsicht. Vorzugswürdig wäre daher nach hiesiger Auffassung eine entsprechende Ermächtigung zugunsten des in der Verordnung vorgesehenen Europäischen Datenschutzausschusses, der sich aus Vertretern der nationalen Datenschutzaufsichtsbehörden zusammensetzen soll[380] und damit auch über die notwendige Unabhängigkeit verfügen dürfte. Für die Ermöglichung einheitlicher Standards wäre allerdings erforderlich, dass der Ausschuss auch tatsächlich verbindliche Entscheidungen treffen kann und nicht nur wie derzeit im Entwurf enthalten „Leitlinien, Empfehlungen und bewährte Praktiken“ vorgibt.[381]

Der DS-GVO-E sieht für bestimmte Fallkonstellationen auch eine unmittelbare Anwendung für verantwortliche Stellen in Drittstaaten vor, etwa wenn diese Betroffenen Produkte und Dienstleistungen auf dem europäischen Markt anbieten.[382] Jedoch dürfte im Rahmen der Anwendungen der I4.0 dies eher die Ausnahme sein, da die einzelnen Datenverarbeitungen der einzelnen Kooperationspartner in der Regel nicht unmittelbar das Angebot von Produkten oder Dienstleistungen gegenüber Betroffenen in Europa bezwecken dürfte.

Insgesamt bleibt die Herausforderung der Umsetzung des Schutzstandards über Unternehmens- und Ländergrenzen hinwegdaher auch nach Inkrafttreten des derzeitigen DS-GVO-E bestehen, sodass sich der Frage der vertraglichen Abbildung im multilateralen Umfeld von I4.0 nach jetzigem Stand weiterhin stellen wird.

5.2.2.2 Exportkontrollrechtliche Umsetzungsaspekte

Aspekte der Datensicherheit können im Rahmen des deutschen Exportkontrollrechts bereits bei der Feststellung einer etwaigen exportkontrollrechtlichen Genehmigungspflichtigkeit auftreten.[383] Denn die Genehmigungspflicht kann bereits bei der bloßen Möglichkeit eines Zugriffs aus einem Drittstaat auf exportkontrollrechtlich relevante Software oder Technologien ausgelöst werden.[384] Dies kann der Fall sein, wenn beispielsweise exportkontrollrechtlich relevante Software oder Technologie im firmeneigenen Intranet oder im Internet bereitgestellt wird.[385] Daher lässt sich nicht ausschließen, dass im Rahmen von Produktionsprozessen bei I4.0 sicherzustellen ist, dass Zugriffsmöglichkeiten auf exportkontrollrechtlich relevante Software oder Technologien durch entsprechende Maßnahmen derart eingeschränkt sind, dass ein Zugriff aus einem Drittstaat heraus de facto nicht mehr möglich ist, um eine entsprechende Genehmigungspflicht ggfs. entfallen zu lassen. Dies setzt naturgemäß einen erheblichen Aufwand voraus und ist selbst dann in aller Regel ohne behördliche Stellungnahme nicht mit der gewünschten Rechtssicherheit verbunden.

379 So auch eine Forderung des Unabhängigen Landeszentrums für Datenschutz in Schleswig-Holstein (ULD), 34. Tätigkeitsbericht, Kapitel 2, Nr. 2.5, abrufbar unter: https://datenschutzzentrum.de/tb/tb34/kap02.html
380 Erwägungsgrund 110 DS-GVO-E.
381 Bspw. Art. 20 Abs. 5a, Art. 9 Ziff. 3, Art. 31 Ziff. 5 DS-GVO-E.
382 Vgl. Art. 3 Ziff. 2a DS-GVO-E.
383 Vgl. Wermelt/Tervooren, CCZ 2013, 81 (83f.).
384 Bundesamt für Wirtschaft und Ausfuhrkontrolle, Kurzdarstellung Exportkontrolle, C.I., 10, 11.
385 Bundesamt für Wirtschaft und Ausfuhrkontrolle, Kurzdarstellung Exportkontrolle, C.I., 7.

Zudem ist zu beachten, dass Exportgenehmigungen nur zu erteilen sind, wenn der Ausführer hinsichtlich der einzuhaltenden exportrechtlichen Bestimmungen die notwendige Zuverlässigkeit besitzt.[386] Um die Anforderungen an die Zuverlässigkeit zu erfüllen, kann der Ausführer verpflichtet sein, entsprechende organisatorische Maßnahmen zu ergreifen. Dabei sind insbesondere die veröffentlichten Grundsätze der Bundesregierung zur Prüfung der Zuverlässigkeit von Exporteuren von Kriegswaffen und rüstungsrelevanten Gütern zu beachten.[387] Danach muss der Ausführer ein innerbetriebliches Exportkontrollsystem implementieren, das durch eine geeignete Aufbau- und Ablauforganisation sicherstellt, dass alle Verbote, Genehmigungs- und sonstige Pflichten eingehalten werden.[388]

Ferner hat das Bundesamt für Wirtschaft und Ausfuhrkontrolle ein Merkblatt („Internal Compliance Programmes") herausgegeben, das die Ausgestaltung innerbetrieblicher Exportkontrollen betrifft und auch technische Mittel umfasst.[389] Diese empfiehlt es sich bei I4.0 daher zu beachten.

Dies gilt umso mehr, als die innerbetrieblichen Exportkontrollsysteme vom Bundesamt für Wirtschaft und Ausfuhrkontrolle in bestimmten Fallgruppen von Amts wegen geprüft werden.[390]

Vor diesem Hintergrund dürften gerade bei I4.0 Prozesse zu implementieren sein, die darauf ausgerichtet sind zu prüfen, ob in Ansehung von Gut und Bestimmungsland eine exportrechtliche Genehmigungsfreiheit, Genehmigungspflicht oder Hinweispflicht besteht und entsprechende Klassifizierungen und Kennzeichnungen durchzuführen sind. Dies nicht zuletzt aufgrund des Umstandes, dass dies für automatisierte Exportprozesse anerkannt ist.[391] In Zweifelsfällen ist das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) vorsorglich zu kontaktieren.

5.3 Organisatorische Implementierungshindernisse

Im Rahmen dieses Abschnitts werden organisatorische Implementierungshindernisse diskutiert. Es geht dabei in erster Linie um die Implementierung von organisatorischen Sicherheitsmaßnahmen. In diesem Zusammenhang erscheint zunächst ein Blick auf Hemmnisse, die die Umsetzung von I4.0 insgesamt einschränken oder beeinträchtigen, lohnenswert.

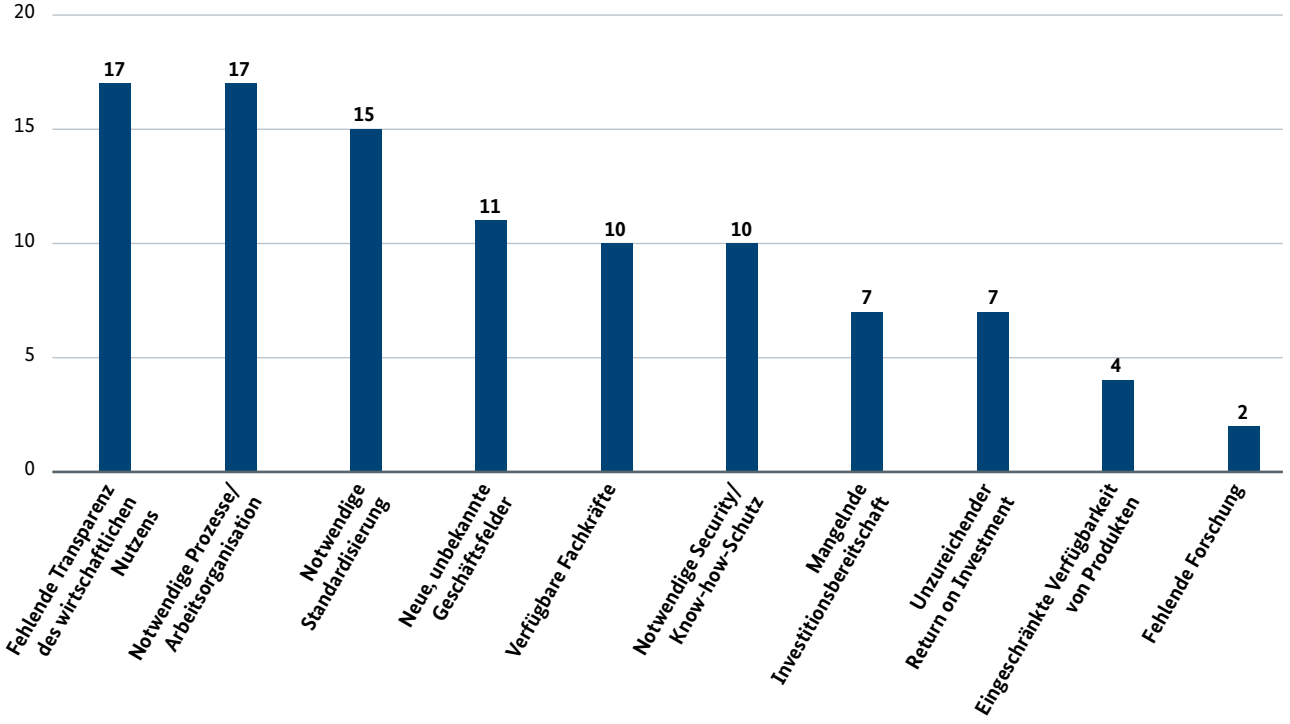
Allgemein betrachtet gelten einer MHP-Studie zufolge die fehlende Transparenz des wirtschaftlichen Nutzens und notwendige Anpassungen von Prozessen sowie der Arbeitsorganisation als die größten Hemmnisse für die Umsetzung von I4.0 (Abbildung 5–1).[392] Aber auch die Gewährleistung eines hinreichenden Sicherheitsniveaus und des Schutzes von Know-How stellen ein großes Hemmnis dar. Gefragt wurden die Studienteilnehmer nach den drei aus ihrer Sicht größten Hemmnissen für die Umsetzung von I4.0.

Die Studie unterstreicht damit die Handlungsbedarfe im Hinblick auf Fragen der IT-Sicherheit in der I4.0. Zudem verdeutlicht die Studie, dass, vor allem im Rahmen der Betrachtung organisatorischer Aspekte der IT-Sicherheit, ein wesentliches Hindernis für die Umsetzung von I4.0 darin gesehen wird, dass Anpassungen von Prozessen und der Arbeitsorganisation im Allgemeinen nötig sind. Insgesamt fallen die Investitionen zur Umsetzung von I4.0 in allen Bereichen aktuell noch verhalten aus.[393]

Im Folgenden werden, unter besonderer Berücksichtigung der Fallbeispiele, organisatorische Implementierungshindernisse betrachtet. Die Hindernisse bei der Umsetzung von organisatorischen IT-Sicherheitsmaßnahmen lassen sich im Wesentlichen in drei Gruppen einteilen: Die erste spiegelt die Problematik der Technikintegration in bestehende Prozesse wider, die zweite die veränderte Rolle des Menschen innerhalb der von I4.0 beeinflussten Prozesse und die dritte betrifft das Thema Vertrauen – sowohl in die

386 Vgl. Wermelt/Tervooren, CCZ 2013, 81 (84).
387 Vgl. Wermelt/Tervooren, CCZ 2013, 81 (82).
388 Vgl. Wermelt/Tervooren, CCZ 2013, 81 (86).
389 Bundesamt für Wirtschaft und Ausfuhrkontrolle, Internal Compliance Programmes – ICP, Januar 2014, abrufbar unter (letzter Aufruf 5. Juni 2015): http://www.ausfuhrkontrolle.info/ausfuhrkontrolle/de/arbeitshilfen/merkblaetter/merkblatt_icp.pdf
390 Bundesamt für Wirtschaft und Ausfuhrkontrolle, Internal Compliance Programmes – ICP, Januar 2014, 23, abrufbar unter (letzter Aufruf 5. Juni 2015): http://www.ausfuhrkontrolle.info/ausfuhrkontrolle/de/arbeitshilfen/merkblaetter/merkblatt_icp.pdf
391 Hauschka/Merz, Corporate Compliance, § 33 Rn. 16.
392 Kelkar, O. (2014): Industrie 4.0 – Eine Standortbestimmung der Automobil- und Fertigungsindustrie, MHP – A Porsche Company, S. 6, http://www.mhp.com/fileadmin/mhp.de/assets/studien/MHP-Studie_Industrie4.0-Zusammenfassung_V1.4.pdf
393 Ebenda, S. 9.

Abbildung 5–1: Hemmnisse für die Umsetzung von Industrie 4.0
in Prozent



Quelle: Kelkar, O. (2014): Industrie 4.0 – Eine Standortbestimmung der Automobil- und Fertigungsindustrie, MHP – A Porsche Company, Seite 6

Technik, aber auch in die Kooperationspartner und das Potenzial der Vision von I4.0.

Die Vision von I4.0 erweist sich als stark technologiegetrieben, allem voran durch die Sensorik und die Informationstechnologie. Hier haben die Entwicklungen der letzten Jahre überhaupt erst die heutige Vision von I4.0 wachsen lassen. Noch gibt es aber weder Standards noch „die I4.0-Technologie", sodass Unternehmen bisher weitestgehend alleine auf ihrem Weg zu einer vernetzten und automatisierten industriellen Produktion da stehen und demensprechend zögerlich agieren. Hinzu kommt, dass die Lebenszyklen von industriellen Produktionsanlagen sehr lang sind. Es ist keine Seltenheit, dass eine Maschine 30 Jahre oder sogar länger im Einsatz ist, so dass sich aktuell die Frage nach einem Austausch oft gar nicht stellt. Diese aktuell eingesetzten Maschinen und Anlagen wurden noch unter ganz anderen Prämissen konstruiert, vorrangig hinsichtlich der Funktionalität. Heutige Anforderungen wie die direkte Einbindung in Manufacturing-Execution-Systeme (MES) oder komplexe und dynamische Wertschöpfungsnetzwerke waren zur Zeit der Konstruktion noch nicht bekannt. Dies führt dazu, dass die Unternehmen heute vor der Entscheidung stehen, entweder a) die Produktionsanlagen unter den aktuellen Bedingungen komplett zu erneuern oder b) die vorhandenen Anlagen weiter zu nutzen und eine eigene IT-Infrastruktur um die bestehenden Investitionsgüter herum zu kreieren. Im Fall a) stellt die nötige Investition in eine Technologie, die sich möglicherweise nicht durchsetzen wird das größte Hemmnis dar, im Fall b) die organisatorische Einbindung einer eigenen IT-Infrastruktur, die möglicherweise jedoch die Anforderungen eines umfassenden „Defence-in-Depth"-Ansatzes nie erfüllen kann, da es an einer Möglichkeit fehlt, eine Härtung des Systems direkt auf Ebene der Anlage umzusetzen. Hier fehlen organisatorische Konzepte zum schrittweisen Übergang zur industriellen Produktion der Zukunft, die es auch KMU erlauben, an der Vision teilzuhaben.

Dies wird aber nur möglich sein, wenn auch die noch bestehenden infrastrukturellen Hindernisse überwunden werden können. Potenziell zentrale Technologien wie zum Beispiel Cloud Computing oder Smart Grid, welche als IT-Infrastruktur genutzt werden können, benötigen eine leistungsstarke Internetanbindung. Fakt ist jedoch, dass heute noch eine Vielzahl von international erfolgreichen

mittelständischen Industrieunternehmen nur unzureichend mit breitbändigen Internet-Anschlüssen versorgt und damit von I4.0 ausgeschlossen ist.[394]

In ähnlicher Weise wirkt sich die noch nicht vorhandene Standardisierung aus – weder für Schnittstellen, noch für die Datenübertragung oder die Sicherheit der Daten beim Datenaustausch über offene Netze gibt es heute Standards, an denen die Unternehmen sich orientieren können. Heutige Insellösungen bei Product Data Management (PDM), Enterprise Resource Planning (ERP) und Produktionsplanungs- und Steuerungssystemen (PPS) führen zu Inkompatibilitäten mangels einheitlicher Schnittstellen und Standards. Mit der Standardisierung geht aber auch die Gestaltung der innerbetrieblichen und der unternehmensübergreifenden Prozesse einher, so dass auch hier von Unternehmen die Gefahr gesehen wird, eine Fehlentscheidung zu treffen, die später wieder revidiert werden muss.

Ein weiteres organisatorisches Problem bringt die erforderliche Reaktionsgeschwindigkeit bei Sicherheitslücken mit sich. Updates und Patches für Anlagensteuerungen können z. B. in Unternehmen der produzierenden Industrie nicht ohne weiteres eingespielt werden. Die Bereitschaft, an einer fehlerfrei arbeitenden Maschine eine Änderung oder ein Update vorzunehmen ist sehr gering, da jede Änderung eine potenzielle Störung der Produktionsabläufe mit sich bringt. Daher werden solche Tätigkeiten oftmals auf das nächste geplante Wartungsfenster verschoben – angesichts von möglichen Angriffen ein zu langer Zeitraum.

Die zweite, ebenso wichtige Kategorie von Hemmnissen bezieht sich auf die Rolle des Menschen innerhalb der der von I4.0 beeinflussten Prozesse. Besonders naheliegend und damit wohl auch am präsentesten ist der erforderliche Schulungs- und Qualifizierungsaufwand im Hinblick auf die technischen und organisatorischen Änderungen, die mit dem Übergang zur industriellen Produktion der Zukunft einhergehen. Eine Anlage, deren Komplexität durch zusätzliche Hard- und Software erhöht wird, erfordert ein tieferes Verständnis durch den Bediener – nicht nur, aber auch im Hinblick auf die vor- und nachgelagerten Prozesse sowie für die Prozesse der Datennutzung. Damit stellt sich die Frage, inwiefern der Mitarbeiter unmittelbar am System überhaupt in der Lage ist, dieses zu kontrollieren und damit die Verantwortung für den Systembereich zu übernehmen.[395] Gleichzeitig erhöhen weitreichende Rechte einzelner Mitarbeiters die Gefahr, dass Produktionsanlagen ausspioniert oder Prozesse manipuliert werden. Ein ausschließlicher Schutz über die Vergabe von Rollen und Berechtigungen innerhalb des IT-Systems berücksichtigt die Rolle des Menschen als Know-how-Träger im Unternehmen nicht ausreichend.

Auch die Rolle eines oftmals konservativen Betriebsrates, der primär die Aufgaben der Mitarbeiter und deren Arbeitsplatzsicherheit im Fokus hat, kann sich als organisatorisches Hemmnis im Zusammenhang mit Maßnahmen der Flexibilisierung sowie der Vernetzung und Automatisierung erweisen, wenn dieser nicht frühzeitig eingebunden wird.

Die dritte Kategorie steht unter dem Oberbegriff Vertrauen – in die Technologie, die kooperierenden Partner und das Potenzial der Vision von I4.0 im Allgemeinen.

Während die Vision von I4.0 für viele Unternehmen heute noch schwer zu greifen ist[396], besteht Einigkeit darüber, dass Daten (zunächst) nur mit vertrauten Geschäftspartnern ausgetauscht werden sollen und dass nur autorisierte Servicepartner beispielsweise Möglichkeiten zur Fernwartung wahrnehmen können sollten. Hier wird Vertrauen aus der Erfahrung mit dem Geschäftspartner abgeleitet. Dieses ermöglicht dann auch die nötige Abstimmung von vor- und nachgelagerten Geschäftsprozessen und IT-Systemen, erfordert aber einen hohen Aufwand und reduziert die Flexibilität maßgeblich. Systemvertrauen existiert mangels standardisierter Lösungen und etablierter Anbieter noch keines – was sich wiederum hemmend auf die Inanspruchnahme von Leistungen, etwa durch IT-Systemhäuser, auswirkt.

Das Thema Vertrauen spielt weiterhin eine große Rolle bei den zu erwartenden Reaktionen der Mitarbeiter und der Gesellschaft auf den Übergang zur industriellen Produktion der Zukunft: Durch die allgegenwärtige Datenerfassung muss der einzelne Mitarbeiter davon ausgehen, dass er in seiner Arbeit stärker als bisher kontrollierbar ist. Abgesehen von der Einhaltung der datenschutzrechtlichen Regeln, sind hier organisatorische Vorkehrungen nötig, die einen ausschließlich zweckgebundenen Einsatz der erfassten Daten und die unverzügliche Löschung von zumindest potenziell personenbeziehbaren Daten garantieren, um das

394 Deutscher Industrie- und Handelskammertag (2014): Industriestandort Deutschland: Risse im Fundament – DIHK-Umfrage im Netzwerk Industrie 2014, S. 4.

395 s. Hirsch-Kreinsen, Hartmut 2014: Welche Auswirkungen hat „Industrie 4.0“ auf den Arbeitsmarkt? in WISO direkt, Hg. v.d. Abteilung Wirtschafts- und Sozialpolitik der Friedrich-Ebert-Stiftung.

396 s. Kelkar/Heger aaO.

Vertrauen und damit die Loyalität der Mitarbeiter langfristig zu sichern.

Als ebenso gravierendes Hemmnis erweist sich das noch fehlende Vertrauen in die Vision von I4.0 im Allgemeinen. Nicht unwesentlich sind in diesem Zusammenhang offene Fragen zur Gewährleistung eines angemessenen IT-Sicherheitsniveaus. Konkret bestehen sowohl Bedenken hinsichtlich des Datenschutzes und der Offenlegung von Geschäftsgeheimnissen als auch Angst vor Sabotage des Produktionsprozesses und vor Kontrollverlust.

5.4 Rechtliche Implementierungshindernisse

Im nachfolgenden Abschnitt werden rechtliche Implementierungshindernisse in Bezug auf Anforderungen an technische und organisatorische Gegebenheiten von IT-Sicherheitsmaßnahmen aus datenschutzrechtlicher (5.4.1) und exportkontrollrechtlicher Sicht (5.4.2) mit Blick auf die I4.0 näher erläutert.

In der Folge wird dann weiter ausgeführt, wie IT-Sicherheit in der I4.0 durch rechtliche Normen in Deutschland gewährleistet werden kann (5.4.3).

5.4.1 Implementierungshindernisse aufgrund von aus dem Exportkontrollrecht folgenden IT-Sicherheitsanforderungen

Für an I4.0 beteiligte Kooperationspartner dürften insbesondere die Beteiligung mehrerer Partner und die Anwendbarkeit des Exportrechts unterschiedlicher Rechtsordnungen für Herausforderungen sorgen. Das gilt – soweit es das hiesige Recht betrifft – ebenfalls für Prüfungen des Bundesamtes für Wirtschaft und Ausfuhrkontrolle, das sich immer mehr auch mit schwierigen technischen Sachverhalten und unterschiedlichen betroffenen Stellen zu beschäftigen haben wird. Soweit besondere Sicherheitsanforderungen zu erfüllen sind, um zu ermöglichen, dass Technologien, deren Verwendung unter exportkontrollrechtlichen Aspekten eigentlich verboten wäre, bei I4.0 gleichwohl genutzt werden dürfen, kann dies zu wirtschaftlichen oder tatsächlichen Hindernissen für die Nutzung von I4.0 führen. Insoweit wären daher klare Leitlinien, Umsetzungshinweise und ggfs. gesetzliche Privilegierungen empfehlenswert, die darauf abzielen, die Nutzung von Technologien zu ermöglichen, die exportkontrollrechtlich eigentlich nicht genutzt werden dürften. Insoweit dürfte sich ein Zusammenwirken des Bundesgesetzgebers mit den Bundesämtern für Wirtschaft und Ausfuhrkontrolle sowie für Sicherheit in der Informationstechnik empfehlen. Dabei sollten die einschlägigen Branchenverbände möglichst frühzeitig eingebunden werden.

5.4.2 Implementierungshindernisse aufgrund von aus dem Datenschutzrecht folgenden IT-Sicherheitsanforderungen

Mit Blick auf die derzeit gültigen Anforderungen des § 9 BDSG dürften datenschutzrechtliche Implementierungshindernisse insbesondere daraus resultieren, dass das BDSG jeweils auf eine sog. „verantwortliche Stelle“ abzielt, also eine juristische Person.[397] An einer vernetzten Infrastruktur im Rahmen von I4.0 dürften häufig zahlreiche verschiedene juristische Personen beteiligt sein, die unterschiedlichen Anforderungen in Bezug auf die Datensicherheit unterliegen.

Diese Herausforderung dürfte in den Grundkonstellationen 1a (sternförmige Kooperationsstruktur mit einem zentralen Partner und weiteren Beteiligten im Inland) und 2a (netzförmige Kooperation, d.h. ohne Zentralpartner, wobei die Partner ausschließlich in Deutschland belegen sind) noch am ehesten handhabbar sein, da in diesem Falle alle Beteiligten derselben Rechtsordnung (BDSG) unterliegen und deshalb zumindest den abstrakten Anforderungen aus § 9 BDSG dieselben technisch-organisatorischen Anforderungen zu erfüllen haben, wobei auch hier bereits das Problem stellen kann, adäquate vertragliche Regelungen zu Datenschutz und Datensicherheit zu treffen, wenn die Anzahl von Kooperationspartnern sehr hoch ist. Herausforderungen ergeben sich indes besonders bei internationalen Kooperationsstrukturen.

Sofern es sich um Beteiligte innerhalb des EWR handelt, dürfte noch Ähnliches gelten wie bei bloß innerdeutschen Sachverhalten, da den jeweils einschlägigen nationalen Datenschutzgesetzen die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EU-Datenschutzrichtlinie) zugrunde liegt und deren grundsätzliches Ziel die Vereinheitlichung der datenschutzrechtlichen Rahmenbedingungen innerhalb des europäischen Binnenmarktes ist.[398]

397 Vgl. Gola/Schomerus/Klug/Gola/Körffer BDSG § 3 Rn. 48.
398 Erwägungsgründe der Richtlinie 95/46/EG.

So normiert Artikel 17 Absatz 1 Satz 1 der EU-Datenschutzrichtlinie, dass die Mitgliedsstaaten vorzusehen haben, dass der für die Verarbeitung Verantwortliche geeignete technischen und organisatorischen Maßnahmen sicherstellen muss, die für den Schutz gegen

- die zufällige oder unrechtmäßige Zerstörung,
- den zufälligen Verlust,
- die unberechtigte Änderung,
- die unberechtigte Weitergabe oder den unberechtigten Zugang – insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden – und
- jede andere Form der unrechtmäßigen Verarbeitung

personenbezogener Daten erforderlich sind. Artikel 17 Absatz 1 Satz 2 der EU-Datenschutzrichtlinie konkretisiert die Maßstäbe zur Beurteilung hinreichender technisch-organisatorischer Maßnahmen weiterhin dadurch, dass festgelegt ist, dass die Maßnahmen unter Berücksichtigung des Standes der Technik und der bei ihrer Implementierung entstehenden Kosten ein Schutzniveau gewährleisten müssen, das gemessen an den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

Die Vorgaben der EU-Datenschutzrichtlinie sind weitgehend deckungsgleich zu den Anforderungen gemäß § 9 BDSG. Der deutsche Gesetzgeber hat von seinen Möglichkeiten der Konkretisierung jedoch Gebrauch gemacht und in der Anlage zu § 9 BDSG die einzelnen Kontrollkategorien gegenüber der Aufzählung in Artikel 17 Absatz 1 Satz 1 der EU-Datenschutzrichtlinie jedoch weiter ausdifferenziert. Diese Ausdifferenzierung zu den neun Geboten der Datensicherheit muss sich in den Gesetzen anderer EU-Staaten daher nicht ausdrücklich wiederfinden. Auch mag die Aufsichtspraxis der Datenschutzaufsichtsbehörden anderer Länder zu der Frage der Angemessenheit der technischen und organisatorischen Maßnahmen von der deutschen Aufsichtspraxis abweichen, sodass innerhalb der Kooperationsstruktur unterschiedliche rechtliche Anforderungen an die Ausgestaltung technisch-organisatorischer Maßnahmen gestellt werden können. In einem „worst case scenario“ wäre es denkbar, dass diese sich gar widersprechen. Hierdurch könnte ein hohes technisch-organisatorische Schutzniveau in einen Land (z. B. Deutschland) im nächsten Verarbeitungsschritt durch die Datenübermittlung in ein anderes EU-Land damit gleichwohl de facto unterlaufen werden. Dies wiederum kann die Legitimität der Datenübertragung an einen anderen Kooperationspartner erheblich in Frage stellen, da dies mit den schutzwürdigen Interessen der Betroffen (z. B. deutscher Beschäftigte) kollidieren kann. Dies wiederum würde einem Eingreifen einer Erlaubnisnorm für die entsprechende Datenverarbeitung im Rahmen von I4.0 (z. B. § 32 Abs. 1 S. 1 BDSG) in aller Regel entgegenstehen.

Für außereuropäische Sachverhalte gilt dies ohnehin, da es insoweit – zumindest derzeit noch – zusätzlich an dem vereinheitlichenden Element der EU-Datenschutzrichtlinie fehlt. Soweit die des DS-GVO-E besteht dieses Problem zumindest für all die Fälle fort, für die eine exterritoriale Geltung der DS-GVO nicht vorgesehen ist.

Diese Herausforderung ließe sich – ohne den Abschluss zahlreicher Verträge zwischen den einzelnen Beteiligten von I4.0 – nur dadurch umgehen, dass international einheitliche Standards und good practices in Sachen Informationssicherheit rechtsverbindlich (z. B. über zwischenstaatliche Abkommen) festgelegt werden. Dies macht es allerdings nicht entbehrlich, möglichst auch Vertragswerke (z. B. angepasste EU-Standardvertragsklauseln und Auftragsdatenverarbeitungsmuster) in dieser Hinsicht bereitzustellen, die die komplexe, d.h. multilaterale, Verarbeitungssituation bei I4.0 hinreichend aufgreifen und abbilden und ggf. auch im nationalen Umfeld einheitlich zu regeln, da hier insgesamt keine einheitlichen regulatorischen Anforderungen zu erkennen sind, was im nachfolgenden Kapitel vertieft erläutert wird.

5.4.3 Strukturelle Merkmale der rechtlichen Anforderungen an die IT-Sicherheit

Die Regulierung der IT-Sicherheit kann im Rahmen dieser Untersuchung nicht flächendeckend analysiert werden. Ziel ist vielmehr, strukturelle Merkmale der gegenwärtigen Lage herauszuarbeiten, die für die Weiterentwicklung der Regulierung im Hinblick auf I4.0 zu berücksichtigen sind.

Zu diesem Zweck sollen die einzelnen Instrumente der rechtlichen Regulierung auf ihre Leistungsfähigkeit zur Regulierung von IT-Sicherheit in Bezug auf die beiden Elemente, die Bildung materieller Normen und die Durchsetzung normativer Anforderungen, hin untersucht werden. Für die Zwecke dieser Untersuchung werden folgende Instrumente der Regulierung anhand ihrer normativen Charakters unterschieden:

- Gesetzgebung;
- Rechtsprechung;
- Behördliche Kontrolle;
- Parteiautonomie (Vertrag);
- Institutionelle Regelwerke und Standards;
- Kodizes/ Selbstbindung;
- Zertifizierung und Gütesiegel.

5.4.3.1 Gesetzgebung

5.4.3.1.1 Technik-Regulierung durch Gesetzgebung

Die Gesetzgebung erfolgt im Bereich der Technik häufig durch eine Kombination von Parlamentsgesetz, Rechtsverordnung und untergesetzlichen Normen. Insbesondere hält sich der Gesetzgeber mit der Formulierung technischer Anforderungen durch Parlamentsgesetz zu Recht zurück, da die Anpassung technischer Anforderungen durch formelle Gesetze mit dem technischen Fortschritt regelmäßig nicht Schritt halten kann. Für das formelle Gesetz bleibt daher die Regelung von Zielen und Grundszenarien, die - soweit möglich - technikneutral formuliert werden sollten, um den technischen Fortschritt nicht ungewollt zu behindern. Daher bedient sich der Gesetzgeber insoweit der Rechtsverordnung. In beiden Fällen bleibt jedoch eine Fülle an technischen Details, die auch durch eine Rechtsverordnung nicht ganz geregelt werden können. Hier wird teilweise auf technische Normen verwiesen.

Gesetzgebung findet sich auch in Bezug auf IT-Sicherheit. Dabei verwendet der Gesetzgeber regelmäßig eine Kombination aus Parlamentsgesetz und Rechtsverordnung. So enthält etwa das deutsche Signaturgesetz etliche Grundsätze, Details werden durch eine Signatur-Verordnung geregelt, das Personalausweisgesetz regelt grundlegende Elemente der elektronischen Identifizierung, die Personalausweis-Verordnung etliche Details. Das BSI-Gesetz ermöglicht eine Zertifizierung für IT-Sicherheit, nähere Aspekte dazu sind in der BSI-Zertifizierungs- und Anerkennungsverordnung (BSIZertV) geregelt.

Ein anderes Instrument zur gesetzlichen Regelung von IT-Sicherheitsanforderungen ist die Formulierung allgemeiner gesetzlicher Anforderungen, verbunden mit einer Normkonkretisierung durch die Verwaltung (dazu unten). Ein bekanntes Beispiel mit Bezug zur IT-Sicherheit stellt § 25a KWG in Verbindung mit den Mindestanforderungen an das Risikomanagment (MaRisk) dar (dazu unten).

In vielen Fällen beschränkt sich der Gesetzgeber auch auf eine recht offene Regelung und überlässt die Konkretisierung der Praxis und der Rechtsprechung. So enthalten etwa die allgemeinen Pflichten der Geschäftsführungsorgane, etwa nach § 92 AktG und nach § 43 GmbH auch Pflichten in Bezug auf die IT-Sicherheit der Unternehmern, die allerdings ohne jegliche gesetzliche Konkretisierung sind.

Bei der Gesetzgebung zu materiellen Anforderungen an IT-Sicherheit sind die gesetzliche Regelung konkreter Technologien zur Gewährleistung von IT-Sicherheit und die gesetzliche Regelung von Anforderungen an IT-Sicherheit zu unterscheiden.

5.4.3.1.2 Gesetzgebung zu Sicherheitstechnologien

Der Gesetzgeber hat verschiedentlich Regelungen zu konkreten technischen Produkten mit dem Ziel, Produkte mit besonderen Eigenschaften in Bezug auf IT-Sicherheit zu schaffen, erlassen. Bekannte Beispiele sind etwa das Signaturgesetz von 1997[399] und die darauf basierende Signaturverordnung[400], die die elektronische Signatur regelt.

Ein anderes Beispiel ist der elektronische Identitätsnachweis, der durch das Personalausweisgesetz[401] von 2009 geschaffen wurde. Hier treffen die §§ 18, 19 des neuen PAuswG eine recht dichte Regelung des elektronischen Identitätsnachweises.

In der Personalausweisverordnung (PAuswV)[402] werden etliche Details, etwa zur Nutzung des elektronischen Identitätsnachweises (§§ 22 f. PAuswV), zur Sperrung des elektronischen Identitätsnachweises (§§ 24 ff. PAusfV),

399 Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG).
400 Verordnung zur elektronischen Signatur (Signaturverordnung – SigV).
401 Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz – PAuswG).
402 Verordnung über Personalausweise und den elektronischen Identitätsnachweis – PauswV.

zur Berechtigung zur Einsicht in die Daten, insb. das Berechtigungszertifikat (§§ 28 ff. PAuswG) geregelt. Die technischen Details hingegen sind im Wesentlichen weder im PAuswG noch in der PAuswV geregelt, sondern werden durch Technische Richtlinien des BSI festgelegt. Insoweit verweist die PAuswV teilweise unmittelbar auf die Technischen Richtlinien, so namentlich für die Zertifizierung von Komponenten in § 3 PAuswV. Gemäß § 2 PauswV sollen die Technischen Richtlinien den Stand der Technik in Bezug auf bestimmte Komponenten konkretisieren.

Durch das De-Mail-Gesetz von 2011[403] will der Gesetzgeber die sogenannte „De-Mail" als sichere und vertrauliche Kommunikationsplattform im Internet etablieren. Das De-Mail-Gesetz regelt Anforderungen an die Sicherheit der Komponenten des De-Mail-Systems. Die Konkretisierung der Anforderungen erfolgt de facto über die Technische Richtlinie 01201 De-Mail des BSI, indem die Einhaltung des Standes der Technik nach § 18 Abs. 2 S. 2 De-Mail-Gesetz vermutet wird, wenn die Anforderungen dieser Technischen Richtlinie eingehalten werden. Für die Weiterentwicklung der technischen und organisatorischen Anforderungen an die Sicherheit wählt das De-Mail-Gesetz einen interessanten Weg: Diese sollen gemäß § 22 De-Mail-Gesetz durch den „Ausschuss De-Mail-Standardisierung" geregelt werden, in dem Diensteanbieter und Behörden, insbesondere das BSI und die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, vertreten sind.

Diese Beispiele der gesetzlichen Regelung konkreter Techniken und ihrer Sicherheit hat interessanterweise nicht nur Zustimmung, sondern auch viel Kritik hervorgerufen. Die elektronische Signatur des deutschen Signaturgesetzes gilt als gescheitert.[404] Zwar wird dies nicht auf konkrete Mängel des Gesetzes zurückgeführt, jedoch geht eine durchaus verbreitete Einschätzung dahin, dass die Regelung zu kompliziert ist und der Aufwand, gemessen am Mehrwert der qualifizierten Signatur zu hoch sei.[405]

Auch der elektronische Identitätsnachweis hat sich in der Praxis bisher nicht durchgesetzt.[406] Auch insoweit wird in der Praxis oft beanstandet, dass die gesetzliche Regelung zu einer zu aufwendigen Gestaltung führt, der kein entsprechender Gegenwert durch Nutzung des elektronischen Identitätsnachweises gegenübersteht.[407]

5.4.3.1.3 Materielle Anforderungen an IT-Sicherheit

Eine allgemeine gesetzliche Regelung zur IT-Sicherheit besteht bisher, wie dargestellt, nicht. Jedoch finden sich in vielen Fällen gesetzliche Anforderungen an Sicherheit, die auch die IT-Sicherheit umfassen. Eines der bekanntesten und wichtigsten Beispiele ist § 9 BDSG für den Bereich des Datenschutzes, der oben bezüglich der rechtlichen Implementierungshindernisse bereits näher erläutert wurde.[408] § 9 BDSG regelt die Anforderungen an die technische Sicherung im Wege einer Generalklausel. Interessanterweise erfolgt eine Konkretisierung nicht durch eine Rechtsverordnung, vielmehr sind in einem Anhang zu § 9 einzelne Elemente der technischen und organisatorischen Maßnahmen geregelt.

Zahlreiche Gesetze enthalten für spezifische Bereiche konkrete IT-Sicherheitsanforderungen, etwa die Anforderungen an die sichere Anmeldung zu einem De-Mail-Dienst nach § 4 De-Mail-Gesetz, das Notfallkonzept für IT-Systeme nach § 25a Abs. 1 Nr. 5 KWG für den Banksektor, die erforderlichen technischen Schutzmaßnahmen nach § 109 TKG oder die Notwendigkeit der Nutzung von dem jeweiligen Stand der Technik entsprechenden Verschlüsselungsfahren nach § 28a Abs. 13 S. 3 SGB IV sowie § 17 Abs. 2 S. 2 SchwArbG.

Eine allgemeine Regelung von IT-Sicherheit, etwa in Art eines IT-Sicherheitsgesetzes oder -Gesetzbuchs, existiert in Deutschland bisher nicht. Umso mehr ist der Entwurf des IT-Sicherheitsgesetzes von Interesse, der nach den Angaben der Bundesregierung eine erhebliche Verbesserung in der IT-Sicherheit herbeiführen soll (dazu unten).

403 De-Mail-Gesetz vom 28. April 2011 (BGBl. I S. 666); siehe einen Überblick bei Roßnagel, NJW 2013, 1473 ff.

404 Fox, DuD 2009, 387; Spindler, CR 2011, 309; http://blogs.faz.net/digitaltwin/2014/05/07/wer-buergt-fuer-unsere-digitale-identitaet-617/ In der Praxis konnte sich die Verwendung qualifizierter elektronischer Signaturen jedenfalls bisher nicht durchsetzen, siehe Borges/Schwenk/Stuckenberg/Wegener, Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 312; Zimmermann, in MüKo, ZPO 371a ZPO Rn. 2.

405 Siehe http://blogs.faz.net/digitaltwin/2014/05/07/wer-buergt-fuer-unsere-digitale-identitaet-617/; Vgl. auch Spindler, CR 2011, 309 Fn. 1 der darauf hinweist, dass die Vorteile zunächst nur dem Vertragspartner zukommen.

406 So sind nach Schätzungen des Bundesinnenministeriums nur bei 30 Prozent aller Ausweise überhaupt die eID-Funktionen aktiviert, siehe http://www.personalausweisportal.de/DE/Wirtschaft/Diensteanbieter-werden/FAQ/faq_node.html (zuletzt abgerufen am 21.05.2015).

407 Siehe etwa http://www.secupedia.info/wiki/Neuer_Personalausweis; https://www.test.de/Neuer-Personalausweis-Enttaeuschung-im-Praxistest-4214969-0/ (zuletzt abgerufen am 21.05.2015).

408 Vgl. hierzu ausführlich unten Ziff. 5.4.2.

5.4.3.1.4 Bedeutung der gesetzlichen Regelung von IT-Sicherheit

Der Erfolg der Regelung von Sicherheitsanforderungen durch Gesetz wurde bisher, soweit ersichtlich, nicht im Einzelnen untersucht. Dies dürfte darauf beruhen, dass die praktische Bedeutung einzelner gesetzlicher Normen zur Verbesserung von IT-Sicherheit nur schwer zu messen ist. Ein Maßstab wäre aber wohl die Frage, ob die Existenz einer gesetzlichen Norm in der Praxis zu einer einheitlichen Auffassung über die maßgeblichen Anforderungen geführt hat.

Insoweit ist insbesondere § 9 BDSG von Interesse, da diese Norm seit 1991 in Kraft ist und für den gesamten Bereich der Wirtschaft maßgeblich ist Da der Begriff des personenbezogenen Datums sehr weit gefasst ist, sind zwar klassische Produktionsprozesse von Industriegütern nicht erfasst, wohl aber zum einen der gesamte Bereich der EDV zur Geschäftsführung und zum Management der vertraglichen Leistungsbeziehungen, zunehmend aber auch IT im Bereich der Produktion.

Insoweit lässt sich aber schon anhand einer Analyse der Literatur feststellen, dass starke Unsicherheit über konkrete Anforderungen herrscht, die durch das Fehlen von Rechtsprechung (dazu unten) verstärkt wird. Dies betrifft selbst essentielle Anforderungen im Bereich der IT-Sicherheit, wie am Beispiel des Zugangsschutzes demonstriert werden soll: Die nach § 9 BDSG erforderlichen technischen und organisatorischen Maßnahmen sollen, wie Nr. 2 der Anlage zu § 9 klarstellt, verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Der Zugangsschutz ist essentiell, insbesondere bei allen per Internet erreichbaren Systemen, die Angriffen von Hackern ebenso wie dem Missbrauch von Authentisierungsmedien ausgesetzt sind.

Während die Bedeutung des Zugangsschutzes als solche anerkannt ist, besteht keinerlei Klarheit hinsichtlich der Anforderungen. In den gängigen Kommentierungen zu § 9 BDSG werden zwar mögliche Maßnahmen zum Zugangsschutz genannt, darunter auch „Passwortschutz“ als konkrete Maßnahme erwähnt.[409]

Es besteht auch Einigkeit darin, dass Passwortschutz oder eine andere Form des Zugangsschutzes gesetzlich geboten ist, wie in Nr. 2 der Anlage zu § 9 BDSG ausdrücklich genannt.[410] Eine Konkretisierung der gesetzlichen Anforderungen an die Qualität des Passwortschutzes oder gar zum Erfordernis weitergehender Schutzmechanismen wie etwa Zwei-Faktor-Authentisierung findet sich jedoch nicht. Zwar wird mitunter eine Zwei-Faktor-Authentisierung für bestimmte Fälle „empfohlen“.[411] Eine solche „Empfehlung“, deren rechtlicher Gehalt völlig unklar ist, hat aber jedenfalls nicht die Wirkung einer Gesetzeskonkretisierung, führt also nicht zu einer verbindlichen Festlegung der empfohlenen Maßnahme als gesetzlicher Standard.

Dies beruht letztlich auf der ungeheuren Vielfalt der Sachverhalte in der Praxis, lässt den Rechtsanwender aber in der Frage, welche Maßnahme anhand der in § 9 BDSG geforderten Abwägung geboten ist, weitgehend allein.

Dies führt dazu, dass das Gesetz letztlich kaum eine Hilfestellung für die Konkretisierung der Anforderungen an IT-Sicherheit gibt und Rechtsunsicherheit selbst in Bezug auf grundlegende Sicherheitsanforderungen besteht.

5.4.3.1.5 Durchsetzungsmechanismen

Die Durchsetzung rechtlicher Anforderungen an IT-Sicherheit kann das Gesetz durch verschiedene andere Mittel sichern, insbesondere durch behördliche Aufsicht oder durch Androhung von Sanktionen strafrechtlicher oder ordnungsrechtlicher Art, durch Instrumente wie Klagemöglichkeiten (Unterlassungsklage) oder durch die Pflicht zum Schadensersatz bei Verstößen.

Insoweit lässt sich feststellen, dass die vom Gesetz eingesetzten Mittel zur Durchsetzung von Anforderungen an IT-Sicherheit sehr unterschiedlich genutzt werden. Teilweise werden mehrere Mittel genutzt, teilweise fehlt es an spezifischen Durchsetzungsmechanismen, so dass nur allgemeine Mittel zu Verfügung stehen, etwa eine Haftungsandrohung nach allgemeinem Deliktsrecht.

409 So etwa Simitis-Ernestus, BDSG, 8. Aufl. 2014, § 9 Rn. 98.

410 Borges/Schwenk/Stuckenberg/Wegener, Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 206; Brennscheidt, Cloud Computing und Datenschutz, S. 89; Gola/Klug/Körffer, in Gola/Schomerus, § 9 Rn. 23; Schultze-Melling in Taeger/Gabel, BDSG, § 9 Rn. 54 ff.

411 So etwa Art.-29-Datenschutzgruppe, Stellungnahme 05/2012 zum Cloud Computing, 1.7.2012, 01037/12/DE, WP 196, S. 19; BSI, Eckpunktepapier, Sicherheitsempfehlungen für Cloud Anbieter – Mindestanforderungen in der Informationssicherheit, S. 43.

Ein Beispiel für den ausdrücklichen Einsatz mehrerer Durchsetzungsinstrumente besteht in Bezug auf die Pflicht zur IT-Sicherheit im Datenschutzrecht. Hier setzt das Gesetz sowohl die behördliche Aufsicht als auch die zivilrechtliche Haftung ein.

Die Datenschutzaufsichtsbehörden können bei Verstößen gegen § 9 BDSG nach § 38 Abs. 5 S. 1 Var. 2, S. 2 BDSG Maßnahmen anordnen oder gar die Datenverarbeitung untersagen. Verstöße gegen die gesetzlichen Anforderungen des § 9 BDSG lösen, soweit dadurch dem Betroffenen ein Schaden entsteht, nach § 7 BDSG eine Verpflichtung zum Schadensersatz aus.[412] Außerdem besteht eine Pflicht zum Schadensersatz nach allgemeinem Deliktsrecht, da § 9 BDSG als Schutzgesetz i.S. des § 823 Abs. 2 BGB angesehen wird.[413]

Der Erfolg der gesetzlichen Durchsetzungsinstrumente in Bezug auf die gesetzlichen Anforderungen an IT-Sicherheit ist bisher, soweit ersichtlich, nicht Gegenstand einer umfassenden Evaluierung gewesen.

Es besteht jedoch Grund zum Zweifel, wie am Beispiel der Anforderungen an die technischen und organisatorischen Maßnahmen nach § 9 BDSG aufgezeigt werden soll. Die Pflicht zur Datensicherheit nach § 9 BDSG ist, wie dargestellt, kumulativ durch behördliche Aufsicht und durch eine Haftung auf Schadensersatz, also durch formal starke Durchsetzungsmechanismen gesichert.

Beide Durchsetzungen haben keine oder allenfalls überwiegend geringe praktische Bedeutung. Ob es überhaupt jemals zur Zahlung von Schadensersatz nach § 7 BDSG oder nach § 823 Abs. 2 BGB wegen unzureichender technischer Maßnahmen kam, lässt sich nicht feststellen. Veröffentlichte Gerichtsentscheidungen zu dieser Frage gibt es, soweit erkennbar, nicht.

Die Beanstandung von Verstößen gegen die Anforderungen des § 9 BDSG nehmen in der Tätigkeit der Datenschutzaufsichtsbehörde, soweit erkennbar, eine vergleichbar geringe Bedeutung ein.

Dieser Befund mag jedenfalls teilweise eine Besonderheit des Datenschutzes sein. So wird die Leistungsfähigkeit der Haftungsandrohung nach § 7 BDSG und nach § 823 Abs. 2 BGB durch den Umstand geschwächt, dass materielle Schäden konkreter Betroffener durch Verstöße gegen Datenschutzbestimmungen nur schwer feststellbar sind. Entsprechend hat die Haftung nach § 7 BDSG nicht nur in Bezug auf Datensicherheit, sondern generell kaum praktische Bedeutung.[414]

Es ist aber zu bedenken, dass die Pflicht zur Datensicherheit nach § 9 BDSG angesichts des sehr weiten Bereichs der personenbezogenen Daten und der damit verbundenen allgemeinen Anwendbarkeit auf Datenverarbeitung in Unternehmen die bisher einzige, allgemein anwendbare gesetzliche Norm zur IT-Sicherheit darstellt, so dass Durchsetzungsdefizite dieser Anforderungen besonders gravierend sind.

5.4.3.1.6 Ergebnis

Als Ergebnis zeigt sich, dass die Regulierung von IT-Sicherheit durch Gesetz bisher allenfalls im Ansatz besteht. Eine allgemeine gesetzliche Regelung besteht nicht, auch wenn § 9 BDSG bzw. Parallelnormen in Landesdatenschutzgesetzen in Privatwirtschaft und Verwaltung flächendeckend anwendbar sind. Die zahlreichen Regeln zu Einzelbereichen sind recht heterogen.

Die praktische Bedeutung der Gesetzgebung zur IT-Sicherheit ist nicht sicher zu ermitteln. Die Eignung zur Prägung der Auffassung der Praxis über die notwendigen Maßnahmen ist zu bezweifeln. Es besteht insbesondere Anlass zur Annahme, dass Durchsetzungsdefizite bestehen, die jedenfalls im Bereich des § 9 BDSG – und damit der Norm zur IT-Sicherheit mit dem wohl breitesten Anwendungsbereich – unverkennbar sind.

5.4.3.2 Rechtsprechung

Die Rechtsprechung ist sowohl für die Formulierung materieller Anforderungen an IT-Sicherheit von Bedeutung als auch für die Durchsetzung gesetzlicher oder anderer (z. B. vertraglicher) Anforderungen von entscheidender Bedeutung.

412 Borges, in Borges/Meents, Cloud Computing (im Erscheinen 2015) § 12 Rn. 38; Borges/Schwenk/Stuckenberg/Wegener, Identitätsdiebstahl und Identitätsmissbrauch im Internet (2010) S. 207; Gabel, in Taeger/Gabel, § 7 Rn. 7; Klett/Lee, CR 2008, 644, 647; Quaas, in Wolff/Brink, BDSG, § 7 Rn. 48; i.E. auch Karg, in Wolff/Brink, BDSG, § 9 Rn. 119. A.A. Plath, in Plath, BDSG § 9 Rn. 19.

413 Gola/Klug/Körffer, in Gola/Schomerus, BDSG, § 1 Rn. 3; Karg, in Wolff/Brink, BDSG, § 9 Rn. 118; Simitis, in Simitis, BDSG, § 7 Rn. 68; Pauschal für alle Normen des BDSG: Däubler, in D/K/W/W, BDSG, § 7 Rn. 33; Gola/Klug/Körffer, in Gola/Schomerus, BDSG, § 7 Rn. 18b.

414 Borges, in Borges/Meents, Cloud Computing (im Erscheinen 2015) § 12 Rn. 40.

5.4.3.2.1 Materielle Anforderungen an IT-Sicherheit

Die Rechtsprechung setzt Normen in Bezug auf technische Anforderungen durch Auslegung allgemeiner Grundsätze oder spezifischer technischer Normen gesetzlicher oder untergesetzlicher Art. Hinsichtlich der Beiträge der Rechtsprechung für die Formulierung materieller Anforderungen an IT-Sicherheit ergibt sich ein heterogenes Bild.

Die Rechtsprechung ist vor allem mit der Formulierung von Verhaltensanforderungen und zu Organisationspflichten hervorgetreten. So hat der Bundesgerichtshof in den letzten Jahren mehrfach Pflichten des Internetnutzers zur Sicherung seiner technischen Infrastruktur formuliert. Beispiele sind etwa:

- Pflicht zur Absicherung eines privaten WLAN durch Passwort[415];
- Pflicht zur Verwendung von Virenschutzprogrammen[416];
- Pflicht zur sicheren Verwahrung von Authentisierungsmedien[417];
- Pflicht zur sicheren Verwahrung von Passwörtern im Online-Handel[418];

Weiterhin verlangt die Rechtsprechung, Angriffe durch sorgfältiges Verhalten abzuwehren und Rechtsverletzungen durch Angehörige zu verhindern, etwa durch:

- Pflicht zur Abwehr von Täuschungsversuchen im Online-Banking[419];
- Pflicht zur Instruktion minderjähriger Kinder über das Verbot von Filesharing.[420]

Bei der Formulierung konkreter technischer Anforderungen ist die Rechtsprechung zurückhaltend. Gleichwohl finden sich Einzelfälle durchaus wichtige Entscheidungen. So bezeichnete das Kammergericht in einer vielbeachteten Entscheidung die Nutzung des klassischen PIN/TAN-Verfahrens im Online Banking im Jahr 2008 wegen unzureichender Sicherheit als pflichtwidrig.[421]

Diese Zurückhaltung zeigt sich deutlich an der einflussreichen Grundsatzsatzentscheidung des BGH zur Absicherung privater WLAN von 2010.[422] Hier formulierte der BGH die Pflicht des WLAN-Betreibers, einen Passwortschutz vorzusehen und konkretisierte dies in zweierlei Hinsicht: Er verlangte, dass der Betreiber ein individuelles Passwort verwendet, und er verlangte Maßnahmen zum Schutz nach dem zum Zeitpunkt des Erwerbs gängigen Standards.[423] Eine Pflicht zur Anpassung der Sicherheit an den jeweiligen Stand der Technik lehnte der BGH hingegen ausdrücklich als unverhältnismäßig ab. Nähere Ausführungen Stand der Sicherheit vermied der BGH und beschränkt sich auf die Aussage, dass eine WPA 2-Verschlüsselung im Jahr 2006 noch nicht geboten gewesen sei.[424]

5.4.3.2.2 Schwierigkeiten der Regelung von IT-Sicherheit durch Rechtsprechung

Hinsichtlich der IT-Regulierung durch die Rechtsprechung ergeben sich einige spezielle Probleme und Fragen:

415 BGHZ 185, 330, 340 Rn. 34 – Sommer unseres Lebens; ebenso LG Berlin, MMR 2011, 401; LG Hamburg, MMR 2013, 322; AG Hamburg, Urt. v. 7.6.2011, 36 a C-71/11, BeckRS 2011, 23447. Siehe dazu auch Borges, NJW 2010, 2624; ders., NJW 2014, 2305; Borges/Schwenk/Stuckenberg/Wegener, Identitätsdiebstahl und Identitätsmissbrauch im Internet (2011), S. 272 ff.

416 LG Köln, MMR 2008, 259, 261; Borges, Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis, S. 146; Libertus, MMR 2005, 507, 509; Werner, Verkehrspflichten privater IT-Nutzer in Bezug auf die Verbreitung von Schadsoftware, S. 175. Koch, NJW 2004, 801, 806 nimmt eine solche Pflicht nur im b2c-Verhältnis an.

417 BGH, BKR 2004, 493, 494; BGHZ 145, 337, 340 f.; OLG Frankfurt, MMR 2009, 856, OLG Frankfurt, MMR 2008, 473; siehe dazu Borges, Verträge im elektronischen Geschäftsverkehr, 2. Aufl. (2007) S. 498; ders, Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis, S. 159 f.

418 BGHZ 180, 134 Rn. 16 – Halzband; siehe auch OLG Hamm, NJW 2007, 611, 612; LG Bonn, MMR 2002, 255; Borges, in Borges, Rechtsfragen der Internet-Auktion, 2, Aufl. 2013, S. 389 ff; ders., NJW 2011, 2400.

419 BGH, NJW 2012, 2422, 2424 Rn. 28; besprochen in Borges, NJW 2012, 2385, 2386 f; siehe auch LG Berlin, MMR 2012, 229; Bender, WM 2008, 2049, 2053 f..; Borges, NJW 2005, 3313, 3315; Erfurth, WM 2006, 2198, 2203; Maihold, in: Schimansky/Bunte/Lwowsky, Bankrechts-Handbuch, 4. Aufl. 2011, § 55 Rn. 121, 132.

420 BGH, NJW 2013, 1441, 1442 Rn. 24 – Morpheus.

421 KG, MMR 2011, 338, 339. Siehe dazu auch Borges, NJW 2012, 2385, 2388; Willershausen, jurisPR-BKR 10/2011, Anm. 4.

422 BGHZ 185, 330 – Sommer unseres Lebens. Siehe dazu auch Borges, NJW 2014, 2305, 2306; Brüggemann, CR 2013, 324, 327; Härting, Internetrecht, 2013, Rn. 2254; Hilbig-Lugani, LMK 2013, 347217; Hoffmann, MMR 2013, 391; Sesing, MMR-Aktuell 2013, 346040; Thora, VersR 2013, 868, 869.

423 BGHZ 185, 330, 340 Rn. 34 – Sommer unseres Lebens.

424 BGHZ 185, 330, 340 Rn. 33 – Sommer unseres Leben.

(1) Komplexität/Kompetenz der Gerichte

Im Hinblick auf die teilweise sehr große Komplexität technischer Aspekte stellt sich die Frage, ob Gerichte überhaupt über technisch komplexe Fragen, wie sie im Bereich der IT-Sicherheit häufig vorkommen können, angemessen entscheiden können.

In der Tat sind Gerichte zur Beurteilung komplexer technischer Sachverhalte regelmäßig auf Gutachter angewiesen. Dies ist freilich keine Besonderheit technischer Sachverhalte. In etlichen Bereichen, etwa dieser Fragen, werden zur Tatsache im Wege des Beweises Sachverständigengutachten herangezogen. Das gerichtliche Verfahren erlaubt es zudem beiden Seiten, im Rahmen ihres Vortrags auch Stellungnahmen von Experten durch Gutachten etc. einzubringen.

Durch diesen Weg kann Sachkunde auch zu technischen Fragen in Gerichtsverfahren eingebracht werden. Das Kernproblem dürfte eher darin liegen, dass dieser Weg der Klärung technischer Fragen – Einbeziehung von Gutachten in Gerichtsverfahren – mit hohen Kosten verbunden ist, die oft sehr einzelfallbezogen anfallen.

(2) Verfahrensdauer

Das gravierendste Problem gerichtlicher Entscheidungsfindung in Bezug auf IT-Sicherheit ist die Dauer dieses Normsetzungsprozesses. Die Praxis orientiert sich meist an obersten oder höchstrichterlichen Entscheidungen. Es ist zu beobachten, dass insbesondere in wichtigen Fragen die Wirtschaft die höchstrichterliche Entscheidung abwartet, bevor sie sich an diese anpasst. Die durchschnittliche Verfahrensdauer in Zivilprozessen bis zu einer Entscheidung des BGH dürfte aber fünf bis sechs Jahre betragen. Hinzu kommt, bezogen auf den zugrundeliegenden Fall, eine Zeitspanne zwischen dem Fall und Klageerhebung, die nach dem Eindruck des Verfassers bei etwa sechs bis zwölf Monaten liegt, aber auch durchaus länger dauern kann, bis zu, im Hinblick auf Verjährung, etwa drei Jahren.

Dies bedeutet in struktureller Hinsicht, dass eine IT-Regulierung durch die Rechtsprechung einen Zeitbedarf von mindestens sechs Jahren hat, die Praxis also durchaus sechs Jahre ohne verlässliche Regelung auskommen muss. Dieser Umstand ist bei schnell wechselnden technischen Aspekten überaus problematisch, da in einem Urteil Leitlinien für gegenwärtige Anforderungen nicht gezogen werden können, wenn sich die technische Grundlage zwischenzeitlich geändert hat.

Ein strukturelles Problem richterlicher Rechtsfindung im Zivilprozess liegt in der Parteiautonomie, konkret in der Bindung an die Prozessführung durch eine Partei (Dispositionsmaxime). Entsprechend dem Grundsatz „Wo kein Kläger, da kein Richter“, ist die Leistungsfähigkeit der Rechtsprechung zur Normsetzung stets schwach, wenn nur wenige Rechtstreitigkeiten durch ein Urteil beendet werden.

Gerade im Bereich der IT-Sicherheit ist die Zahl der (abgeschlossenen) Gerichtsverfahren, insbesondere die Zahl veröffentlichter Entscheidungen auffallend gering. Dies dürfte ebenso mit den hohen Kosten der Vorbereitung und Durchführung von Gerichtsverfahren in diesem Bereich und wohl auch mit dem Problem der Verfahrensdauer zusammenhängen. Der Mangel an Gerichtsentscheidungen führt aber dazu, dass die Rechtsprechung in Bezug auf konkrete technische Anforderungen im Bereich der IT-Sicherheit keinen nennenswerten Beitrag leistet.

5.4.3.2.3 Durchsetzung

Die Rechtsprechung ist grundsätzlich ein sehr starkes Instrument zur Durchsetzung normativer Anforderungen. Zwischen den Parteien eines Rechtsstreits kann die gerichtliche Entscheidung mit Zwang durchgesetzt werden. Die Wirkung geht aber weit darüber hinaus. Da die Gerichte sich an höchsten Entscheidungen orientieren, haben insbesondere höchstrichterliche Entscheidungen eine hohes Maß an prägender Kraft (Richterrecht).

Diese prägende Kraft von Urteilen ist umso stärker, desto häufiger die konkret entschiedene Frage auftritt. Folglich lässt diese Kraft nach, wenn sich die tatsächlichen Verhältnisse ändern und somit von einer Entscheidung nicht mehr auf einen gegenwärtigen Sachverhalt geschlossen werden kann.

Der Umstand, dass eine höchstrichterliche Entscheidung etwa sechs Jahre nach dem entsprechenden Sachverhalt erfolgt, führt angesichts des schnellen Wandels in der Informationstechnik dazu, dass eine Beachtung in der Praxis kaum erfolgen kann, weil vergleichbare Sachverhalte oft nicht mehr existieren.

5.4.3.2.4 Ergebnis

Als Ergebnis zeigt sich, dass die Rechtsprechung für die IT-Regulierung nur eingeschränkt geeignet ist. Sie ist leis-

tungsfähig für die Formulierung von Verhaltensanforderungen, aber, schon wegen der langen Verfahrensdauer und der hohen Kosten, kaum geeignet zur Normsetzung in Bezug auf technische Anforderungen. Auch ihre Eignung zur Durchsetzung ist bei technischen Anforderungen stark eingeschränkt, da sich aufgrund des schnellen technischen Wandels in der IT-Gerichtsentscheidungen oft nicht mehr auf gegenwärtige Sachverhalte übertragen lassen.

5.4.3.3 Behördliche Normsetzung und Kontrolle

Die klassischen Mittel zur Regulierung in der deutschen Rechtstradition sind Aufsicht und Kontrolle durch Behörden. Diese werden nicht zuletzt im Bereich der technischen Sicherheit eingesetzt. In vielen Branchen sind branchenspezifische Behörden mit Aufsichtsbefugnissen tätig. Diese Aufsicht erstreckt sich regelmäßig auch auf die technische Sicherheit von Produkten und Diensten. Daneben sind sektorübergreifende, fachspezifische Aufsichtsbehörden vorhanden, wie etwa die Aufsichtsbehörden für Datenschutz.

Entsprechend dieser Tradition ist der gegenwärtige Stand der behördlichen Kontrolle im Bereich der IT-Sicherheit durch eine starke Fragmentierung gekennzeichnet. Eine allgemeine Aufsicht für IT-Sicherheit besteht nicht. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) besitzt nach dem BSI-Gesetz weder Eingriffsbefugnisse, noch Befugnisse zur Formulierung verbindlicher technischer Anforderungen.

IT-Sicherheit wird daher derzeit ausschließlich von sektorspezifischen oder fachbezogenen Regeln erfasst.

Aufsichtsbehörden können durch unterschiedliche Maßnahmen materielle Anforderungen an IT-Sicherheit formulieren. Das klassische Mittel der Normkonkretisierung durch behördliches Handeln ist der Verwaltungsakt, in dem die gesetzlichen Anforderungen für einen konkreten Einzelfall konkretisiert werden. Diese Möglichkeit wird in der Praxis stark genutzt, etwa in der sektorspezifischen Aufsicht, wenn Genehmigungen wegen Sicherheitsmängeln versagt werden. Die Bindung der Betriebserlaubnis an eine Sicherheitsüberprüfung ist der breiten Öffentlichkeit vor allem durch die Hauptuntersuchung für Kfz nach § 29 StVZO (umgangssprachlich „TÜV“) vertraut. Bei Fehlen einer gültigen Prüfplakette kann gemäß § 29 Abs. 7 S. 4 StVZO der Betrieb des Kfz untersagt werden. In der Öffentlichkeit weniger bekannt ist das für die Sicherheit wesentliche Verfahren der Fahrzeugtypgenehmigungen. Zu unterscheiden sind insoweit die EU-weit geltenden EG-Fahrzeugtypgenehmigungen (Art. 3 ff. EG-FGV) sowie die nationale allgemeine Betriebserlaubnis (§ 20 StVZO). Mit einer Typgenehmigung bzw. allgemeiner Betriebserlaubnis bescheinigt das Kraftfahrtbundesamt (KBA), dass ein Fahrzeugtyp den erforderlichen Sicherheits- und Umweltanforderungen genügt.[425]

Die Bedeutung der IT-Sicherheit im Rahmen der behördlichen Sicherheitskontrolle und die maßgeblichen Anforderungen an IT-Sicherheit sind bisher jedoch oft unklar. Ein Beispiel ist etwa die Kontrolle von Kfz. Diese enthalten in hohem Umfang IT-Systeme, eine Verbindung zum Internet ist in aktuellen Modellen vorgesehen. Eine klare, einheitliche Linie der aufsichtsrechtlichen Anforderungen, etwa in Bezug auf die technische Absicherung des Internetzugangs, ist, soweit erkennbar, bisher noch nicht gefunden.

Ein besonders wichtiges Instrument für die Formulierung allgemeiner Anforderungen an IT-Sicherheit sind behördliche Regelwerke. Ein bekanntes Beispiel mit Bezug zur IT-Sicherheit sind die von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) formulierten MaRisk.[426] § 25a KWG verpflichtet Kreditinstitute zu einer ordnungsgemäßen Geschäftsorganisation. Dies schließt nicht zuletzt ein hinreichendes Risikomanagement ein. Die BaFin, die nach § 6 Abs. 1 KWG zur Aufsicht über Kreditinstitute nach den Vorschriften des KWG verpflichtet ist, konkretisiert durch die MaRisk die Anforderungen des § 25a KWG an eine ordnungsgemäße Geschäftsorganisation für Kreditinstitute.[427] Rechtlich sind die MaRisk als norminterpretierende Verwaltungsanweisungen einzuordnen[428] denen zwar kein Gesetzescharakter zukommt, die jedoch (Selbst-) Bindungswirkung für die Verwaltung haben.[429] Die MaRisk, die modular aufgebaut sind und regelmäßig aktualisiert

425 Siehe ausfürhlich zum Verfahren der Erteilung der EG-Farhzeugtypgenehmigung: Kraftfahrt-Bundesamt, Wegweiser zur EG-Fahrzeugtypengenehmigung nach der RL 2007/46/EG, 6.5.2009, abrufbar unter http://www.kba.de/DE/Fahrzeugtechnik/Zum_Herunterladen/ErteilungTypgenehmigungen/Wegweiser_pdf.pdf?__blob=publicationFile&v=4, zuletzt abgerufen am 21.05.2015.

426 Rundschreiben 10/2012 (BA) – Mindestanforderungen an das Risikomanagment – MaRisk.

427 Braun/Wolfgarten, in Boos/Fischer/Schulte-Mattler, KWG, § 25a Rn. 110; Spindler, in MüKo, AktG, § 91 Rn. 58.

428 Knierim, in Wabnitz/Janovsky, Handbuch des Wirtschafts- und Steuerstrafrechts, 5. Kap. Rn. 60; Spindler, in MüKo AktG, § 91 Rn. 42; Thalhofer, in Reinsdorff/Conrad, Beck'sches Mandatshandbuch IT-Recht. § 17 Rn. 211.

429 Braun/Wolfgarten, in Boos/Fischer/Schulte-Mattler, KWG, § 25a Rn. 110; Thalhofer, in Reinsdorff/Conrad, Beck'sches Mandatshandbuch IT-Recht. § 17 Rn. 211.

werden enthalten etwa in AT 7.2 technisch-organisatorische Anforderungen an IT-Systeme.[430] Allerdings sind diese behördlichen Regelwerke nur in einigen Bereichen bekannt und decken allenfalls einen Teil der Wirtschaft ab.

Ein weiteres Mittel zur Formulierung materieller Anforderungen an IT-Sicherheit sind Empfehlungen. Diese werden etwa von Datenschutzbehörden häufig genutzt. Schon wegen des breiten Geltungsbereichs des Datenschutzrechts in Verwaltung und Wirtschaft sind diese ist die Bedeutung von Empfehlungen von besonderem Interesse und können auch für I4.0 prägend sein.

Allerdings bleibt in allen Fällen unklar, inwieweit eine empfohlene Maßnahme rechtlich geboten ist. Daher sind Empfehlungen ggf. eine Leitlinie für die Konkretisierung gesetzlicher Anforderungen, stellen selbst aber noch keine Konkretisierung dar.

5.4.3.4 Vertragspraxis

Parteiautonomie, die Grundlage der sogenannten „Selbstregulierung", verwirklicht sich rechtlich vor allem durch Verträge, die für die Vertragspartner bindende Normen setzen, darüber hinaus durch einheitliche Vertragspraxis, die Entstehung von Gewohnheiten und Bräuchen. Wesentliche Treiber einer überindividuellen Selbstregulierung durch einheitliche Vertragspraxis sind Musterbedingungen, die etwa von anerkannten Institutionen herausgegeben und verwaltet werden. Die Abgrenzung zu anderen Formen der Selbstregulierung wie Kodizes, Zertifizierung und Handelsbrauch ist daher schwierig.

5.4.3.4.1 Materielle Anforderungen

5.4.3.4.1.1 Keine allgemeine Vertragspraxis zur IT-Sicherheit

Zur Existenz einer einheitlichen Vertragspraxis in Bezug auf IT-Sicherheit liegen keine gesicherten Erkenntnisse vor, da es an empirischen Untersuchungen fehlt. Es spricht aber alles dafür, dass jedenfalls eine flächendeckende, d.h. die Wirtschaftspraxis in allen relevanten Bereichen umfassende, einheitliche Vertragspraxis nicht besteht.

Die Leitfrage für das Bestehen wäre, ob es Standardklauseln für IT-Sicherheit gibt, die ähnlich wie eine Rechtswahl- und Gerichtsstandsklausel, zur Grundausstattung vertraglicher Beziehungen gehören. Dabei ist zu unterscheiden zwischen Verträgen mit konkretem IT-Bezug, etwa Outsourcing-Verträge, oder Verträge über IT-Dienste, wie etwa Cloud-Dienste, und sonstige Vertragsbeziehungen.

5.4.3.4.1.2 IT-Sicherheit in IT-Outsourcing und Cloud Computing-Verträgen

Selbst bei Verträgen über IT-Outsourcing oder Cloud-Verträgen gibt es heute, soweit erkennbar, noch keine einheitliche Vertragspraxis in Bezug auf IT-Sicherheit. Zwar ist die Bedeutung vertraglicher Maßnahmen zum Schutz der Daten und Rechtsgüter von Cloud-Nutzern erkannt. So enthalten etwa Rechtshandbücher zur Gestaltung von Cloud Computing-Verträgen teilweise umfangreiche Hinweise zur Gestaltung vertraglicher Regeln in Bezug auf Maßnahmen der IT-Sicherheit.[431]

Ebenso wird IT-Sicherheit in Musterverträgen zu IT-Dienstleistungen adressiert. In Musterverträgen für Auftragsdatenverarbeitungsverträge wird regelmäßig die Pflicht des Dienstleisters nach § 9 BDSG aufgenommen.[432] Der Bundesverband Materialwirtschaft, Einkauf und Logistik e.V. hat einen Mustervertrag zu SaaS veröffentlicht der eine Pflicht zur Wahrung des Stands der Technik vorsieht.

430 Braun/Wolfgarten, in Boos/Fischer/Schulte-Mattler, KWG, § 25a Rn. 111 f.

431 Umfassend etwa Meents, in Borges/Meents, Rechtshandbuch Cloud Computing, im Erscheinen 2015, § 4 Rn. 202–212. Siehe auch Conrad/Schultze-Melling, in Reinsdorff/Conrad, Beck'sches Mandats-Handbuch IT-Recht, § 2 Rn. 183 f.; Intveen/Hilber/Rabus, in Hilber, Handbuch Cloud Computing, Teil 2 Rn. 302-330.

432 Siehe etwa BITKOM, Mustervertragsanlage zur Auftragsdatenverarbeitung, Version 4.0, 2013, 3 3, abrufbar unter http://www.bitkom.org/files/documents/140109_Mustervertragsanlage.pdf; BITKOM, Beispielsvertrag für Application Service Providing, 2006, § 4.5, abrufbar unter http://www.bitkom.org/de/publikationen/38336_30774.aspx

Allerdings gehen die Regeln generalklauselartig meist nicht über einen Verweis auf § 9 BDSG oder eine, allgemeine Pflicht zur Sicherheit hinaus.[434]

Ein interessantes Indiz für das Fehlen einheitlicher Vertragsbedingungen ergibt sich aus dem Leitfaden „Vertragsgestaltung beim Cloud-Computing" der AG „Rechtsrahmen des Cloud Computing" vom März 2014 (der Vertragsleitfaden ist abrufbar unter www.trusted-cloud.de), der den Aspekt der Datensicherheit zwar nennt (Seite 21), aber letztlich nur unter dem Gesichtspunkt der Einhaltung gesetzlicher Anforderungen des Datenschutzes und des Strafrechts (§ 203 StGB) und keinerlei Hinweise auf eine vertragliche Klausel enthält.

Nach eigener Kenntnis der Verfasser besteht jedenfalls eine einheitliche Vertragspraxis im Sinne inhaltlich gleicher Vertragsklausen in Bezug auf IT-Sicherheit auch bei Cloud-Verträgen nicht.

5.4.3.4.1.3 Austausch- und Kooperationsverträge

Bei Austauschverträgen, etwa Kaufverträgen, sind spezifische Klauseln zur IT-Sicherheit nicht zu erwarten. Anders ist es bei Kooperationsverträgen, die eine längerfristige Kooperation zwischen IT-Systemen der Kooperationspartner regeln. Die Kooperation im Rahmen der I4.0 ist ein Musterbeispiel für eine solche Kooperation.

Bei solchen Kooperationsverträgen wäre nach der Sachlage – erhebliche Gefährdungslage für IT-Systeme – eine intensive vertragliche Gestaltung der erforderlichen Sicherheitsmaßnahmen zur erwarten. Tatsächlich lässt sich diese aber nicht feststellen. Gerade hier macht sich das Fehlen einer empirischen Untersuchung schmerzlich bemerkbar, da keine gesicherten Erkenntnisse über die Vertragspraxis vorliegen. Es spricht aber einiges dafür, dass es nicht nur an einer flächendeckenden, einheitlichen Vertragspraxis fehlt, sondern dass vielmehr in erheblichem Maße spezifische IT-Sicherheitsregeln fehlen. Stattdessen findet sich meist eine allgemeine Sorgfalts- und Haftungsregelung.

5.4.3.4.1.4 Gründe für das Fehlen einer einheitlichen Vertragspraxis

Über die Gründe für das Fehlen einer gesicherten Vertragspraxis zu materiellen Anforderungen an IT-Sicherheit kann derzeit mangels empirischer Untersuchungen nur spekuliert werden.

Unkenntnis/mangelnde Erfahrung mit IT-Sicherheit

Eine denkbare Ursache ist, dass die Bedeutung einer vertraglichen Vereinbarung von IT-Sicherheit noch nicht in hinreichendem Maße in der Praxis bekannt ist. Allerdings kann die Kenntnis der Bedeutung von IT-Sicherheit als allgemein bekannt vorausgesetzt werden, sodass man sich dem Bedarf an vertraglicher Regelung nicht verschließen sollte, wenn eindeutige sachliche Gründe bestehen und eine inhaltlich angemessene Regelung bekannt ist. Es ist daher zu vermuten, dass eher die Unsicherheit über die angemessene Regelung über IT-Sicherheit die Ursache ist.

Fehlende praktische Relevanz

Fehlende praktische Relevanz ist eine denkbare Ursache für das Fehlen vertraglicher Regelungen; zu IT-Sicherheit könnte die fehlende praktische Erfahrung relevant sein, da insoweit erhebliche Schwierigkeit hinsichtlich der Durchsetzung vertraglicher Anforderungen zur IT-Sicherheit besteht.

Bestehen gesetzlicher Standards

Über das Datenschutzrecht bestehen gesetzliche Anforderungen an IT-Sicherheit, sodass auch denkbar ist, dass die Parteien hierauf vertrauen. Da die gesetzliche Regelung nicht abdingbar ist, besteht insofern kein Bedarf an einer vertraglichen Regelung. Diese erscheint aber als alleiniger Grundsatz nicht plausibel, da Parteien auch bei zwingenden gesetzlichen Bestimmungen eine vertragliche Konkretisierung anstreben, soweit diese sinnvoll erscheint. Der Bedarf an einer Konkretisierung der gesetzlichen Vorschriften wiederrum ist, wie gesetzlich dargestellt, im Bereich der IT-Sicherheit sehr hoch.

Verhandlungsmacht

In wichtigen Fallgruppen werden die maßgeblichen Vertragsbedingungen einseitig vorgegeben, namentlich vom Anbieter einer IT-Dienstleistung. Hier darf es nicht überraschen, wenn spezifische Anforderungen an IT-Sicherheit nicht vertraglich geregelt werden.

Unklarheit über angemessene Anforderungen

Der vermutlich zentrale Grund für das Fehlen gesicherter oder gar einheitlicher Vertragspraxis zur IT-Sicherheit ist Unklarheit über die angemessenen vertraglichen Anforderungen. Zwar besteht zwischen Fachleuten der IT-Sicher-

434 So etwa die in den beiden vorherigen Fn. genannten Musterverträge.

heit, bei aller Divergenz im Detail, in vielen Bereichen ein Konsens über Grundfragen und fachlich empfehlenswerte Maßnahmen zur IT-Sicherheit. Es gibt aber auch bei Vertragsjuristen, soweit erkennbar, keinen Konsens darüber, welche vertraglichen Anforderungen in Bezug auf IT-Sicherheit sinnvoll sind. Dabei ist zu bedenken, dass es kaum Erfahrungen mit der praktischen Auswirkung vertraglicher IT-Sicherheitsbestimmungen gibt, sodass für die vertragliche Gestaltung die Kenntnis fehlt, welche Regelung sinnvollerweise getroffen werden sollte.

5.4.3.4.2 Durchsetzung

Bei vertraglichen Bestimmungen zu IT-Sicherheit steht das allgemeine Instrumentarium der Durchsetzung vertraglicher Pflichten zur Verfügung, das generell sehr stark ist. Die Erfüllung vertraglicher Pflichten kann in der ordentlichen Gerichtsbarkeit oder in Schiedsverfahren erzwungen werden. Vertragsstrafen oder andere Mechanismen können wirkungsstarke Durchsetzungsinstrumente darstellen.

Ob und inwieweit vertragliche Pflichten zur IT-Sicherheit in der Praxis durchgesetzt werden, lässt sich derzeit nicht zuverlässig feststellen. Insoweit bestehen dieselben Schwierigkeiten wie bei der Durchsetzung gesetzlicher Pflichten zur IT-Sicherheit.

Mangelnde Kenntnis

Es fehlt den Vertragsparteien regelmäßig an hinreichender Kenntnis über die Durchsetzung der IT-Sicherheit beim Vertragspartner, sodass Sicherheitsmängel regelmäßig nur im Zusammenhang mit Schadensfällen bekannt werden können.

Feststellung und Nachweis von Schäden

Oft ist es in der Praxis schwierig, Schäden und vor allem die Kausalität von Pflichtverletzungen für Schäden festzustellen. Allerdings sind in der Industrie sehr häufig auch konkrete Vermögensschäden feststellbar und nachweisbar, sodass sich, anders als etwa im Datenschutzrecht, dieses Problem wohl nicht in gleicher Schärfe stellt.

Mangelnder Nachweis einer Pflichtverletzung

Entscheidend dürfte die Schwierigkeit des Nachweises von Pflichtverletzungen sein. Ausgangspunkt einer Sanktion (auch Schadensersatz) ist grundsätzlich der Nachweis einer Pflichtverletzung. Diese ist in Bezug auf Mängel der IT-Sicherheit regelmäßig kaum möglich, da es meist über Kenntnisse über das konkrete Verhalten des Vertragspartners fehlt. Es ist zu vermuten, dass aus diesem Grund häufig Haftungsregeln, soweit sie überhaupt vereinbart werden oder auf zusätzlicher Grundlage bestehen, in Bezug auf IT-Sicherheit in der Praxis oft ins Leere laufen und daher Pflichten zur IT-Sicherheit nicht effektiv durchgesetzt werden können.

5.4.3.4.3 Zwischenergebnis

Als Ergebnis zeigt sich, dass die Vertragspraxis gegenwärtig nicht in der Lage ist, angemessene Maßnahmen zur IT-Sicherheit zu formulieren und effektiv durchzusetzen. Da die Ursachen derzeit nicht genau bekannt sind, sind weitere Untersuchungen zu diesen Aspekten dringend geboten.

Es lässt sich aber auch schon jetzt vermuten, dass vor allem drei Aspekte von Bedeutung sind: Die Unsicherheit über konkrete materielle Anforderungen, Unsicherheit über angemessene Pflichten in Bezug auf IT-Sicherheit und die fehlende Möglichkeit des Nachweises einer Pflichtverletzung für den Vertragspartner.

5.4.3.5 Institutionelle Regelwerke und Standards

5.4.3.5.1 Rechtliche Anforderungen durch technische Regelwerke

Das Bedürfnis der Praxis nach einheitlichen Normen wird häufig durch technische Regelwerke erfüllt, die von einer Institution herausgegeben und verwaltet werden. Ein sehr bekanntes und in der Praxis überaus erfolgreiches Beispiel ist die Vergabe- und Vertragsordnung für Bauleistungen (VOB), ein von der Praxis erarbeitetes Regelwerk. Die VOB wird heute von der DIN im Auftrag des Deutschen Vergabe- und Vertragsausschusses für Bauleistungen (DVA) herausgegeben.[435] Die technischen Normen, die im Teil C aufgeführt sind, sind zugleich DIN-Normen.[436]

435 http://www.vob-online.de/cn/bGV2ZWw9dHBsLXZvbGx0ZXh0JmFydGlkPTMwMDQ4ODkzJnBhZ2VpZD0xJmxhbmd1YWdlaWQ9ZGU*.html#d1ca827d:d1ca827d, zuletzt abgerufen am 26.05.2015.

436 http://www.vob-online.de/de/artikel/hinweis-teil-c, zuletzt abgerufen am 26.05.2015.

Den Regelwerken sind Standards vergleichbar. Standards haben im Bereich der Regelung von Technik als technische Normen, wie DIN- oder ISO-Normen, eine große technische und immense praktische Bedeutung.

Die große Stärke technischer Normen liegt in der Herausbildung einheitlicher Anforderungen, sofern sie innerhalb der maßgeblichen Verkehrskreise anerkannt sind und zugrunde gelegt werden.

Institutionelle Regelwerke und Standards könne auch rechtliche Bindung erzeugen. Die für die Praxis wohl wichtigste rechtliche Bedeutung von Standards und Regelwerken hat deren Bindung durch vertragliche Einbeziehung. So wird etwa Teil B der VOB (VOB/B)[437] regelmäßig in Verträge über Bauleistungen vertraglich einbezogen.[438]

Derartige Regelwerke sind aus vertragsrechtlicher Sicht grundsätzlich allgemeine Geschäftsbedingungen, die entsprechend der AGB-Kontrolle unterliegen.[439] Die AGB-Kontrolle kann aber dadurch wesentlich gemildert werden, dass die einzelnen Klauseln keiner Inhaltskontrolle nach § 307 BGB unterliegen. Für Verträge zwischen Unternehmern ist dies in § 310 Abs. 1 S. 3 BGB für die VOB/B ausdrücklich geregelt. Diese gesetzliche Privilegierung ist jedoch an die Voraussetzung geknüpft, dass die VOB/B ohne inhaltliche Abweichungen insgesamt einbezogen ist. Da in der Praxis die meisten Verträge Abweichungen vorsehen, kommt der Ausnahme somit nur geringe praktische Bedeutung zu.[440] Gegenüber Verbrauchern besteht eine solche Privilegierung entgegen der früheren Rechtsprechung[441] ohnehin nicht.[442]

Daneben können Standards enorme Bedeutung für die Konkretisierung rechtlicher Anforderungen haben. Dies gilt insbesondere im Bereich der Technik und nicht zuletzt für sicherheitsbezogene Aspekte. So wird, wie dargestellt, der Begriff des „Standes der Technik“ im Zusammenhang mit sicherheitsbezogenen Pflichten von Gerichten häufig durch Rückgriff auf Standards konkretisiert.

5.4.3.5.2 Materielle Anforderungen an IT-Sicherheit

Standards haben im Bereich der konkreten materiellen Anforderungen an IT-Sicherheit derzeit wohl die größte Bedeutung, auch wenn sie nicht flächendeckend vorhanden sind.

Große Bedeutung haben ISO-Normen, namentlich die ISO 270xy-Familie. Der bekannte ISO/IEC 27001-Standard[443] spezifiziert die Anforderungen an ein Informationssicherheitsmanagementsystem. Die Anforderungen sind generisch und passen daher auf Organisationen unabhängig von Größe und Tätigkeitsfeld.[444] Die Einhaltung der ISO/IEC 27001 wird etwa vom BSI zertifiziert.[445] Darauf aufbauend enthält der Standard ISO/IEC 27002[446] weitergehende Empfehlungen für Standards in der Informationssicherheit sowie für das Informationssicherheitsmanagement.[447]
In Deutschland hat auch der BSI-Grundschutz Bedeutung. Der BSI-Grundschutz bietet nach Auffassung des BSI eine einfache Möglichkeit dem Stand der Technik entsprechende Sicherheitsmaßnahmen zu erkennen und umzusetzen.[448] Der BSI-Grundschutz besteht aus verschiedenen Werkzeugen, z. B. den IT-Grundschutz-Katalogen[449] und den IT-Grundschutzstandards.[450] Der BSI-Grundschutz differenziert dabei zwischen den drei Schutzniveaus „Normal“, „Hoch“ und „Sehr Hoch“.[451]

437 Vergabe und Vertragsordnung für Bauleistungen, Teil B: Allgemeine Bestimmungen für die Ausführung von Bauleistungen, 2012.
438 Dammann, in Wolf/Lindacher/Pfeiffer, 5. Teil Rn. B 162; Hänsel, in Graf von Westphalen, Teil „Klauselwerke“, Bauvertrag Rn. 4.
439 Zu den VOB/B: BGHZ 178,1, 4 Rn. 10; Dammann, in Wolf/Lindacher/Pfeiffer, 5. Teil Rn. V 403 ff.
440 Hänsel, in Graf von Westphalen, Teil „Klauselwerke“, Bauvertrag Rn. 16.
441 BGHZ 86, 135, 142.
442 BGHZ 178,1, 6 Rn. 22 ff.; Dammann, in Wolf/Lindacher/Pfeifer, 5. Teil, Rn, V 410.
443 ISO/IEC 27001: 2013. Information Technology – Security techniques – Information security management systems – Requirements.
444 http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534, zuletzt abgerufen am 26.05.105.
445 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzZertifikat/itgrundschutzzertifikat_node.html, zuletzt abgerufen am 26.05.2015.
446 ISO/IEC 27002:2013. Information Technology – Security techniques – Code of practice for information security controls, 01.10.2013, zuletzt abgerufen am 26.05.2015.
447 http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54533, zuletzt abgerufen am 26.05.2015.
448 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html, zuletzt abgerufen am 26.05.2015.
449 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html, zuletzt abgerufen am 26.05.2015.
450 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html, zuletzt abgerufen am 26.05.2015.
451 Siehe BSI-Standard 100-2, IT-Grundschutz-Vorgehensweise, S. 49 ff., abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf.pdf?__blob=publicationFile, zuletzt abgerufen am 26.05.2015.

Allerdings ist derzeit unklar, welche Bedeutung Standards zur IT-Sicherheit in der Praxis derzeit tatsächlich haben. Es fehlt an empirischen Untersuchungen zur Verbreitung der Standards durch Bezugnahme in Verträgen. Mangels Gerichtsentscheidungen (siehe dazu oben) kann auch nicht durch Auswertung der Rechtsprechung ermittelt werden, welche Bedeutung den Standards tatsächlich zukommt.

Die Standards haben spezifische Schwächen. So gilt der BSI-Grundschutz als sehr aufwendig. In der Tat fehlt es an einem Standard für einen Basisschutz, der auch für KMU leicht umsetzbar wäre. Dies gilt insbesondere für Marktteilnehmer, die nicht IT-Leistungen anbieten, sondern IT lediglich als Nutzer verwenden. Für diese Gruppe, die den Großteil der Unternehmen umfasst, ist ein Standard mit verständlichen, klaren Sicherheitsanforderungen nicht vorhanden. Dies hat auch für I4.0 große Bedeutung, da hier vielfach Unternehmen eingebunden sind, deren Kernkompetenz außerhalb der IT liegt und die in Bezug auf IT-Sicherheit gewöhnliche Nutzer sind.

5.4.3.5.3 Rechtliche Durchsetzung

Standards verfügen nicht über eigenständige Durchsetzungsmechanismen. Daher können sie nicht allein, sondern nur im Zusammenwirken mit anderen Instrumenten eine Regulierung bewirken, wie etwa durch Einbeziehung in einen Vertrag oder Selbstbindung (Kodex), durch Konkretisierung gesetzlicher Normen durch die Rechtsprechung, durch Verwaltungsakte von Behörden oder auch durch Verweise des Gesetzgebers.

Die rechtliche Durchsetzung von Anforderungen an IT-Sicherheit durch Standards ist bisher, soweit ersichtlich, nicht systematisch erforscht worden. Die praktische Erfahrung belegt, dass Standards insbesondere durch vertragliche Bezugnahme auch rechtlich bindend werden. Allerdings ist unklar, ob dies flächendeckend der Fall ist. Da für I4.0 solche Standards fehlen, ist zu vermuten, dass Standards insbesondere nur in Teilbereichen Bedeutung haben. In der Praxis verlangen Kooperationspartner einer Industrie-Kooperation in ihren Kooperationsverträgen teilweise Sicherheit nach Maßgabe von ISO-Normen oder nach BSI-Grundschutz. Dies ist aber nicht flächendeckend der Fall. Insbesondere lässt, sich, wie dargestellt, nicht feststellen, dass Musterverträge regelmäßig eine Konkretisierung der IT-Sicherheitsanforderungen anhand von ISO-Normen oder BSI-Grundschutz vorsehen.

5.4.3.6 Kodizes/Selbstbindung

Den institutionellen Regelwerken verwandt sind Kodizes, die ebenfalls ein Mittel der Selbstregulierung sind. In Bezug auf die materiellen Anforderungen sind Kodizes den institutionellen Regelwerken vergleichbar, funktional wohl identisch. Im Unterschied zu Regelwerken, die auf eine vertragliche Einbeziehung abzielen, setzen Kodizes typischerweise auf eine Selbstbindung durch einseitige Erklärung, den Kodex befolgen zu wollen.

Kodizes sind nicht per se mit Durchsetzungsinstrumenten ausgestattet. Sie können mit diesen verbunden werden etwa durch Zertifizierung, oder durch gesetzliche Regeln, wie etwa im Gesellschaftsrecht durch die Erklärungspflicht in Bezug auf den Corporate Governance Kodex nach § 161 AktG.

Im Bereich der IT-Sicherheit haben Kodizes, soweit erkennbar, bisher keine nennenswerte Bedeutung. Zwar sind in der Praxis einheitliche Regeln innerhalb von Unternehmensgruppen weit verbreitet. Das Datenschutzrecht beispielsweise enthält auch Ansätze, dies zu fördern, etwa durch das Institut der verbindlichen Unternehmensregeln (binding corporate rules). Dies sind aber eben keine allgemeinen Kodizes. Branchenübergreifende Kodizes zur IT-Sicherheit existieren, soweit erkennbar, nicht.

Dies bedeutet nicht, dass Selbstbindungsmaßnahmen im Bereich der IT-Sicherheit ohne Bedeutung wären. Ganz im Gegenteil, diese haben im Zusammenhang mit der Zertifizierung ganz erhebliche praktische Bedeutung. Darüber hinaus könnte Kodizes künftig wesentlich größere Bedeutung im Bereich der IT-Sicherheit zukommen. So findet die Selbstregulierung im Bereich des IT-Rechts in jüngster Zeit vermehrt Unterstützer.[452] Nach Art. 38 Abs. 1 der geplanten Datenschutzgrundverordnung[453] soll die Ausarbeitung von Verhaltensregeln (Code of Conduct), welche die besonderen

452 Siehe Selbstregulierung Informationswirtschaft e.V., Chancen und Voraussetzungen effektiver Selbst- und Ko-Regulierung zur Förderung des Verbraucherschutzes und des Datenschutzes in der digitalen Welt, Positionspapier, Mai 2014, abrufbar unter http://gis-service.it2media.de/images/pdf/Broschueren/140521_SRIW_Positionspapier_Selbst-_und_Ko-Regulierung_v03.pdf; Spindler/Thorn, Eckpunkte einer digitalen Ordnungspolitik, Politikempfehlungen zur Verbesserung der Rahmenbedingungen für eine effektive Ko-Regulierung in der Informationsgesellschaft, 14.04.2015, abrufbar unter http://gis-service.it2media.de/images/pdf/Spindler_Thorun-Eckpunkte_digitale_Ordnungspolitik_final.pdf

453 Rat der europäischen Union, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), 19.12.2014, 15395/15, 2012/0011(COD), abrufbar unter http://data.consilium.europa.eu/doc/document/ST-15395-2014-INIT/en/pdf

Anforderungen von Kleinst-, Klein- und mittleren Unternehmen berücksichtigen, von staatlicher Seite gefördert werden.

5.4.3.7 Zertifizierung

5.4.3.7.1 Zertifizierung in der Technikregulierung

Zertifizierungsverfahren können ein Mittel zur Technikregulierung sein und werden in großem Umfang eingesetzt. Die Spannbreite von Zertifizierungen ist extrem weit und umfasst umfangreiche, gesetzlich angeordnete technische Prüfungen ebenso wie Qualitätsaussagen oder Bewertungen beliebiger Art nach eigenen Kriterien des Bewertenden.

Zertifizierung ist für die Regulierung von Sicherheit in der Technik von erheblicher Bedeutung. Dabei ist der Zusammenhang von rechtlicher Regulierung und Zertifizierung durchaus vielfältig. Das Gesetz kann eine Zertifizierung anordnen, wie es etwa bei der Überprüfung von Kraftfahrzeugen nach § 29 StVZO der Fall ist. Im Bereich der IT-Sicherheit schreibt etwa das De-Mail-Gesetz für De-Mail-Anbieter eine Zertifizierung vor. So kann gemäß § 18 Abs. 3 Nr. 3 De-Mail-Gesetz der Nachweis über die Erfüllung der technischen und organisatorischen Anforderungen nur durch Testate des BSI erbracht werden. Weiterhin kann nach § 18 Abs. 3 Nr. 4 De-Mail-Gesetz der Nachweis der Erfüllung der datenschutzrechtlichen Anforderungen nur durch ein Zertifikat des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erbracht werden.

Das Gesetz kann aber auch indirekte Anreize zur Zertifizierung setzen, indem das Vorhandensein eines Zertifikats zur Voraussetzung für eine Rechtsfolge gemacht wird, die den Inhaber des Zertifikats oder Dritte, etwa Kunden des Zertifikatsinhabers, begünstigt. Ein interessantes Beispiel, das auch für I4.0 von Bedeutung ist, betrifft die Zertifizierung im Bereich der Auftragsdatenverarbeitung (dazu unten). Hier wird die künftige Datenschutz-Grundverordnung möglicherweise eine Bezugnahme auf Zertifizierungen rechtlich begünstigen.

Im Bereich der IT-Sicherheit fehlt es bisher weitgehend an allgemeinen rechtlichen Regelungen in Bezug auf Zertifizierungen. Zertifizierungen haben durchaus Bedeutung im Bereich der IT, auch in Bezug auf IT-Sicherheit. So werben viele Anbieter von IT-Diensten mit Zertifizierungen, etwa nach ISO/IEC 27001.

5.4.3.7.2 Materielle Anforderungen an IT-Sicherheit

Ein wesentliches Problem der Regulierung von IT-Sicherheit betrifft die materiellen Anforderungen. Derzeit werden im Rahmen von IT-Sicherheitszertifizierungen häufig eigene Standards der Zertifizierer verwendet, die nicht veröffentlicht sind. Es besteht daher häufig keine Transparenz über die Prüfanforderungen.

Insbesondere wegen der fehlenden Transparenz haben Zertifikate derzeit wohl kaum mehr als einen Werbeeffekt. Insbesondere ist eine Bezugnahme von Gesetzen auf derartige Zertifizierungen ausgeschlossen; ausgeschlossen, solange keine Klarheit über die materiellen Prüfanforderungen besteht.

Ein weiteres Problem stellt die fehlende Einheitlichkeit des Prüfgegenstands dar. Dies wird sehr deutlich an den ISO-Standards. Der Standard ISO/IEC 27002 enthält zwar umfassende und recht detaillierte Anforderungen an die IT-Sicherheit, die auch Grundlage einer Zertifizierung sein könnte, versteht sich selbst aber nicht als Prüfstandard. Im System der ISO-Zertifizierung wird der Prüfgegenstand im Einzelfall durch den Anwendungsbereich (Scope) der Prüfung definiert. Daher kann ein ISO/IEC 27001-Zertifikat für äußerst unterschiedliche Prüfgegenstände erteilt werden.

Das BSI bietet eine ISO/IEC 27001 Zertifizierung auf Basis von BSI-Grundschutz an.[454] Neben den Anforderungen von ISO/IEC 27001 deckt diese die Anforderungen der BSI-Standards und der IT-Grundschutz-Kataloge ab.[455] Rechtliche Grundlage für Zertifizierungen durch das BSI ist § 9 BSI-Gesetz. Daneben werden ISO-Zertifizierungen aber auch von zahlreichen Prüfunternehmern, letztlich nach eigenen Prüfanforderungen, durchgeführt.

5.4.3.7.3 Durchsetzung

Die Zertifizierung ist, wie dargestellt, als solches kein Instrument zur Durchsetzung von Normen, kann aber im Bereich der Selbstregulierung Bedeutung haben und durch Gesetz gefördert werden.

454 BSI, Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz. Zertifizierungsschema, Version 1.2, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/ISO27001/Zertifizierungsschema.pdf?__blob=publicationFile

455 BSI, Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz. Zertifizierungsschema, Version 1.2, S. 4.

IT-Sicherheits-Zertifizierungen erfolgen derzeit, außerhalb der engen Ausnahmen, regelmäßig ohne gesetzliche Anordnung oder sonstige rechtliche Pflicht. In Ausnahmefällen bestehen gesetzliche Anreize zur Zertifizierung. So gilt nach § 4 Abs. 2 Landesdatenschutzgesetz Schleswig-Holstein, dass Produkte, die über ein Datenschutzgütesiegel des ULD nach der Datenschutzgütesiegel-Verordnung Schleswig-Holstein verfügen, „vorrangig eingesetzt" werden sollen. Gerade diese Ausnahmen machen deutlich, dass derzeit keine flächendeckenden gesetzlichen Anreize zur Zertifizierung im Bereich von IT-Sicherheit bestehen.

5.4.3.7.4 Ergebnis

Zertifizierungen haben im Bereich der IT-Sicherheit große praktische Bedeutung. Jedoch ist das Potential dieses Instruments zur Förderung von IT-Sicherheit bei weitem nicht ausgeschöpft. Im Bereich der materiellen Anforderungen fehlt es weitgehend an transparenten und einheitlichen Prüfstandards. Ebenso sind Durchsetzungsinstrumente, wie sie in anderen Bereichen üblich sind, nicht verfügbar. Dies beruht jedenfalls in Bezug auf gesetzliche Anforderungen unmittelbar auf dem Fehlen einheitlicher Prüfstandards. Derzeit liegt ein wesentliches Potential für Regulierung von IT-Sicherheit brach.

5.5 Zwischenergebnis

Die Betrachtung des Standes der Technik hinsichtlich der relevanten technischen Sicherheitsmaßnahmenpakete *Inbetriebnahme in sicherer Konfiguration, Fernwartung, Absicherung von Feldgeräten und Netzen, Datensicherung, Schutz vor Schadsoftware, Härtung, Patchmanagement, Authentisierung, Zugriffskontrolle, Protokollierung/Auswertung und mobile Datenträger* hat ergeben, dass diese vorrangig auf die Security derzeitiger Industrieanwendungen und ICS abzielen und grundsätzlich einen guten Basisschutz für ICS, auch im Kontext von I4.0, bilden können. Dieser Basisschutz ist jedoch nach entsprechender Risikoanalyse immer in Abhängigkeit von der jeweiligen Sicherheitsarchitektur zu betrachten und umzusetzen. Die Analyse hat jedoch auch ergeben, dass viele Hindernisse bei der Implementierung einzelner Maßnahmen im Kontext von ICS in I4.0 entsprechend der Fallbeispiele auftreten können, die eine Eignung in bestimmten Teilaspekten in Frage stellen. Die Gründe für diese Hindernisse bei der Implementierung von technischen IT-Sicherheitsmaßnahmen bezogen auf I4.0 sind vielfältig. Sie beginnen bei Herstellerstandards und -Interessen , einer durch etablierte Vorgehens- und Denkweisen schwierigen Einführung von Patchmanagement und IAM und enden bei einer gewollten Höherpriorisierung von Verfügbarkeitsanforderungen aufgrund von Safety-Gesichtspunkten da integrierte Ansätze hinsichtlich Safety und Security fehlen. Spezifische Produkte sind für bestimmte Maßnahmen wie Firewalls und Whitelisting vorhanden, für einige Maßnahmen gibt es jedoch Stand heute keine entsprechenden am Markt verfügbaren Produkte oder gar vollumfängliche Konzepte, oft nur in Projekten für bestimmte Umgebungen und Kunden geschaffene Speziallösungen. Es wurden die entsprechenden Aspekte und Felder identifiziert in denen Bedarf an der Förderung von Produktisierung vorhandener Konzepte oder Erarbeitung neuer Konzepte besteht.

Es hat sich gezeigt, dass viele der organisatorischen Sicherheitsmaßnahmen, die heute für das industrielle Umfeld empfohlen und dort auch vielfach bereits umgesetzt sind, auch für die I4.0 geeignet sind. Es ist allerdings zu beachten, dass durch die Überwindung von Unternehmensgrenzen zahlreiche neue Schnittstellen entstehen und neue Prozesse etabliert werden müssen. Diese müssen jeweils einzeln für sich und für ihre Auswirkungen auf andere Prozesse hin untersucht werden, um geeignete organisatorische Maßnahmen vornehmen zu können. Die Gefahren, die von einer fehlenden oder mangelhaften Umsetzung der Maßnahmen ausgehen, sind im I4.0-Kontext allerdings als deutlich größer einzuschätzen, zumal es mehr Akteure im Wertschöpfungsnetzwerk gibt und zwischen diesen eine wesentlich größeren Menge an sensiblen Daten (und Unternehmensgeheimnissen) ausgetauscht wird.

Aus der rechtlichen Perspektive ist deutlich geworden, dass die Fragestellungen, die derzeit in der juristischen Literatur vermehrt betrachtet werden (v.a. Datenschutz), nur teilweise die faktischen Probleme der KMU bei der Umsetzung von I4.0 betreffen: Vordringlich sind hier strukturelle Maßnahmen im Rechtsraum nötig, um Unsicherheiten über konkrete Anforderungen zu beseitigen, wirksame Durchsetzungsmechanismen zu schaffen, zu einer einheitlichen Vertragspraxis zu gelangen und Standards und Zertifikate zu etablieren auf deren Basis die Unternehmen ihre Leistungen anbieten und weiterentwickeln können.

6. Vorhandene und neuartige Sicherheitskonzepte

Dieses Kapitel dient der Identifizierung bzw. Entwicklung geeigneter Konzepte zur Erzielung eines angemessenen Schutzniveaus in Industrie 4.0 (I4.0). Dabei werden sowohl Überlegungen zu gänzlich neuen Konzepten angestellt, als auch zur Übertragbarkeit existierender Konzepte aus anderen Anwendungsfeldern.

Zunächst wird in Abschnitt 6.1 auf technische Aspekte eingegangen, wie z. B. der Frage nach dem Eigentum, dem Zugriff auf und der Nutzung von Daten, die in einem Produktionsprozess verarbeitet werden, aber von verschiedenen Akteuren erzeugt oder verarbeitet werden. Der Schwerpunkt liegt dabei auf neuartigen IT-Sicherheitsarchitekturen für I4.0-Szenarien, dem Schutz von Prozess-Know-how und geistigem Eigentum sowie Digital Rights Management (DRM) für Produktions- und Maschinendaten. Die Auswahl von Konzepten geschieht insbesondere im Hinblick auf die in Kapitel 5 identifizierten offenen Problemstellungen. Beispielhaft sei hier der Einsatz von Werkzeugmaschinen genannt, die Bestandteil von Produktionsprozessen sind und dabei verwertbare Daten erzeugen, die sowohl dem Werkzeugmaschinenhersteller, als auch dem Produktionsprozess-Besitzer zugeschrieben werden können.

In Abschnitt 6.2 werden Konzepte zur Überwindung organisatorischer Hemmnisse vorgestellt. Dabei werden die in Kapitel 5.3 identifizierten organisatorischen Implementierungshemmnisse als Ausgangspunkt verwendet, um Konzepte und organisatorische Ansätze zur Umgehung von derartigen Hinderungsgründen zu entwickeln. Dies geschieht besonders im Hinblick auf die Bedürfnisse und Ressourcen kleinerer und mittlerer Unternehmen.

Es folgt eine rechtliche Betrachtung in Abschnitt 6.3. Dabei wird auf Grundlage der gefundenen wesentlichen Risiken aus rechtlicher Sicht sowie aus Sicht der IT-Sicherheit nach Lösungen und Auswegen gesucht, um die rechtlichen Risiken zu minimieren und dabei auch wesentliche Aspekte der IT-Sicherheit zu berücksichtigen. Basierend auf den gefundenen Lösungen werden Konzepte entwickelt, welche die wesentlichen Risiken aus rechtlicher Sicht, wie bspw. bestimmte vertragliche Gestaltungen, Zertifizierungen oder Ähnliches, minimieren können. Dabei werden auch gesetzgeberische Maßnahmen, wie z. B. das IT-Sicherheitsgesetz betrachtet. Abschließend wird eine Bewertung der Konzepte mit Blick auf ihre Eignung zur Risikominimierung vorgenommen.

Am Ende des Kapitels erfolgt eine Bewertung der relevanten Standards und Normen (Abschnitt 6.3).

6.1 Konzepte zur Erzielung eines angemessenen Schutzniveaus

Das angemessene Schutzniveau von I4.0-Anlagen wurde eng in Anlehnung an konkrete Sicherheitsbedarfe der Industrie ermittelt. Dazu wurden, wie in Kapitel 4 dargestellt wird, die Fallbeispiele „Automobilbau“, „Anlagen- und Maschinenbau“, „Chemische Industrie“ sowie „grenzüberschreitende Logistik“ analysiert und auf IT-Sicherheitsaspekte hin bewertet. Darüber hinaus wurde eine Extrapolation der Erkenntnisse in Richtung für I4.0 zu erwartende Anpassungen erzeugt. Die hier identifizierten Aspekte wurden dazu in ein so genanntes Teilnehmer- und Kommunikationsmodell übergeführt. Parallel wurde eine Methodik beschrieben, mittels derer man entsprechende Bedrohungs- und Risikomodellierungen für alle Fallbeispiele erzeugen kann. Dieses so genannte Referenzmodell, also Teilnehmer- und Kommunikationsmodell sowie Risiko- und Bedrohungsmodell, wird in Kapitel 4.2 entsprechend dargestellt.

Die Operationalisierung der Modelle auf die Fallbeispiele führt zu einem Spektrum von Bedrohungen, die im Abschnitt 4.5.1.5.4 auf die Domänen „Rechenzentrumsbetrieb“, „Internetkommunikation“, „Maschinenbetreiber“, „Maschinenhersteller“ und „Fernwartungsdienstleister“ abgebildet wurden.

Die identifizieren Aspekte wurden entsprechend der Vorgaben des ICS-Kompendiums des Bundesamts für Sicherheit in der Informationstechnik (BSI) auf verfügbare und angemessene Gegenmaßnahmen hin analysiert und bewertet. Als Ergebnis liegt eine Matrix vor[456], welche die gegenwärtigen Lücken bezüglich der IT-Sicherheitsbedrohungen sowie Hemmnisse bei der Umsetzung der etablierten Maßnahmen aufzeigt (siehe Kapitel 5).

Nachfolgend werden neue konzeptionelle Ansätze zur Lösung der technischen Hemmnisse und damit zur Erreichung eines angemessenen Sicherheitsniveaus vorgestellt und diskutiert, die sowohl die Lücken des ICS-Kompendiums adressieren, als auch die erweiterten Ansprüche von I4.0 berücksichtigen.

456 Siehe Kreuztabelle ICS-Security im Anhang.

6.1.1 Industrial Rights Management

I4.0 wird nur Wirklichkeit werden, wenn Unternehmen ihre wirtschaftlichen Interessen wahren können. Besonders wichtig sind den Unternehmen dabei der Schutz von Know-how und die Kontrolle von Nutzungsrechten in der industriellen Produktion.

Die fortschreitende Anbindung von Produktionsumgebungen an Datennetze, z. B. durch die Integration von Produktions- und Verwaltungs-IT, trägt dazu bei, dass IT-Sicherheitsrisiken aus dieser Welt in die Produktion Einzug halten. Industrielle Komponenten, Prozesse und Daten werden zu attraktiven Zielen für Angreifer.

Schon heute existieren globale Wertschöpfungsnetzwerke, in denen Betreiber einer Produktionsanlage und Produktdesigner nicht mehr Teil desselben Unternehmens sein müssen. Einige Werkzeugmaschinenhersteller liefern bereits Produktionskomponenten, die ganze Teilfertigungszyklen innerhalb einer Werkzeugmaschine umsetzen, ohne dass der Produzent hier mehr als die Fabrikationsdaten bereitstellt. Zukünftig werden diese Kooperationen zwischen den Akteuren sehr viel agiler gestaltet werden. Möglicherweise produzieren Maschinen im Produktionsumfeld eines Produzenten auch Teile, die an andere Kunden geliefert werden. Es gilt daher zu verhindern, dass Intellectual Property (IP) wie Produktions-Know-how oder Produktdesign, in falsche Hände gelangt. Diese Daten müssen dem Grunde nach schon heute geschützt werden, im I4.0-Szenario wird der Schutz dieser Daten unerlässlich, da dann der Perimeterschutz der Anlagen nicht mehr die erforderliche Sicherheit bieten kann.

Wir unterscheiden an dieser Stelle zwischen Produktionsdaten und Fabrikationsdaten. Die Produktionsdaten sind zum einen Konstruktionsdaten, die z. B. als Computer Aided Design (CAD) Daten aus einem Konstruktionsprozess abgeleitet werden, und sich auf der anderen Seite mit den Datensätzen aus den klassischen Enterprise Ressource Programmen (ERP) verschneiden. Sie werden typischerweise auf Office-IT-Systemen verarbeitet und gespeichert. Mit dem Begriff Fabrikationsdaten umschreiben wir im Folgenden alle Daten ab der Manufacturing Execution System (MES) Ebene der Automatisierungspyramide bis hinunter zu den Speicherprogrammierbaren Steuerungen (SPS) der Produktionslinien. Sie enthalten also nur die notwendigen Steuerdaten und ggf. begleitenden Informationen, welche zur Ausführung eines Fertigungsauftrages innerhalb einer Produktionsanlage vorliegen und werden dort typischerweise auch gespeichert. Sowohl Produktions- als auch Fabrikationsdaten enthalten potenziell sensible Daten und müssen daher gleichermaßen geschützt werden.

Während für Produktionsdaten verschiedene Schutzkonzepte in Form kommerzieller Software existieren, wird die Problematik für Fabrikationsdaten bis heute kaum adressiert bzw. sind keine Lösungen zur Rechtewahrung/-verwaltung des geistigen Eigentums von Unternehmen bekannt, mit denen sich Know-how-Schutz und Produktionskontrolle für verteilte und vernetzte Produktionsumgebungen umsetzen ließen.

Auf der Ebene der Produktionsdaten gehen immer mehr Anbieter von CAD Systemen auf Cloud Technologie über und bieten ihre Konstruktionssysteme, aber auch nachgelagerte Systeme für Ausschreibung, Vergabe und Abrechnung (AVA), als Software as a Service an (SaaS)[457, 458, 459] an. Hier werden mittlerweile deutsche Datenschutzvorgaben, wie z. B. Speicherung und Verarbeitung der Daten in einem deutschen Rechenzentrum sowie Verschlüsselung der Daten bei Transport und Lagerung, weitgehend umgesetzt. Auch die zunehmende Ausrichtung an internationalen Standards, wie z. B. ISO/IEC 27001 oder Service Organization Control 2 (SOC 2) Report, schreitet voran. Sicherlich ist damit immer noch keine durchgängige Informations- und IT-Sicherheit aus Sicht des Nutzers gegeben, da am Ende immer noch dem Cloud-Dienstanbieter vertraut werden muss in Bezug auf die Haltung der Daten in dem entsprechenden Rechenzentrum. Allerdings werden an dieser Stelle zzt. ebenfalls Entwicklungen sichtbar, die auch diese Problematik entschärfen könnten.[460] So bieten solche Systeme seit Anfang der 2000er Jahre die Möglichkeit, rollenbasierte Zugangsbeschränkungen umzusetzen. Auch Ansätze für die Kollaboration und den sicheren Datenaustausch sind seit Mitte der 2000er Jahre erkennbar.

Bei den Fabrikationsdaten hingegen ist nach wie vor problematisch, dass diese auf Maschinen und Systemen ausgeführt werden, die teilweise so alt sind, dass zzt. oft nicht einmal rollenbasierte Zugriffsmodelle existieren. So wurde

457 Vergl. z. B. Flugzeugbau, Dessault Systems, CATIA.
458 Vergl. z. B, Baudaten: Nemetschek, NEVARIS, AVA System.
459 Vergl. z. B. ThinkProject!, https://www.thinkproject.com/de/produkt/cloud/
460 Vergl.: Panbox, http://www.bmjv.de/SharedDocs/Kurzmeldungen/DE/2015/20150310_Panbox.html?nn=3433226 und Omnicloud, http://www.omnicloud.sit.fraunhofer.de/index_de.php

auch bei der Modellierung der Kommunikationsprozesse und Datenflüsse eine offensichtliche Notwendigkeit für eine neuartige Sicherheitsarchitektur zum Schutz von Fabrikationsdaten während ihrer Übertragung zu und Speicherung auf Produktionsanlagen des Auftragnehmers erkannt. Der Schutz geistigen Eigentums in Fabrikationsdaten würde die Auslagerung der Produktion auch in nicht-vertrauenswürdige Umgebungen erlauben. Im Rahmen eines solchen „Industrial Rights Managements" (IRM) würde sich auch eine Kontrolle und Limitierung der Stückzahl herzustellender Produkte realisieren lassen. Dadurch ließen sich neue vertrauenswürdige und zugleich flexible Wertschöpfungsnetzwerke verwirklichen und zum Beispiel Marktplätze für Produktions- und Fabrikationsdaten etablieren.

Für die Umsetzung ganzheitlicher IRM-Lösungen werden Sicherheitsmaßnahmen sowohl an den Produktionsstätten, als auch den Systemen der Entwickler benötigt. Die Daten müssen während Ihrer Erzeugung, Speicherung, Übertragung und Verarbeitung geschützt werden. Die notwendigen Voraussetzungen hierfür sind in erster Linie:

- Eindeutige, sichere, digitale Identitäten der am jeweiligen Produktionsprozess beteiligten Komponenten, Systeme und Anlagen
- Integrität der am jeweiligen Produktionsprozess beteiligten Komponenten, Systeme und Anlagen
- Vertraulichkeit, Integritäts- und Authentizitätsschutz der sensiblen Daten die zwischen Komponenten, Systemen und Anlagen ausgetauscht werden, z. B. durch Verschlüsselung

Es ist daher wichtig, dass zukünftig möglichst alle relevanten, am Fertigungsprozess beteiligten und Fabrikationsdaten verarbeitenden Systeme mit eigenen, eindeutigen und nicht übertragbaren physikalischen Identitäten ausgestattet sind. Auf einer solchen Basis kann die Integrität aller Komponenten in einer Produktionslinie, welche sensible Daten verarbeiten, kontinuierlich überwacht und somit gewährleistet werden. Darüber hinaus sollten die Identitäten über die Grenzen eines Unternehmens überprüfbar sein und entsprechende Vertrauensbeziehungen zwischen den Unternehmen existieren.

Es gibt in der klassischen IT bereits viele Ansätze zur Organisation von Identitäten. Mitte der 2000er Jahre kamen so genannte Identity Management Systeme (IDMS) mit entsprechenden Schnittstellen (Security Assertion Markup Language (SAML)) zum sicheren Austausch der Identitäten über entsprechende Produkte auf. SAML bietet z. B. bestimmte Werkzeuge (Security Tokens), um Benutzerinformationen in Authentifizierungs- und Autorisierungs-Szenarien umzusetzen. Heute trifft man diese bewährte Technologie im klassischen IT-Umfeld bei der Realisierung von Single-Sign-On-Lösungen und Datenanbindungen, z. B. in Cloud-Umgebungen, an. Diese Identitäten sind in der Regel aber an Personen gebunden.

Zudem sind auch Reputationsmodelle bekannt, bei denen die Identität eines Nutzers durch Bestätigung durch andere Nutzer oder Verschneidung mit anderen Datensätzen erfolgt. Ein prominentes Beispiel dazu findet sich z. B. im Bereich der Pretty Good Privacy (PGP) Methode zur asymmetrischen Verschlüsselung. Hier gibt es keine zentrale Ausgabestelle für Identitäts- und Verschlüsselungszertifikate, sondern jeder Nutzer erstellt diese selbst. Die Validierung der Identität erfolgt durch die Weitergabe im Rahmen einer bestehenden Vertrauensbeziehung. Die Akteure haben dabei die Möglichkeit, die Zertifikate zu bestätigen. Je länger ein Zertifikat unkompromittiert im Umlauf ist, desto höher leitet sich die Reputation ab.

Es gibt bereits Ansätze[461, 462, 463, 464], Identitäten mittels kryptografischer Verfahren untrennbar mit einer physikalischen Komponente, z. B. einer Produktionsmaschine, zu verbinden. Diese scheinen zzt. am geeignetsten zu sein, um auf dieser Basis Fabrikationsdaten mittels einer zusätzlichen durchgängigen „Ende-zu-Ende-Verschlüsselung" sicher auszutauschen. Dabei würden alle Daten bereits im Entstehungsprozess verschlüsselt und erst auf einer eindeutig identifizierbaren Maschine wieder entschlüsselt. Dies könnte beispielsweise Anwendung bei der Übertragung von Daten zwischen einem cloud-gestützten CAD-System bis zur Maschinensteuerung in einer CNC-Maschine finden, wobei

461 Trusted Platforum Module (TPM), BSI, https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/TrustedComputing/TrustedPlatformModuleTPM/TrustedPlatformModuleTPM/aufbaustruktur.html
462 Physical unclonable functions for device authentication and secret key generation, G. Edward Suh, Cornell University, Ithaca, NY, Proceeding DAC, 07 Proceedings of the 44th annual Design Automation Conference.
463 Protecting electronic products (PEP), Fraunhofer AISEC, http://www.aisec.fraunhofer.de/de/presse-und-veranstaltungen/presse/pressemitteilungen/2013/20130408_pep-protecting-electronic-products.html
464 ProAuthent, Forschungsprojekt zur Verknüpfung von Electronic Product Code (EPC) und RFID-Tag-ID, http://www.fml.mw.tum.de/ProAuthent/Download/Beitrag%20Durchholz_WGTL_2010.pdf

der Fokus explizit auf dem unternehmensübergreifenden Datenaustausch liegt bzw. auf der vertikalen Kommunikation zwischen den mittleren und oberen Ebenen der Automatisierungspyramide, da bereits hier neben dem Schutzziel Datenintegrität auch das Schutzziel Vertraulichkeit zwingende Voraussetzung wird.

Die dazu erforderlichen kryptografischen Methoden sind bereits heute State-of-the-art[465, 466, 467] und werden z. B. schon seit längerem im Bereich der Email-Verschlüsselung eingesetzt, können aber ebenso für die Absicherung jeden anderen Datentyps genutzt werden. Prinzipiell können also auch Produktions- und Fabrikationsdaten mittels symmetrischer und asymmetrischer Kryptografie oder auch der Betrieb eines Chips oder sonstigen Bauteils als solches geschützt werden, z. B. mittels „Initial Unlocking“[468]. Für das Produktionsumfeld gelten jedoch andere Rahmenbedingungen, die den Einsatz von Kryptographie betreffen. Die am häufigsten angeführten Hinderungsgründe, die gegen den Einsatz von Kryptographie sprechen, sind Verfügbarkeits-, Echtzeit- und Safety-Anforderungen.

Seitens der Industrie werden oft Technologien abgelehnt, die möglicherweise der Verfügbarkeit von Produktionsumgebungen entgegenstehen. Dabei spielt die Latenz, die diese Systems auf die sehr zeitkritischen Prozesse ableiten, eine entscheidende Rolle. Darüber hinaus gibt es Zwänge, die sich aus den Safety-Anforderungen ableiten, und dort gegebenenfalls den Einsatz von verschlüsselten Daten nicht erlauben.

Diese Bedenken haben bisher maßgeblich verhindert, dass sich kryptographische Lösungen im Automatisierungs- und Produktionsumfeld durchsetzen konnten. In Kapitel 5 wurde bereits näher auf die Eignung verschiedener Maßnahmen im industriellen Umfeld eingegangen. Zu allgemeinen Empfehlungen im Bereich Kryptographie sei hier auf die TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“[469] verwiesen. Für die Implementierung besonders „leichtgewichtiger“ kryptographischer Verfahren sei ergänzend auf die ISO/IEC 29167 verwiesen. Dort sind Verfahren definiert, die mit geringen Ressourcen auskommen.

Sowohl die Ansätze zur Umsetzung eindeutiger, sicherer Identitäten als auch die zur Verschlüsselung benötigen zwingendermaßen ein Identitätsmanagement (englisch Identity Management (IdM)), also die nachvollziehbare, zuverlässige Zuordnung von Schlüsseln zu Identitäten auf Basis von Zertifikaten. Das Identitätsmanagement stellt bereits im Umfeld der Office-IT eine bekannte Problematik dar. Gängig ist der Aufbau zentraler, vertrauenswürdiger Instanzen, so genannter Public Key Infrastrukturen (PKI), die für Aufgaben wie Schlüssel- und Zertifikatserzeugung sowie Verteilung und Revokation der selbigen zuständig sind. Die wichtigste Aufgabe einer PKI ist die Zuordnung von digitalen zu physischen Identitäten und die Veröffentlichung von Informationen über die Gültigkeit von Zertifikaten. Das den PKI-Strukturen zugrundeliegende Konzept von Zertifikaten scheint auch für die Absicherung von Maschinen und IT-gestützten Systemen dem Grunde nach geeignet, also auch für das industrielle Produktionsumfeld. Mit dem Aufbau einer PKI können je nach Größe und Zweck hohe Aufwände und Kosten verbunden sein. Darüber hinaus erschließen sich die gesamten Potenziale der gesamten Zertifikatskommunikation am besten, wenn eine zentrale Zertifizierungsstelle (CA) als erste Instanz verfügbar ist. Das ist aber schon in der klassischen IT selten der Fall. Hier können durchaus Zertifikate unterschiedlicher CAs miteinander genutzt werden. Dazu ist allerdings eine erste gegenseitige Anerkennung erforderlich. Diese würde bereits in Industrie 3.0 Verfügbarkeits- und Latenzprobleme erzeugen. Es müssten also Schlüsselverteilungsmethoden entwickelt werden, die diesen Rahmenbedingungen gerecht werden können.

Die grundlegenden Konzepte und Technologien für eindeutige digitale Identitäten, Integritätsschutz und die Verschlüsselung von Daten wurden z. B. unter anderem von Fraunhofer SIT verwendet, um einen Prototyp eines IRM-Systems zu entwickeln.[470] Mit der prototypischen Struktur wurde nachgewiesen, dass Daten in einem Produktionsumfeld technisch geschützt werden können. Die am Beispiel eines Produktionsprozesses entwickelte Lösung, bei der verschlüsselte Konstruktionsdaten zu Fabrikationsdaten verarbeitet und erst auf einem 3D-Drucker entschlüsselt und

465 Message-Digest Algorithm 5 (MD5, 128 Bit-Hashwert); https://de.wikipedia.org/wiki/Message-Digest_Algorithm_5
466 Asymmetrisch: (RSA) min. 2048 Bit-Hashwert, besser 4096 Bit-Hashwert; Symmetrisch: (AIS), min. 128 Bit-Hashwert, am besten 256 Bit-Hashwert.
467 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html
468 Jarrod A. Roy et al: EPIC: Ending Piracy of Integrated Circuits. DATE 2008. (1069-1074) + IEEE Computer 2010 V10 Issue 43 (30-38).
469 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html
470 IT-Gipfel 2014, Vorstellung einer vertrauenswürdigen Maschinensteuerung an verschiedenen Standorten, Fraunhofer SIT, Deutsche Telekom, Infineon – in Kooperation mit Hirschmann, WIBU Systems und TRUMPF.

ausgegeben werden können, reicht von den Produktionsdaten der Entwickler durchgängig bis hin zu den entsprechenden Fabrikationsdaten auf den Werkzeugmaschinen und setzt neben der Vertraulichkeit der Daten auch die Kontrolle über die Häufigkeit ihrer Verwendung durch.

6.1.2 Verwendung hardware-basierter Sicherheitsanker

Die Identifizierbarkeit und Integrität von computergestützten Geräten ist eine der zentralen Sicherheitsanforderungen in vernetzten Umgebungen, insbesondere wenn Produktionsprozesse auf sensiblen Unternehmensdaten aufsetzen, in diesem Fall Produktions- und Fabrikationsdaten. Um verbindliche Aussagen über Identität und Integrität treffen zu können, werden Technologien benötigt, die Maschinen und Komponenten eine verlässliche und eindeutige digitale Identität zuweisen – so genannte „hardware-basierte Sicherheitsanker".

Zurzeit laufen Untersuchungen und Entwicklungen, die auf die Anwendbarkeit einer bestehenden Technologie aus der klassischen IT abstellen, dem Trusted Computing[471]. Die damit verbundene Trusted Computing Group[472] (TCG) stellt das spezifizierte[473] Trusted Platform Module[474, 475] (TPM) zur Verfügung, wodurch in der Vergangenheit Zertifikate für Identitäten und Verschlüsselung auf Rechnern zur Verfügung gestellt wurden. Auch wenn die Funktionalität der Chips noch nicht den in I4.0 wünschenswerten Reifegrad aufweist, so sind mit der Entwicklung des TPM 2.0 Stacks[476] schon jetzt Weiterentwicklungen verfügbar, die z. B. eine Implementierung auf in Maschinen bereits vorhandener Hardware ermöglichen kann.

Die kryptographischen Schlüssel, die auf einem solchen TPM-Chip hinterlegt werden, können aus diesem nicht mit vertretbarem Aufwand unautorisiert entnommen und somit auch nicht von Dritten genutzt werden. Der TPM-Chip implementiert standardisierte kryptographische Verfahren und verfügt über einen eigenen Prozessor zur Durchführung von kryptographischen Operationen. Auf Basis geeigneter hardware-basierter Sicherheitsanker können sowohl das Schutzziel der eindeutigen Zuordenbarkeit (eindeutige Identität) als auch das Schutzziel der Integrität für Hard- und Softwarekomponenten erreicht werden. Im Umfeld der klassischen Office-IT sind beispielsweise TPM-Chips seit vielen Jahren im Einsatz. Auch wenn sich die Akzeptanz der Technologie im Consumer-Segment nicht ganz durchsetzen konnte, werden im Business-Sektor immer mehr Systeme standardmäßig mit TPM-Chips ausgeliefert. Bezüglich der Maschinen-Identitäten liegen hier allerdings sehr viel günstigere Voraussetzungen vor, die den Einsatz begünstigen. Die ausgestatteten Systeme sind dezidierten Einsatz-Szenarien gewidmet und können daher bessere Rahmenbedingungen für die Operationalisierung bereitstellen. Mit TPM 2.0 adressiert der Standard seit etwa einem Jahr auch verstärkt andere Bereiche mit wachsenden Sicherheitsanforderungen, z. B. eingebettete Systeme in Produktionsumgebungen. Dennoch sind hardware-basierte Sicherheitsanker im Umfeld der Produktionsautomatisierung bisher nicht weit verbreitet.

Im Rahmen des IT-Gipfels[477] 2014 in Hamburg haben die Firmen Infineon, Deutsche Telekom, Fraunhofer SIT, Trumpf, WIBU-Systems und Hirschmann erstmals prototypisch gezeigt, wie eine Sicherheitslösung für industrielle Anwendungen auf Basis eines solchen hardware-basierten Sicherheitsankers aussehen könnte, um eine lückenlos gesicherte Kommunikation über Standort- bzw. Unternehmensgrenzen hinweg zu realisieren. Die Durchsetzung von hardware-basierten Sicherheitsankern im PC-Umfeld, das Engagement großer Chiphersteller (Infineon) im Kontext von I4.0 und die erfolgreiche Implementierung des oben beschriebenen Prototypen lässt darauf schließen, dass sich ähnliche Lösungen[478] vermutlich auch im Umfeld der produzierenden Industrie durchsetzen werden.

Ein weiterer bei der Optimierung der Infrastruktur zu betrachtender Aspekt betrifft das zu verwendende Hardware-Modul: Sollten sich TPM-Chips für gewisse Geräte oder

471 Informationen und Stellungnahmen zu aktuellen Entwicklungen im Bereich vertrauenswürdiger Plattformen, Bundesamt für Sicherheit in der Informationstechnik (BSI), https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/TrustedComputing/tcg.html
472 Trusted Computing Group (TCG), http://www.trustedcomputinggroup.org/about_tcg
473 TCG Architecture Overview, Version 1.4, https://www.trustedcomputinggroup.org/resources/tcg_architecture_overview_version_14
474 S. L. Kinney. Trusted platform module basics: using TPM in embedded systems, Newnes, 2006.
475 https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/TrustedComputing/TrustedPlatformModuleTPM/uebersicht_TPM.html
476 http://www.trustedcomputinggroup.org/resources/tpm_20_library_specification_faq
477 IT-Gipfel 2014, Vorstellung einer vertrauenswürdigen Maschinensteuerung an verschiedenen Standorten, Fraunhofer SIT, Deutsche Telekom, Infineon – in Kooperation mit Hirschmann, WIBU Systems und TRUMPF.
478 Ergänzende und alternative Techniken zu Trusted Computing, Bundesamt für Sicherheit in der Informationstechnik (BSI), 25.08.2010, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/TC_ErgA/TC-ErgA_Teil1.pdf

Bauteile als zu schwergewichtig erweisen, weil die volle Funktionalität gar nicht benötigt wird, so sind unter dem Aspekt der Optimierung auch alternative Hardware-Sicherheits-Module in Betracht zu ziehen, welche nur die benötigten Funktionen beinhalten. Auch abgestufte Versionen von Hardware-Modulen für verschiedene Komponenten sind möglich, wie es beispielsweise bei der Spezifikation der Sicherheitsarchitektur für Automotive On-Board-Netze im Rahmen des EVITA-Projektes[479] praktiziert wurde. Konkrete Komponenten aus dem Produktionsumfeld, wie z. B. Werkzeugmaschinen, ICS- oder SCADA-Systeme (Supervisory Control and Data Acquisition) bzw. Komponenten, welche entsprechende Technologien implementieren, sind aber am Markt bisher nicht bzw. kaum verfügbar.

6.1.3 Production Line IT-Security Monitoring

Die Erfahrung vieler Industrieunternehmen ist, dass insbesondere die Überwachung von Anlagen in Bezug auf das kontinuierliche IT-Sicherheitsmonitoring große Probleme bereitet, da keine geeigneten Technologien zu Erkennung oder Abwehr von IT-Sicherheits-Angriffen existieren. Dabei spielen nicht nur die gezielten Angriffe auf Systeme eine Rolle. Es sind vielmehr Sicherheitsprobleme, die aus Alltagsereignissen entstehen. So nutzen bspw. Mitarbeiter in der Produktion USB-Ports der Anlagensteuerung, um ihre Mobiltelefone aufzuladen. Hier können sowohl Schadsoftware auf die Produktionssysteme übertragen, als auch Performance-Artefakte erzeugt werden, die allein durch das Vorhandensein einer neuen, nicht systemkonformen Komponente erzeugt werden. Zukünftig wird sich die Situation dahin gehend verändern, dass man gewollt mobile Endgeräte in die Produktion einbringt, z. B. als Display für Werkzeugmaschinen. Es ist also zwingend erforderlich, über Werkzeuge zu verfügen, welche die Überwachung der Anlagen gewährleisten und gleichzeitig in der Lage sind, gewünschte Muster von unerwünschten Mustern zu differenzieren.

In der klassischen IT finden wir zwei Ansätze vor, die es erlauben, ungewollte Aktivitäten innerhalb einer IT-Infrastruktur zu analysieren und zu evaluieren. Bezüglich der Integrität von IT-Umgebungen werden sog. Intrusion Detection Systeme (IDS) eingesetzt.[480, 481, 482] In netzwerkbasierten IDS werden alle Pakete aufgezeichnet und analysiert. Hier können zzt. in der Regel IP-basierte Umgebungen auf Mustererkennung hin betrachtet werden. Mittlerweile können sog. Intrusion Prevention Systeme (IPS) auch bestimmte Datenpakete verwerfen.

Dem Einsatz dieser Systeme für die Überwachung einer Produktionsumgebung stehen einige Faktoren entgegen. Zum einen laufen die relevanten Daten nicht alle über IP-Protokolle, zum anderen tragen die Systeme ggf. Latenzzeiten in die Produktion. Abschließend ist festzustellen, dass die aktuellen Infrastrukturen nicht geeignet sind, diese Software Produkte anzuwenden. Zudem gibt es keine Muster für IT-Sicherheitsvorfälle.

Auf der anderen Seite existieren seit längerem sog. Security Information Event Management (SIEM)[483, 484] Systeme. Diese Systeme ermöglichen das Speichern, Analysieren und Bewerten von Logdaten. Allerdings fehlt diesen Systemen noch eine Anbindung an die Aktuatorik- und Sensorik-Datenebene.

Zur Erhöhung des Sicherheitsniveaus benötigt die Industrie eine Technologie, die eine kontinuierliche Überwachung der Systeme erlaubt, eine Anbindung an die Feldbusebene mitbringt und keine Latenzzeiten in die Systeme einträgt. Es müssen für diesen Anwendungsfall also alternative Methoden gefunden werden, um die IT-Landschaft der Produktion im laufenden Betrieb einer Analyse und Absicherung zu unterziehen, ohne die primären Schutzziele zu gefährden. Um den Sicherheitsrisiken nachhaltig zu entgegnen, sind neue, adaptive Verfahren notwendig, welche die IT-Systeme nicht isoliert betrachten, sondern zielgerichtet den Produktionsprozess selbst schützen.

479 M. Wolf and T. Gendrullis. Design, implementation, and evaluation of a vehicular hardware security module. In Information Security and Cryptology-ICISC2011, pages 302–318. Springer, 2012.
480 Henk Birkholz and Ingo Sieverdingbeck. Link-failure assessment in redundant ICS networks supported by the Interconnected-asset Ontology. In Annual IEEE CQR International Workshop, Tucson, Arizona, USA, 2014.
481 Teng, Henry S., Chen, Kaihu, and Lu, Stephen C-Y, „Adaptive Real-time Anomaly Detection Using Inductively Generated Sequential Patterns," 1990 IEEE Symposium on Security and Privacy.
482 Henk Birkholz and Ingo Sieverdingbeck. Supporting Security Automation for Multi-Chassis Link Aggregation Groups via the Interconnected-asset Ontology. In Availability, Reliability and Security (ARES), 2014 Ninth International Conference on, Fribourg, CH, 2014.
483 https://securosis.com/blog/understanding-and-selecting-siem-lm-use-cases-part-1
484 http://mosaicsecurity.com/categories/85-log-management-security-information-and-event-management

Das Konzept von Anomalie-Erkennungssystemen erscheint dabei als ein möglicher Ansatz. Anomalie-Erkennungssysteme könnten als reaktive Maßnahme zur Verbesserung der IT-Security derart implementiert werden, dass die Abläufe, unabhängig vom jeweiligen Einsatzszenario, nicht gestört werden. Passiv arbeitende Sensoren, die entweder ohnehin in der jeweiligen Automatisierungslösung vorhanden sind oder zusätzlich für die Anomalie-Erkennung eingebracht werden, messen zunächst relevante Größen im Prozess (z. B. Druck, Temperatur, Geschwindigkeit, Spannung etc.), mit denen eine entsprechende Erwartung verbunden ist. Im zweiten Schritt werden diese Daten auf dedizierten Systemen ausgewertet und auf Sicherheitsimplikationen hin überprüft. Diese Methoden werden zzt. schon sehr effizient bei der Performanz-Optimierung von Anlagen eingesetzt. Es ist daher durchaus denkbar, dass potenziell auf Angriffe zurückzuführende Abweichungen im Prozess erkannt und passende Gegenmaßnahmen eingeleitet werden können.

Es sollten daher intelligente, kombinierte und adaptive Anomalie-Erkennungssysteme entwickelt werden, die sowohl die vernetzen IT-Systeme als auch das Prozessverhalten überwachen, semantische Bezüge herstellen und die Verhaltensmuster korrelieren. Es soll bewertet werden können, wie und wann IT-Sicherheitsprobleme Anomalien im Produktionsprozess verursachen und wie solche Probleme frühzeitig diagnostiziert und verhindert werden können.

Für die Entwicklung derartiger Lösungen kann in vielen Teilbereichen auf bereits existierende Forschungsgrundlagen zurückgegriffen werden. So können Erfahrungen aus der Aktuatorik- und Sensorik-Auswertung auf IT-Sicherheit[485, 486] übertragen werden. Es gibt bereits erhebliche Erfahrung mit der Auswertung dieser Daten in Bezug auf Performanzerhöhung[487] und Störfallidentifikation. Es existieren informatische Methoden zu Datenauswertung und Fehlerindikation.[488] Es ist heute bereits möglich, zu erkennen, welche Produktionsstörung vorliegt, ohne eine Anlage direkt zu betrachten, allein auf der Basis von Mustererkennung und Datenauswertung.

Ebenfalls existieren Forschungsergebnisse aus dem Bereich der Erstellung von Wissens-Datenbanken, welche Ontologie-orientiert die semantische Auswertung von Infrastrukturdaten eines Produktionsprozesses unterstützen können.[489] Vorhandene Vorarbeiten stellen das Know-how für das Design eines solchen Datenbank-Schemas sowie die Expertise für ein Framework-Design zur Befüllung und aufgabenbezogenen Bereitstellung der Datenbank mit entsprechendem Inhalt.

Verschiedene Referenzprojekte, zeigen den Einsatz von Systemen zur Anomalie-Erkennung im Umfeld eingebetteter Systeme.[490] Werkzeuge zur (ggf. auch cloud-gestützten) Auswertung von Aktuatorik- und Sensorikdaten einer Produktionsanlage und zur Abbildung der Muster auf IT-Sicherheitsvorfälle werden mehrere aktuelle Probleme der Industrie lösen und auch für die Zukunft der I4.0 höchste Relevanz haben:

- Analyse und Bewertung von IT-Sicherheit in Produktionsanlagen bereits in der Planungsphase.
- Kontinuierliche Überwachung einer Anlage im Betrieb, ohne direkt auf die Systeme physikalisch zugreifen zu müssen.
- Berücksichtigung von Kontextinformationen und semantischem Bezug auf den IST-Zustand.
- Bereitstellung eines Tools als Cloud-Dienst ermöglicht die dezentrale und zeitgleiche Überwachung mehrerer Standorte.
- Protokollierung aller Ereignisse für die Einhaltung der ges. Compliance Auflagen.

Hersteller und Ausrüster sollten daher im Rahmen von Forschungsprojekten motiviert werden, in Zusammenarbeit mit Forschungsinstituten, an Lösungen zur Anomalie-Erkennung zu arbeiten, die auf der passiven Erfassung von Prozess- und Produktionsdaten basieren und somit nicht

485 Windmann, Stefan; Niggemann, Oliver: Efficient Fault Detection for Industrial Automation Processes with Observable Process Variables. In: IEEE International Conference on Industrial Informatics (INDIN 2015), Cambridge, UK, Jul. 2015.
486 VDE-Positionspapier „Taktiles Internet“ – Das IT-Netz der Zukunft, VDE, 2014.
487 Steckel, Thilo; Bernardi, Ansgar; Gu, Ying; Windmann, Stefan; Volgmann, Sören; Niggemann, Oliver: Anomaly Detection and Performance Evaluation of Mobile Agricultural Machines by Analysis of Big Data. In: VDI International Conference on Agricultural Engineering, Hannover, Germany, Nov. 2015.
488 Windmann, Stefan; Eickmeyer, Jens; Badinger, Johann: Evaluation of Model-Based Condition Monitoring Systems in Industrial Application Cases. In: Machine Learning for Cyber Physical Systems (ML4CPS 2015), Lemgo, Germany, Okt. 2015.
489 Vgl. Birkholz 2014, Birkholz 2014.01, Birkholz 2014.02.
490 ANSII, https://www.sit.fraunhofer.de/de/angebote/projekte/ansii/

die Echtzeitfähigkeit und Verfügbarkeit von Industrieanlagen beeinträchtigen.

6.1.4 Safety & Security

Mit dem deutschen Begriff Sicherheit werden oft sowohl die IT-Sicherheit (Security) als auch die Betriebssicherheit (Safety) bezeichnet. Security betrifft den Schutz von Systemen vor unbefugten Zugriffen von außen sowie den Schutz sensibler Daten vor Verfälschung, Verlust und unbefugtem Zugriff im Innenverhältnis. Dies schließt sowohl explizite Angriffe als auch nicht-intendierte Security-Vorfälle ein. Safety verlangt, dass Restrisiken, die vom Betrieb eines Systems ausgehen, akzeptable Werte nicht übersteigen. Unter Restrisiken versteht man dabei eine Kombination aus einem mit schädlichen Konsequenzen verbundenen und auf eine Gefährdung zurückzuführenden Ereignis sowie einer Auftretenswahrscheinlichkeit – kurz: Schadenshöhe und Eintrittswahrscheinlichkeit. Dies gilt sowohl für Gefährdungen der Umgebung des Systems, wie z. B. Umweltschäden, als auch für Personen und Wirtschaftsgüter innerhalb und außerhalb des Systems.

Derzeit findet unter den Oberbegriffen des „Internets der Dinge“ und der „cyber-physischen Systeme“ eine zunehmende Integration von Informationssystemen und technischen Systemen statt, die häufig sowohl im Hinblick auf Security als auch im Hinblick auf Safety kritisch sind. Zudem sind die Eigenschaften nicht wechselwirkungsfrei: Security-Lücken können zu Gefährdungen im Sinne von Safety führen und Maßnahmen zur Wiederherstellung von Safety, wie z. B. das Öffnen der Türen von Rechnerschränken bei einem Brand, können Security-Lücken nach sich ziehen. Darüber hinaus ist ebenfalls denkbar, dass der technischen Spezifikation gemäß wirkende Sicherheitsmaßnahmen, wie z. B. Verschlüsselung, den Safety-Anforderungen entgegenstehen, z. B. wenn diese bestimmte Prozesse verzögern würden. Hinzu kommt, dass sich solche Systeme modular ergänzen oder anpassen lassen sollen und dass sich Systeme sogar autonom zur Laufzeit integrieren und adaptieren. Diese Charakteristika stehen den Grundannahmen des etablierten Safety und Security Engineering diametral entgegen. Etablierte Ansätze gehen stets davon aus, dass sowohl das zu betrachtende System als auch dessen Kontext vollständig bekannt sind und entsprechend umfassend analysiert werden können. Basierend auf den Analyseergebnissen kann daraufhin ein adäquates Sicherheitskonzept erstellt und umgesetzt werden. Dies wird im Kontext von I4.0 nicht mehr ohne Weiteres möglich sein, da aufgrund der Offenheit und Anpassungsfähigkeit der Systeme, eine mit bestehenden Methoden nicht beherrschbare Komplexität entsteht. Es ist ein neuartiger, integrativer Ansatz vonnöten, um Sicherheit im Kontext cyber-physischer Systeme umfassend zu adressieren.

Das zentrale Ziel des hier vorgestellten Konzepts ist die Erarbeitung eines integrativen Ansatzes zur Behandlung von Safety und Security im Kontext cyber-physischer Systeme, der die beschriebene Trennung überwindet. Dieser Ansatz soll im Rahmen der Industrie-4.0-Domäne entwickelt werden, in der z. B. die Sicherheit von Mitarbeitern, Produktionsanlagen und der Umwelt zentrale Themen sind. Bereits am Beispiel eines relativ kleinen und einfachen Subsystems wie einem Industrieroboter wird die Notwendigkeit eines integrativen Ansatzes zur Behandlung von Safety und Security deutlich. Die Herausforderungen in umfangreichen cyber-physischen Systemen sind natürlich unvergleichlich größer.

In heutigen Systemen werden Industrieroboter in der Regel lokal programmiert und verfügen ggf. über eine Schnittstelle zu einem IT-Netzwerk, um Programme zu laden oder Daten zu sichern. Durch Organisationsanweisungen wird sichergestellt, dass die Roboter eventuell gar nicht vernetzt oder nur mit geschlossenen Netzen der Produktions-IT verbunden sind. Durch physische Absperrungen wird erreicht, dass sich keine Menschen in der Reichweite der Roboter befinden, wenn diese arbeiten. Um die in einer I4.0-Umgebung erforderliche Flexibilität bei der Gestaltung von Produktionsumgebungen für Mensch und Maschine zu erreichen, ist es jedoch wünschenswert, solche Absperrmaßnahmen zu vermeiden. Darüber hinaus ist es auch im Sinne einer flexibleren Konfiguration bei wechselnden Produktionsaufträgen oder im Wartungsfall wünschenswert, die Roboter an eine offene Netzinfrastruktur anzubinden und einen Fernzugriff über standardisierte Endgeräte zu ermöglichen, um z. B. Fernwartung betreiben zu können. Ein integrativer Ansatz für Security und Safety muss in der Lage sein, die Maßnahmen zu identifizieren, die umzusetzen sind, damit die Roboter sicher an ein offenes Netz angeschlossen werden können, ohne dass Menschen in ihrer Umgebung gefährdet werden. Dies muss idealerweise unter Verzicht auf physische Absperrungen möglich sein.

Zukünftig müssen moderne, teiloffene Produktionssysteme (cyber-physische Produktionssysteme) umfassend abgesichert werden, um unbefugten Zugriff im Sinne von Security zu unterbinden und gefahrbringende Betriebszustände im Sinne von Safety abzuwenden. Hierbei ist es wichtig, auch den Menschen als aktiven und passiven Bestandteil des Gesamtsystems einzubeziehen: Aktiv bedeutet, dass er

mutwillig (Sabotage) oder durch Ermüdung und nachlassende Zuverlässigkeit (menschliche Fehler) die Systemsicherheit reduziert; passiv bedeutet, dass er vor Risiken und negativen Folgen im Rahmen gesetzlicher Vorgaben zu schützen ist.

Neben Safety und Security interessieren die Wirtschaft Optimierungspotenziale des Produktionsbetriebs. Hier kann die Integration der IT-Systeme dabei helfen, enorme Synergie-Effekte auszunutzen. Voraussetzung ist aber, dass die gesetzlichen Vorgaben für Safety nach wie vor eingehalten werden können und die Restrisiken der IT-Security beherrschbar bleiben. Als Ersatz für physische Absperrungen werden in Zukunft vermehrt Sensorsysteme und Kameras eingesetzt, welche die safety-kritischen Umgebungen der Anlagen überwachen. Dies trifft in gleicher Weise für Produktionsassistenzsysteme zur Unterstützung von Menschen in der Produktion zu, z. B. zur Überwachung manueller Montagevorgänge, Qualitätssicherung etc.. Die dabei anfallenden Daten müssen die Privatsphäre der betroffenen Menschen berücksichtigen und rechtliche Bestimmungen des Datenschutzes einhalten. Die Transparenz der Überwachungssysteme soll für Akzeptanz bei den betroffenen Personen, Betriebsräten und Aufsichtsbehörden sorgen. Es muss auch hinterfragt werden, inwieweit die bestehenden Maßnahmen im Kontext von I4.0 noch aufrechterhalten werden können oder durch neue Ansätze ersetzt werden müssen.

Idealerweise könnten offene, standardisierte IT-Netze für die Vernetzung der Komponenten in Produktionsumgebungen eingesetzt werden. Eine flexible Automatisierung erfordert die Fähigkeit zur autonomen Rekonfiguration und Optimierung der Produktionsumgebung, ohne dabei Safety oder Security zu gefährden. Gleichzeitig wird aus Kosten- und Flexibilitätsgründen eine Verschmelzung von Büro-, Gebäude- und Anlagen-IT vorangetrieben. Dies erfordert eine kontinuierliche, integrierte IT-Sicherheitsüberwachung von Anlagen und Systemen. Sofern hier die IT-Umgebungen weiter konvergieren, ist mit weiterer Verschränkung der IT-Sicherheitsprobleme aus beiden Welten zu rechnen.

Ein weiterer Trend in I4.0 ist die nahtlose Interaktion von Mensch und Maschinen. Hierzu sind streng überwachte Bereiche mit Kamerasystemen für die Überwachung und Lokalisierung von Menschen notwendig. Zur Kostenoptimierung könnten zukünftig die Gebäudeautomatisierung und die Überwachung integriert werden. Geeignete IT-Maßnahmen können die Überwachung ergänzen. Allerdings greifen die Daten in die Privatsphäre der Menschen ein, weshalb transparente und durch strenge Datenschutzmaßnahmen gesicherte Systeme für die Akzeptanz essenziell sind. Unter Umständen ist auch eine neue Definition des Begriffs Privatsphäre im Zusammenhang mit Safety-kritischen Systemen notwendig. Auch das menschliche Verhalten in Produktionsbereichen soll erfasst, modelliert und quantifiziert werden. Daraus können dann sowohl Systemoptimierungen als auch Maßnahmen zur Reduktion erfasster Daten abgeleitet werden. Künftig sorgen zudem in einem solchen cyber-physischen Produktionssystem (CPPS) verteilte eingebettete Systeme, wie beispielsweise Intelligente Ladungsträger oder Sensoren, für die dezentrale Steuerung und Optimierung von Produktion und Materialfluss. Folglich hat auch deren Security einen nicht unerheblichen Einfluss auf die Safety des Systems und muss daher ebenfalls mitbetrachtet werden.

Für Safety gibt es eine Vielzahl branchenspezifischer Standards. In diese Standards sollen zukünftig die notwendigen Ergänzungen für IT-Security so eingebracht werden, dass Vernetzung über offene Netzwerke möglich wird. In Zukunft werden auch vermehrt Security-Zertifizierungen gefordert werden. Ziel ist es hier, eine integrierte Safety-Security-Zertifizierung vorzubereiten, die auch Systeme erfasst, welche sich zur Laufzeit autonom verändern.

Entsprechend gibt es auch keine etablierten Ansätze zur integrierten Analyse von Systemen oder zur Erstellung integrierter Sicherheitskonzepte. Darüber hinaus werden die dynamischen Aspekte von I4.0 heute noch nicht ausreichend adressiert, wie etwa dynamische Updates, Rekonfiguration oder auch dynamische Integration im Sinne von Plug & Play: Nach etablierten Safety-Standards würden derlei Änderungen am System in der Regel eine komplexe Rezertifizierung nach sich ziehen.

6.1.5 Fazit

Bezüglich der Anforderungen an den Schutz der Konstruktions- und Fabrikationsdaten scheinen die notwendigen Technologien dem Grunde nach verfügbar zu sein. Alle Konzepte und IT-Produkte für die Verschlüsselung von Daten sind aus der klassischen IT bekannt und werden dort bereits verlässlich eingesetzt. Allerdings stehen der Übertragung auf die Produktion einige bisher ungelöste Fragestellungen entgegen. Es ist zzt. noch ungeklärt wie Verfügbarkeitsansprüche der Produktion mit den bestehenden Konzepten verbunden werden können. Hier besteht dringender Forschungs- und Entwicklungsbedarf. Darüber hinaus gestaltet sich der Aufbau und der Betrieb z. B. einer PKI auch in

der Verwaltungs-IT nicht immer einfach. Hier müssen Konzepte und Lösungen erarbeitet werden, wie diese Methoden auf Produktionsumgebungen abgebildet werden können.

Ähnlich sieht es im Bereich der hardware-basierten Vertrauensanker für Produktionssysteme – digitale Identitäten – aus. Auch hier existieren bereits Produkte, die prinzipiell Lösungsansätze zur Verfügung stellen. Hier müssen allerdings auch noch Fragestellungen der Skalierbarkeit solcher Systeme und der Kosten für die zusätzliche Hardware beantwortet werden. Möglicherweise bieten Weiterentwicklungen, wie z. B. TPM 2.0, mehr Freiheitsgrade in Bezug auf die Integration der Funktionen auf bestehende digitale Bausteine der Maschine. Diese Entwicklungen sollten gefördert und als Ziel entsprechend in mögliche Forschungsprogramme aufgenommen werden.

Die Fragestellung nach einer Methode zur kontinuierlichen Sicherheitsüberwachung von Produktionssystemen steht allerdings eher am Anfang. Zurzeit sind keine Konzepte bekannt, die sich unmittelbar übertragen ließen. Erfahrungen aus dem Bereich der Intrusion Detection im Zusammenhang mit Big Data Analytics Know-how lassen es denkbar erscheinen, dass die Erkennung von IT-Sicherheitsvorfällen durch Auswertung von Aktuatorik- und Sensorik-Daten möglich sein könnte. Allerdings fehlen hier zzt. sowohl der wissenschaftliche Beweis als auch die technische Erprobung im Produktionsumfeld.

Bezüglich der fortschreitenden Konvergenz von Safety und Security liegen die Notwendigkeiten auf der Hand. Hier ist allerdings festzustellen, dass Safety ein bereits gut erfasster und entsprechend regulierter Bereich ist, bei dem allen Akteuren die Sicherheitsableitungen nicht schwer fallen. Die IT-Sicherheit zählt – im Gegensatz zu z. B. Safety – momentan zu den deregulierten Bereichen. Es gibt kaum gesetzliche Vorgaben oder verbindlichen Standards für die Industrie, nach denen man sich ausrichten kann. Daher fällt es allen Akteuren sehr schwer angemessene IT-Sicherheitsmaßnahmen zu identifizieren. Dies wird im Kapitel 6.3 entsprechend beleuchtet und bewertet.

Zudem ist zzt. noch nicht in vollem Umfang erkennbar, welche Wechselwirkungen Safety auf Security und umgekehrt erzeugen wird. Klar ist, dass Probleme in einem Feld mit hoher Wahrscheinlichkeit Auswirkungen auf das andere erzeugen werden. Daher besteht auch hier erhöhter Forschungsbedarf für die Integrationskonzepte und das Management der möglichen Wechselwirkungen.

All diese Fragestellungen müssen dringend adressiert werden und bedürfen unmittelbarer Unterstützung seitens der politischen Entscheider, sei es durch weitere Förderungen von Forschung und Entwicklung (F&E), gesetzliche Regelungen oder flankierenden Maßnahmen zur Akzeptanz in der Wirtschaft und Bevölkerung.

6.2 Konzepte zur Überwindung organisatorischer Hemmnisse

Im Folgenden werden Konzepte und Ansätze zur Überwindung der in Kapitel 5.3 beschriebenen Hemmnisse, denen sich Unternehmen bei der Umsetzung von organisatorischen IT-Sicherheitsmaßnahmen im Kontext einer hochgradig vernetzten und automatisierten industriellen Produktion gegenüber sehen, vorgestellt. Betrachtet werden dabei einerseits die im Abschnitt 5.2.1.1 diskutierten und aus Unternehmenssicht primär relevanten organisatorischen IT-Sicherheitsmaßnahmen (Richtlinien und Verfahren, Methoden und Werkzeuge sowie Schulungen und Sensibilisierungsmaßnahmen) und andererseits Maßnahmen die von der Politik zur Optimierung der Rahmenbedingungen für die Umsetzung der organisatorischen IT-Sicherheitsmaßnahmen getroffen werden können. Besonderes Augenmerk wird im Folgenden auf Aspekte der Eignung der vorgestellten Konzepte und Ansätze für KMU gelegt.

Vor allem KMU stehen im Hinblick auf die I4.0 zahlreichen neuen Aufgaben und Herausforderungen gegenüber.[491] Nicht wenige davon betreffen die IT-Sicherheit und fast alle erfordern spezielle Kompetenzen. Da es für KMU weder möglich noch sinnvoll ist, alle geforderten Kompetenzen selbst aufzubauen, werden sie in einigen Bereichen vorübergehend oder dauerhaft auf Dienstleister zurückgreifen müssen. Trotz der Möglichkeit, Dienstleister einzubeziehen ist es wichtig, dass Unternehmen stets den Überblick über die eigene Lage behalten. Dienstleister können vor allem im Bereich der IT-Sicherheit nur unterstützen und einen Beitrag leisten, aber nicht die Verantwortung

491 s. Kagermann, Henning; Wahlster, Wolfgang; Helbig, Johannes (2013): Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0. Abschlussbericht des Arbeitskreises Industrie 4.0. 1. Aufl. Hg. v. Promotorengruppe Kommunikation der Forschungsunion Wirtschaft – Wissenschaft: acatech – Deutsche Akademie der Technikwissenschaften e.V., S. 18, 20, 47, 65; Bildstein, Andreas; Seidelmann, Joachim (2014): Industrie 4.0-Readiness: Migration zur Industrie 4.0-Fertigung. In: Thomas Bauernhansl, Michael ten Hompel und Birgit Vogel-Heuser (Hg.): Industrie 4.0 in Produktion, Automatisierung und Logistik. Anwendung, Technologien, Migration. Wiesbaden: Springer Vieweg (SpringerLink), S. 580–597, S. 585.

abnehmen. Dies gilt auch im Hinblick auf Security-as-a-Service-Lösungen, die zunehmend angeboten werden.

6.2.1 Technikintegration in bestehende Prozesse

Für die Hemmnisse, die die Problematik der Technikintegration in bestehende Prozesse widerspiegeln, existieren verschiedene komplementäre Lösungsansätze. Hier geht es primär darum, den Unternehmen den Einstieg in die industrielle Produktion der Zukunft zu erleichtern. Bedarf besteht hier nicht nur im Hinblick auf Fragen, die direkt mit der Gewährleistung eines angemessenen IT-Sicherheitsniveaus zusammenhängen, sondern auch im Hinblick auf Fragen in anderen Bereichen, die Auswirkungen auf die IT-Sicherheit haben können (z. B. wirtschaftlicher Nutzen, Prozesse/Arbeitsorganisation, Fachkräfte).

Wie viele Menschen haben auch Unternehmen Vorbilder und die Imitation von oder die Orientierung an erfolgreichen Vorgehensweisen ist ein legitimer Ansatz zur Optimierung von Strukturen und Prozessen im Unternehmen.[492] Von besonderem Interesse sind dabei I4.0-Vorreiter, die in der Lage sind, Herausforderungen im Bereich der IT-Sicherheit zu bewältigen, mit denen sich auch andere Unternehmen konfrontiert sehen, und die bereit sind, ihre Ansätze zu kommunizieren und mit Interessierten weiterzuentwickeln. Mittel, um Erfahrungen von einem Unternehmen an ein anderes weiterzugeben, sind beispielsweise Erfahrungsberichte (Success-Stories), Best-Practices und Handlungsleitfäden, die von einem oder mehreren, in einem bestimmten Bereich besonders erfolgreichen oder erfahrenen Unternehmen, verantwortet werden.[493] Während positive Erfahrungsberichte in der Regel von Herstellern oder Dienstleistern in einem bestimmten Bereich veröffentlicht und mit oder von ihren Kunden erstellt werden, ist es im Zusammenhang mit Best-Practices häufig nicht so, dass die Praktiken in dokumentierter Form vorliegen und der breiten Öffentlichkeit zugänglich sind. Die in vielen Bereichen gebräuchlichen Best-Practice-Sammlungen wären deshalb auch für die I4.0, insbesondere im Hinblick auf rasche Identifikation und Umsetzung von geeigneten IT-Sicherheitsmaßnahmen, hilfreich. Leitfäden gehen durch die Abstraktion von einzelnen Unternehmen noch einen Schritt weiter und sind deshalb für eine besonders breite Zielgruppe von Interesse. Im Hinblick auf IT-Sicherheit können diese Mittel Hilfestellungen zu Richtlinien und Verfahren, Methoden und Werkzeugen sowie zu Schulungen und Sensibilisierungsmaßnahmen geben. Sie sind meist in der Lage, betriebliche und organisatorische Entscheidungen zu unterstützen und mögliche Folgen von Entscheidungen transparent werden zu lassen. Sie werden in der Regel auch der verbreiteten Tatsache gerecht, dass die Entwicklung hin zur industriellen Produktion der Zukunft im Hinblick auf die Technikintegration eine schrittweise Entwicklung ist und kein plötzlicher Umbruch. Unternehmen – und vor allem KMU – können mithilfe von Erfahrungsberichten, Best-Practice-Sammlungen und Handlungsleitfäden in ihrer schrittweisen aber kontinuierlichen Annäherung an das Konzept I4.0 bestärkt werden und von Entwicklungen in anderen Unternehmen oder Industriezweigen profitieren. Erfahrungsberichte, Best-Practice-Sammlungen und Handlungsleitfäden sind nicht nur für Betreiber von Produktionsanlagen relevant, sondern auch für Dienstleister, die Unternehmen auf dem Weg zu einer hochgradig vernetzten und automatisierten industriellen Produktion begleiten.

Ergänzend werden besondere, an die Anforderungen im Bereich IT-Sicherheit in der I4.0 angepasste Bewertungs- und Entscheidungsunterstützungsmodelle für hilfreich gehalten. Die Modelle sollen das Treffen von fundierten und rationalen Entscheidungen erleichtern.[494] Bis alle relevanten Faktoren, vor allem im Zusammenhang mit organisatorischen IT-Sicherheitsmaßnahmen, bekannt sind und in solchen Modellen berücksichtigt werden, ist allerdings noch beachtlicher Forschungsbedarf gegeben. Insbesondere bei organisatorischen Entscheidungen sind nicht nur die monetär direkt abbildbaren Faktoren sondern auch die so genannten „weichen“ Faktoren entscheidend.[495] Die systematische Identifizierung von Faktoren, die eine Bewertung von Chancen und Risiken sowie Potenzialen und Herausforderungen erlaubt, ist ein wichtiger Punkt, den es im Hinblick auf die Integration neuer Techniken in bestehende Prozesse unter Aufrechterhaltung eines als angemessen

492 s. Schlick, Jochen; Stephan, Peter; Loskyll, Matthias; Lappe, Dennis (2014): Industrie 4.0 in der praktischen Anwendung. In: Thomas Bauernhansl, Michael ten Hompel und Birgit Vogel-Heuser (Hg.): Industrie 4.0 in Produktion, Automatisierung und Logistik. Anwendung, Technologien und Migration. 1. Aufl. Wiesbaden: Springer Vieweg, S. 57–84, S. 63.

493 s. Kagermann 2013, a. a. O., S. 34; Diemer in Bauernhansl, Thomas; Hompel, Michael ten; Vogel-Heuser, Birgit (Hg.) (2014): Industrie 4.0 in Produktion, Automatisierung und Logistik. Anwendung, Technologien und Migration. 1. Aufl. Wiesbaden: Springer Vieweg, S. 488 f..Ten Hompel in Bauernhansl et al (2014) a. a. O., S. 619.

494 s. Kagermann 2013, a.a.O., S. 57; Schlick et al a.a.O., S. 69 f.

495 s. Kagermann 2013, a.a.O., S. 18, 20, 27 f.; Bauer et al. 2014, S. 37; Botthof, Alfons; Hartmann, Ernst Andreas (Hg.) (2015b): Zukunft der Arbeit in Industrie 4.0. Berlin: Springer Vieweg, S. 5.

erachteten Sicherheitsniveaus zu lösen gilt. Entscheidungsunterstützung wird aufgrund der zunehmenden Komplexität und Dynamik im Zusammenhang mit vernetzter und automatisierter industrieller Produktion immer wichtiger – nicht nur, aber auch im Kontext der IT-Sicherheit.

Ein weiterer zentraler Punkt aus organisatorischer Sicht ist das Vorantreiben der Standardisierung. Bei einer in die Zukunft gerichteten Initiative wie I4.0 ist die Standardisierung keine Festschreibung von Technologien, die sich in der Praxis bewährt und am Markt durchgesetzt haben, sondern eine kooperative und durchaus konzeptionelle Arbeit zwischen Industrie, Forschungseinrichtungen und Verbänden. Dabei sollten, insbesondere beim Thema IT-Sicherheit, auch die Belange von KMU explizit einbezogen werden, um die Anwendbarkeit der Standards auch für diese zu gewährleisten. Standardisierung ist nicht nur im Zusammenhang mit Technikintegration relevant, sondern auch um Vertrauen in Kooperationspartner entlang der Wertschöpfungskette aufzubauen. Aus diesem Grund wird das Thema in diesem Kapitel im Zusammenhang mit Vertrauen nochmals aufgegriffen. Neben technischen Standards, ergibt Standardisierung auch im Zusammenhang mit organisatorischen Aspekten Sinn – vor allem auch im Kontext von organisatorischen IT-Sicherheitsmaßnahmen. Unternehmen müssen sich darauf verlassen können, dass nicht nur aus technischer Sicht von kooperierenden Unternehmen Mindeststandards eingehalten werden, sondern auch im Hinblick auf Strukturen und Prozesse.[496] Das gilt für KMU genauso wie für große Unternehmen. Zu klären ist allerdings noch, wie diese Mindeststandards ausgestaltet sein sollen und wie ihre Einhaltung überprüft werden kann. Zu beachten ist bei der Ausgestaltung vor allem im Hinblick auf KMU, dass die IT-Sicherheitsstandards umsetzbar und mit verhältnismäßigem Aufwand überprüfbar bleiben müssen – nur so kann vermieden werden, dass bestimmte, vor allem kleine Unternehmen von der Teilnahme an der I4.0 ausgeschlossen werden. Darüber hinaus erscheint auch eine Abstimmung auf internationaler Ebene sinnvoll. Der Einsatz von Standardprodukten, wie auch die Umsetzung von standardisierten Strukturen und Prozessen, bietet ein höheres Maß an Sicherheit für strategische Entscheidungen; nicht zuletzt dadurch, dass das Anknüpfen an einen anerkannten Standard einen reibungslosen Datenaustausch zwischen Partnern ermöglicht, die ebenfalls auf Standards aufsetzen. Im Zusammenhang mit der Einigung auf Mindeststandards geht es weniger um die Erarbeitung neuer Standards, sondern vielmehr um die zweckmäßige Integration und Anwendung bestehender Standards im Bereich der IT-Sicherheit.

Essenziell ist, dass mit der zunehmenden Vernetzung und Automatisierung, das Bewusstsein für die sich durch Technikintegration in bestehende Prozesse verändernde Bedrohungslage nicht zu kurz kommt.[497] Unvermeidlich ist in diesem Zusammenhang eine integrierte Abschätzung von technischen und organisatorischen Folgen der Integration neuer Techniken. Einerseits müssen in der industriellen Produktion etablierte Praktiken auf ihre Eignung für die I4.0 und andererseits neue technische Möglichkeiten auf ihr Nutzen-Risiko-Verhältnis hin überprüft werden. Ein Beispiel für zu hinterfragende, etablierte Praktiken ist die ausschließliche Nutzung von Wartungsfenstern für das Einspielen von Updates und Patches. Wenn einerseits die Produktions-IT mit der Office-IT bzw. direkt mit dem Internet verbunden ist und andererseits in der Produktions-IT zunehmend Standardkomponenten zum Einsatz kommen, muss man sich über diese Praktik ernsthaft Gedanken machen. Es muss Betreibern von Produktionsanlagen sowie Dienstleistern, die solche Unternehmen begleiten, klar sein, dass die I4.0 nicht nur mit Vorteilen verbunden sein kann, sondern an einigen Stellen auch Nachteile in Kauf genommen werden müssen. Ein Beispiel in dem das Nutzen-Risiko-Verhältnis genau betrachtet werden sollte, ist der direkte Zugriff von Smartphones und Tablets auf die Produktions-IT.[498] Auch wenn es technisch ohne weiteres realisierbar und ein Nutzen nicht von der Hand zu weisen ist, muss doch hinterfragt werden, ob der Nutzen die entstehenden Risiken überwiegt.

Solange noch keine I4.0-spezifischen Best-Practice-Sammlungen, Leitfäden und Standards existieren, die Fragen der IT-Sicherheit umfassend behandeln, sollten sich Betreiber von Produktionsanlagen sowie solche Unternehmen begleitende Dienstleister bei der Planung und Umsetzung organisatorischer IT-Sicherheitsmaßnahmen an vorhandenen, teils auf die industrielle Produktion spezialisierten Leitfäden und Standards für die IT-Sicherheit orientieren.

496 s. Kagermann a.a.O. 2013, S. 43ff, 65; Bauer et al. 2014, S. 24 f.; Bauernhansl et al. 2014 a.a.O., S. 124; Botthof und Hartmann 2015a, S. 103.

497 s. Fallenbeck, Niels; Eckert, Claudia (2014): IT-Sicherheit und Cloud Computing. In: Thomas Bauernhansl, Michael ten Hompel und Birgit Vogel-Heuser (Hg.): Industrie 4.0 in Produktion, Automatisierung und Logistik. Anwendung, Technologien und Migration. 1. Aufl. Wiesbaden: Springer Vieweg, S. 397–431, S. 414.

498 s.Bauer et al. 2014 a.a.O., S. 9; Hoffmann, Franz-Josef (2014): iBin – Anthropomatik schafft revolutionäre Logistik-Lösungen. In: Thomas Bauernhansl, Michael ten Hompel und Birgit Vogel-Heuser (Hg.): Industrie 4.0 in Produktion, Automatisierung und Logistik. Anwendung, Technologien und Migration. 1. Aufl. Wiesbaden: Springer Vieweg, S. 207–220, S. 213 ff.

Während bei Richtlinien und Verfahren mit einem größeren Anpassungsbedarf an die betrieblichen Erfordernisse zu rechnen ist, dürften sich unbedingt notwendige Anpassungen bei Methoden und Werkzeugen in Grenzen halten. Bei Schulungen und Sensibilisierungsmaßnahmen ist eine Anpassung der Inhalte an die betrieblichen Erfordernisse unvermeidlich – das ist aber kein I4.0-spezifischer Aufwand. Zusätzlich ist vor allem im Hinblick auf Richtlinien und Verfahren das Ergreifen von Maßnahmen ratsam, die die Einhaltung derselben sicherstellen oder zumindest fördern.

6.2.2 Rolle des Menschen in von der Industrie 4.0 beeinflussten Prozessen

Menschen sind aufgrund der zunehmenden Vernetzung und Automatisierung der industriellen Produktion mit unzähligen Veränderungen konfrontiert.[499] Während im Hinblick auf die Technikintegration von einer relativ langsamen Entwicklung hin zur I4.0 auszugehen ist, verändert sich die Rolle des Menschen mit deutlich höherem Tempo.[500] Der Mensch ist nicht nur eine Komponente im Konzept I4.0, er ist als Mitarbeiter ein von Angreifern besonders häufig genutzter Zugang zu Unternehmensgeheimnissen. Die meisten technischen Maßnahmen, um IT-Sicherheit zu gewährleisten, lassen sich durch einen fachkundigen Menschen innerhalb des Unternehmens umgehen, weshalb es im Umfeld der IT-Sicherheit notwendig ist, auch die Rolle und die Verantwortung des Menschen im Kontext von IT-Sicherheitsmaßnahmen zu beleuchten. Im Folgenden werden Ansätze beschrieben, die einen Umgang mit diesen Veränderungen erleichtern und dadurch helfen, in der sich ändernden Rolle des Menschen begründete Hemmnisse auszuräumen. Eine eigehende Beschäftigung mit dem Faktor Mensch sowie mit Fragen der Organisationsentwicklung und insbesondere des Change Managements, ist insofern wichtig, da der Mensch nicht nur eine zentrale Schwachstelle in einem mehr und mehr automatisierten Prozess darstellt, sondern gleichzeitig im Hinblick auf die Gestaltung und Überwachung der Prozesse sowie vor allem auch bei der Lösung von unvorhergesehenen Problemen vorerst unersetzbar bleibt.[501] Menschen spielen auch im Hinblick auf Vertrauen in die Technik, in Kooperationspartner entlang der Wertschöpfungskette und in die Vision von I4.0 eine wesentliche Rolle. Aus diesem Grund wird die Rolle des Menschen in diesem Kapitel im Zusammenhang mit Vertrauen nochmals aufgegriffen.

Es ist natürlich und verständlich, wenn Menschen mit Unbehagen auf Veränderungen reagieren, weil diese mit dem Aufbrechen vertrauter Routinen und dadurch mit Unsicherheiten verbunden sind.[502] Im Hinblick auf die IT-Sicherheit kann dieses Unbehagen zu menschlichem Fehlverhalten, vor allem bei der Umsetzung von Richtlinien und Verfahren, führen – in Extremfällen ist sogar denkbar, dass sich Mitarbeiter gegen das eigene Unternehmen wenden. Für den Arbeitsalltag bedeutet dies, dass dem Mitarbeiter bewusst sein muss, was von ihm erwartet wird und dass er weiß, dass sein Arbeitsplatz nicht gefährdet ist, solange er die an ihn gestellten Erwartungen erfüllt.[503] Das Konzept I4.0 bringt nun weitreichende Änderungen mit sich, die auch Einschränkungen der erlebten Freiräume, wie zum Beispiel das Einbüßen von Privilegien oder Machtempfinden, mit sich bringen können.

Aufbauend auf wirtschaftspsychologischen Erkenntnissen könnte ein Lösungsansatz etwa darin bestehen, die Neuausrichtung als Chance zu sehen und den Mitarbeitern auch so zu vermitteln. In der Praxis hat sich dazu der Einsatz von Promotoren, etwa nach dem Modell von Witte[504], bewährt. Promotoren sind Personen, die einen Änderungsprozess aktiv und intensiv fördern – nicht nur, aber auch im Bereich IT-Sicherheit. Hauptaufgabe von Promotoren ist es Willens- und Fähigkeitsbarrieren der Mitarbeiter abzubauen und zu überwinden. Auch ein Einsatz von Projektteams und gegebenenfalls einer Pilotumgebung bietet sich zur Überwindung möglicher Hemmnisse an.

Der mit I4.0 einhergehende Wandel erfordert, vor allem auch in KMU, immer mehr Interdisziplinarität sowie die Arbeit in interdisziplinären Teams. Doch auch die Qualifizierungsbedarfe auf der fachlichen und methodischen Ebene, vor allem auch aufgrund der neuen Herausforderungen im Bereich IT-Sicherheit, sind nicht zu vernachlässigen. Sowohl die Anforderungen an Mitarbeiter, die mit dem Aufbau und der Betreuung der Produktionsumgebung betraut sind, als auch jene an Mitarbeiter die Anlagen

499 s. Kagermann 2013 a.a.O., S. 59, 100; Bauer et al. 2014, S. 8.
500 s. Kagermann 2013 a.a.O., S. 6, 27; Bauer et al. 2014, S. 9; Botthof und Hartmann 2015a, S. 131.
501 s. Bauer et al. 2014, S. 38.
502 s. Barrantes/Zülch: „Die erfolgreiche Implementierung fernerbrachter Dienstleistungen“ in: Meier (Hg.): Embedded Online Service, Frankfurt 2004, S. 43–52.
503 s. Ebenda.
504 s. Witte, E.: Organisation für Innovationsentscheidungen – Das Promotoren-Modell. Göttingen 1973.

bedienen oder überwachen wachsen rasant und erfordern flankierende Schulungsmaßnahmen. Auch wenn die IT-Sicherheit nicht das einzige Thema ist, das es vertieft zu behandeln gilt, ist es doch ein Zentrales. Die zunehmende Komplexität und Dynamik der industriellen Produktion der Zukunft erfordert von Mitarbeitern umfassenden Einblick in die betrieblichen und überbetrieblichen Strukturen und Prozesse. Gleichzeitig führt die Konzentration von Möglichkeiten und Wissen bei einzelnen Mitarbeitern aber auch zu besonderen Gefahren. Aus diesem Grund ist neben regelmäßigen Schulungen auch eine gewissenhafte Personalauswahl notwendig. Der Forschungsbedarf im Hinblick auf die Abwehr möglicher Angriffe, die menschliches Fehlverhalten ausnützen oder gezielt auf Social Engineering setzen, ist noch erheblich. Vorhandene wirtschaftspsychologische Erkenntnisse sollten als Ausgangpunkt für die Untersuchung von I4.0-spezifischen Fragestellungen mit IT-Sicherheitsbezug dienen. Im Hinblick auf Schulungen würden beispielsweise multidisziplinäre Maßnahmen von Verbänden eine gute Möglichkeit bieten, auch über Unternehmensgrenzen hinweg zu lernen – was vor allem für KMU hilfreich wäre. Zentral ist, dass Produktionswissen und IT-Wissen zusammengeführt werden. In solchen Schulungen sollte auch ein Bewusstsein für das notwendige Zusammenwirken von Recht, Organisation und Technik zur Gewährleistung eines angemessenen IT-Sicherheitsniveaus im Kontext von I4.0 vermittelt werden.

Ein weiterer Ansatz besteht in der Entwicklung von Assistenzsystemen, die dem Menschen dann weiterhelfen, wenn er zusätzlichen Informationsbedarf hat. Es ist offensichtlich, dass entsprechende Systeme auch im Kontext der Umsetzung von organisatorischen IT-Sicherheitsmaßnahmen hilfreich sein können.[505] Gezielte Auswertungen von Ereignissen und kontinuierliche Verbesserungen führen im Idealfall zu einem lernenden System, das im Zeitverlauf immer besser darin wird, den Menschen zu unterstützen. Vor allem angesichts der Komplexität und Dynamik der Produktion in der I4.0 sind geeignete Assistenzsysteme zunehmend von Bedeutung, etwa zur Unterstützung des IT-Sicherheitsmanagements. Der Einsatz solcher Systeme könnte zu einem gewissen Grad auch eine Möglichkeit zur Erhaltung der Arbeitsplätze gering qualifizierter Mitarbeiter darstellen. Der Wandel hin zu einer industriellen Produktion der Zukunft reduziert die monotonen Tätigkeiten für Mitarbeiter und erhöht damit die Anforderungen.

6.2.3 Vertrauen in die Technik, in die Kooperationspartner und die Vision von Industrie 4.0

Für die Hemmnisse, die mit dem Vertrauen in die Technik, in die Kooperationspartner und die Vision von I4.0 zusammenhängen, existieren nur wenige konkrete Lösungsansätze. Vertrauen hängt sehr eng mit der Überzeugung zusammen, dass trotz der für die Produktion der Zukunft erwarteten hohen Komplexität und Dynamik ein angemessenes IT-Sicherheitsniveau gewährleistet werden kann.

Grundlegendes Vertrauen in das Konzept oder die Vision von I4.0 kann zu einem gewissen Grad durch eine breite Diskussion und Aufklärung erreicht werden. Es muss verständlich gemacht werden, dass auch KMU kurz vor dem bedeutenden Sprung in die vierte industrielle Revolution stehen. Der damit verbundene Wandel setzt auf Interdisziplinarität[506], worunter die Nutzung von Ansätzen, Denkweisen oder Methoden verschiedener Fachrichtungen zu verstehen ist. Ein Ansatz Vertrauen zu schaffen, besteht darin, den Wandel als zentrales Innovationsthema im Unternehmen zu verstehen und entsprechend top-down zu treiben und zu kommunizieren. Positive Erfahrungsberichte aus anderen Unternehmen und Branchen können den Prozess der Vertrauensbildung unterstützen. Eine schrittweise Einführung innerhalb des Unternehmens macht die Entwicklung besser nachvollziehbar und hilft Hemmschwellen und Widerstände abzubauen. Der Prozess kann durch den Aufbau von Systemvertrauen, zum Beispiel durch den Einsatz von zertifizierten Produkten und Prozessen, zusätzlich unterstützt werden.

Bestehende Kooperationen können genutzt werden, um I4.0-Pilotprojekte in einem etablierten Umfeld zu testen und um sie zu vertiefen. Vertrauen in Kooperationen kann gestärkt werden, indem gemeinsam – zumindest für die bestehende Wertschöpfungskette – Mindeststandards, nicht nur aus technischer Sicht, sondern auch im Hinblick auf Strukturen und Prozesse, definiert und eingehalten werden. Auch die erforderlichen, aber für viele Unternehmen völlig neuen, formalisierten Regelungen für die Datennutzung und den Datenaustausch können innerhalb der bestehenden Vertrauensbeziehung diskutiert und nach Bedarf angepasst werden. Hier sprechen der zeitliche Vorlauf und das bestehende persönliche Vertrauen für die Adressierung innerhalb einer bestehenden Kooperation. Der betriebliche

505 s. Fallenbeck, Eckert a.a.O., S. 413.

506 s. Kagermann et al. 2013, S. 59, 62; Günthner, Willibald; Klenk, Eva; Tenerowicz-Wirth, Peter (2014): Adaptive Logistiksysteme als Wegbereiter der Industrie 4.0. In: Thomas Bauernhansl, Michael ten Hompel und Birgit Vogel-Heuser (Hg.) a.a.O., S. 296–323, S. 310; Kagermann, Henning (2014): Chancen von Industrie 4.0 nutzen. In: Thomas Bauernhansl, Michael ten Hompel und Birgit Vogel-Heuser (Hg.) a.a.O., S. 603–614, S. 608; Botthof und Hartmann 2015a, S. 36.

Alltag, der nicht selten durch hohen Erfolgsdruck geprägt ist, lässt Unternehmen zu wenig Raum, sich neben den technischen auch mit den rechtlich-organisatorischen Gegebenheiten zu beschäftigen. In diesem Zusammenhang würden auch Musterverträge zur sicheren unternehmensübergreifenden Datennutzung und zum sicheren Datenaustausch mit Unternehmen, die sich auf unbekanntem Terrain befinden, unterstützen.

6.2.4 Fazit

Mit dem Konzept von I4.0 entstehen vielfältige Herausforderungen gerade für KMU. Nicht wenige davon betreffen die IT-Sicherheit und fast alle erfordern den Aufbau spezieller Kompetenzen. Da es für KMU weder möglich noch sinnvoll ist, alle geforderten Kompetenzen selbst aufzubauen, werden sie in einigen Bereichen auf Dienstleister zurückgreifen müssen. Da diese vor allem im Bereich der IT-Sicherheit nur unterstützen, nicht aber die Verantwortung abnehmen können, sind KMU gefordert, sich selbst eine umfassende Strategie zu erarbeiten und das Unternehmen auf allen Ebenen auf die Herausforderungen vorzubereiten.

Ein guter Ansatzpunkt dazu ist der Rückgriff auf Erfahrungsberichte, Best-Practice-Sammlungen und Handlungsleitfäden. Diese sind nicht nur für Betreiber von Produktionsanlagen relevant, sondern auch für Dienstleister die Unternehmen auf dem Weg zu einer hochgradig vernetzten und automatisierten industriellen Produktion begleiten möchten.

Ein weiterer zentraler Punkt aus organisatorischer Sicht ist das Vorantreiben der Standardisierung unter Einbeziehung der KMU. Zu beachten ist bei der Ausgestaltung vor allem, dass die Standards umsetzbar und mit verhältnismäßigem Aufwand überprüfbar bleiben müssen – nur so kann vermieden werden, dass bestimmte, vor allem kleine Unternehmen von der Teilnahme an der I4.0 ausgeschlossen werden. Darüber hinaus erscheint auch eine Abstimmung auf internationaler Ebene sinnvoll. Der Einsatz von Standardprodukten, wie auch die Umsetzung von standardisierten Strukturen und Prozessen, bietet ein höheres Maß an Sicherheit für strategische Entscheidungen. Im Zusammenhang mit Mindeststandards geht es in erster Linie um die zweckmäßige Integration und Anwendung bestehender Standards.

Um die wesentliche Rolle des Menschen im Konzept von I4.0 und vor allem die damit einhergehende Verantwortung für Informationen und Prozesse zu gestalten, bedarf es multidisziplinärer Schulungsmaßnahmen, geeigneter Assistenzsysteme und sinnvollerweise auch des Einsatzes von Promotoren, die die Änderungen im Unternehmen begleiten und positiv verstärken.

Begleitend können positive Erfahrungsberichte aus anderen Unternehmen und Branchen den Prozess der Vertrauensbildung unterstützen. Eine schrittweise Einführung innerhalb des Unternehmens macht die Entwicklung besser nachvollziehbar und hilft Hemmschwellen und Widerstände abzubauen.

Zusammenfassend lässt sich festhalten, dass IT-Sicherheit im Umfeld von I4.0 auch organisatorischer Maßnahmen bedarf, die in ihrer Gesamtheit am ehesten zu erfassen sind, wenn der bevorstehende Wandel als zentrales Innovationsthema im Unternehmen betrachtet und aus allen Perspektiven gleichrangig angegangen wird.

6.3 Rechtliche Konzepte zur IT-Sicherheit in der Industrie 4.0

In diesem Abschnitt werden, ausgehend von den Ergebnissen der bisherigen Untersuchung, aktuelle Konzepte zur IT-Sicherheit im Hinblick auf ihre Leistungsfähigkeit zur Verbesserung der IT-Sicherheit in I4.0 untersucht. Die Untersuchung kann im Rahmen dieser Studie nur exemplarisch erfolgen. Daher werden nachfolgend zwei Ansätze erörtert, die insoweit von Bedeutung sind: das IT-Sicherheits-Gesetz (Abschnitt 6.3.1) und die Zertifizierung mit Bezug zur IT-Sicherheit (Abschnitt 6.3.2). Abschließend werden Folgerungen für den rechtlichen Rahmen für IT-Sicherheit gezogen (Abschnitt 6.3.3).

6.3.1 Das IT-Sicherheitsgesetz

6.3.1.1 Überblick

Am 25. Februar 2015 hat die Bundesregierung den Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vorgelegt.[507] Der Bundestag hat das Gesetz am 12. Juni 2015 entsprechend der Beschlussempfehlung des Innenausschusses, die einige

507 Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), BT-Drs. 18/4096, 25.02.2015.

Änderungen vorsieht[508], beschlossen. Das Gesetz ist am 25. Juli 2015 in Kraft getreten. Ziel des Gesetzes ist ausweislich der Gesetzesbegründung eine „signifikante Verbesserung der Sicherheit informationstechnischer Systeme (IT-Sicherheit) in Deutschland".[509]

Die Gesetzesbegründung nennt eine Reihe von Einzelzielen. So soll der „Schutz der Systeme im Hinblick auf die Schutzgüter der IT-Sicherheit" erhöht werden, die „IT-Sicherheit bei Unternehmen" soll verbessert, und es soll weiterhin ein verstärkter Schutz der Bürger im Internet sowie eine „Stärkung" des BSI erreicht werden.

Das Gesetz dient zugleich der Umsetzung der künftigen NIS-Richtlinie (Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit), deren Entwurf die EU-Kommission im Februar 2013 vorgelegt hat.[510] Die Richtlinie wird für die Regulierung der IT-Sicherheit möglicherweise von erheblicher Bedeutung sein. Sie soll ausweislich der Begründung des Kommissionsentwurfes eine hohe gemeinsame Netz- und Informationssicherheit (NIS) erreichen.[511] Angestrebt wird „die Erhöhung der Sicherheit des Internets und der privaten Netze und Informationssysteme, die für das Funktionieren unserer Gesellschaften und Volkswirtschaften unverzichtbar sind."[512]

Die Richtlinie setzt bei Betreibern kritischer Infrastrukturen und „wichtige(n) Anbietern von Diensten der Informationsgesellschaft" an. Diese sollen „geeignete Schritte zur Beherrschung von Sicherheitsrisiken" unternehmen und „gravierende Sicherheitsvorfälle" melden.[513] Ziel der Richtlinie ist also nicht die IT-Sicherheit allgemein, sondern primär die Funktionsfähigkeit des Internets und wichtiger Dienste in verschiedenen Bereichen, wie Energie, Verkehr und Gesundheit.

Die Richtlinie befindet sich derzeit im europäischen Gesetzgebungsverfahren. Das Parlament hat dem Entwurf schon am 13. März 2014 zugestimmt, die Beratungen im Rat dauern an. Der Richtlinienentwurf sieht eine Umsetzungsfrist von 18 Monaten vor.

Das IT-Sicherheitsgesetz ist ein Artikelgesetz, das mehrere Gesetze ändert. Die umfangreichsten Änderungen sind für das BSI-Gesetz vorgesehen, in dem die Regelungen für kritische Infrastrukturen zusammengefasst werden. Weiterhin sollen das Energiewirtschaftsgesetz, das Telekommunikationsgesetz, das Atomgesetz und das Telemediengesetz geändert werden.

Das IT-Sicherheitsgesetz enthält zwei Regelungsbereiche unterschiedlicher Art. Zum einen werden Sicherungsmaßnehmen für kritische Infrastrukturen geregelt, und zum anderen Sicherungsmaßnahmen für Telemedien. Die Regelungen unterscheiden sich sehr deutlich: Für kritische Infrastrukturen sieht das Gesetz jeweils vor allem zwei Instrumente zur Verbesserung der IT-Sicherheit vor: eine Pflicht zur Vornahme von Maßnahmen zur Gewährleistung der IT-Sicherheit und eine Pflicht zur Meldung von Sicherheitsvorfällen. Bei Telemedien fehlt die Meldepflicht. Hier bleibt es bei materiellen Anforderungen an die IT-Sicherheit. Nachfolgend werden die beiden Regelungsgegenstände im Hinblick auf ihre Bedeutung für die IT-Sicherheit untersucht.

6.3.1.2 Die Pflichten der Betreiber von Telemediendiensten

Durch das IT-Sicherheitsgesetz wird in das TMG ein neuer § 13 Abs. 7 TMG eingefügt, der die Anbieter geschäftsmäßig angebotener Telemedien zu technischen und organisatorischen Schutzmaßnahmen verpflichtet.

6.3.1.2.1 Anwendungsbereich

Diese Schutzpflichten gelten nach dem § 13 Abs. 7 TMG für alle geschäftsmäßigen Telemedien. Der Bereich der Telemedien ist sehr weit und umfasst insbesondere Websites und die über Websites zugängigen Dienste.

508 BT-Drucks. 18/4096.
509 Begr. RegE IT-SicherheitsG, A. I. BT-Drucks. 18/4096, S. 19.
510 Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, 07.02.2013, COM (2013) 48 endg., 2013/0027 (COD).
511 Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, 07.02.2013, COM (2013) 48 final, 2013/0027 (COD). S. 2.
512 Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, 07.02.2013, COM (2013) 48 final, 2013/0027 (COD). S. 2.
513 Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, 07.02.2013, COM (2013) 48 final, 2013/0027 (COD). S. 2.

Nach der Begründung sind Telemedien „geschäftsmäßig", soweit sie auf einer nachhaltigen, also planmäßigen und dauerhaften Tätigkeit beruhen.[514] Bei entgeltlichen Diensten wie werbefinanzierten Seiten sei dies in der Regel gegeben, nicht-kommerzielle Websites von Privaten oder Idealvereinen seien dagegen ausgenommen.[515] Mit dem Begriff der Geschäftsmäßigkeit soll also offensichtlich dieselbe Eingrenzung des Adressatenkreises vorgenommen werden, die auch für die Impressumspflicht nach § 5 TMG gilt.[516] Dort spricht das Gesetz allerdings von „geschäftsmäßigen, in der Regel gegen Entgelt angebotenen" Diensten. Dies versteht die Bundesregierung aber offenbar synonym. Auch im Rahmen des § 5 TMG ist der Adressatenkreis letztlich aber unklar und umstritten. Diese Unklarheit wird nun auf die sicherheitsbezogenen Pflichten erweitert.

Inwieweit § 13 Abs. 7 TMG im Bereich der I4.0 anwendbar ist, ist unklar. Zwar sind alle Industrieunternehmen, soweit sie Websites unterhalten, Adressaten des Gesetzes. Fraglich ist aber, inwieweit eigentliche Bereich der I4.0 erfasst sind. Elektronische Kommunikation innerhalb eines Unternehmens ist nicht erfasst. Inwieweit Kommunikationsbeziehungen in Netzen eines geschlossenen Kreises von Kommunikationsteilnehmern, wie sie der Kooperation in der I4.0 entspricht, erfasst werden, muss derzeit noch als offen angesehen werden. Es spricht aber einiges dafür, dass sie jedenfalls nicht generell erfasst werden, da Telemedien Dienste sind, die sich an die Öffentlichkeit richten. Dies ist bei geschlossenen Systemen jedenfalls bei einer begrenzten Zahl von Teilnehmern nicht der Fall.

6.3.1.2.2 Schutzpflichten der Betreiber

Der Inhalt der Pflichten nach § 13 Abs. 7 TMG ist recht unklar. Die Norm lautet: „Diensteanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1. kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und
2. diese

a) gegen Verletzungen des Schutzes personenbezogener Daten und

b) gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind,

gesichert sind. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens."

Bei Ziffer 1 geht es wohl vor allem um den Schutz des Webservers gegen Angriffe. In Ziffer 2 sind wohl nicht (nur) die technischen Einrichtung sondern (auch) die Telemedien, also die Dienste, gemeint. Mit dem in lit. a) genannten Schutz gegen Verletzungen von personenbezogenen Daten ist wohl auch der Schutz von Zugriffen Unbefugter auf Nutzerkonten gemeint. Die Dienste, wohl auch die Einrichtungen als solche, sind nach Ziffer 2 lit. b) gegen Störungen, auch durch Angriffe zu schützen. Die Pflicht nach Ziff. 2 lit. a) ist sprachlich kaum verständlich, denn es fragt sich, wann eine solche Verletzung des Schutzes personenbezogener Daten vorliegt. Möglicherweise soll hier eine ähnliche Regelung wie nach § 9 BDSG getroffen werden, der allerdings für Anbieter von Telemedien ohnehin gilt.

Die Gesetzesbegründung beschreibt, welches Ziel die Bundesregierung mit der Norm verfolgt. Es ist indes ein anderes als der Wortlaut indiziert. Nach der Gesetzesvorlage soll die Regelung die Verbreitung von Schadsoftware durch Drive-by-Downloads bekämpfen. Als insoweit geeignete technische Maßnahme sieht die Bundesregierung die Aktualisierung von Software, insbesondere durch Sicherheitspatches seitens der Betreiber von Websites an. Darüber hinaus soll der Betreiber der Website als organisatorische Maßnahme Werbedienstleistern, denen er gestattet, Inhalte, etwa Werbebanner, auf der Website einzubringen, eine entsprechende vorherige Vertragspflicht auferlegen.[517]

Es geht aber auch der Bundesregierung um mehr, denn die Gesetzesbegründung erwähnt das Erfordernis angemessener Authentifizierungsverfahren. Dieses Ziel ist zu begrüßen.

514 Begr. RegE zu Art. 4 Nr. 1 lit. a IT-SicherheitsG, BT-Drucks. 18/4096, S. 34.
515 Begr. RegE zu Art. 4 Nr. 1 lit. a IT-SicherheitsG, BT-Drucks. 18/4096, S. 34.
516 Vgl. Begr. RegE zu § 4 TDG a. F., BT-Drs. 14/6098, S. 17; Brönnecke, in Roßnagel, § 5 TMG Rn. 41; Micklitz/Schirmbacher, in: Spindler/Schuster, § 5 TMG Rn. 8; Ott, in: BeckOK Informations- und Medienrecht, § 5 TMG Rn. 9.
517 Begr. RegE zu Art. 4 Nr. 1 lit. a IT-SicherheitsG (§ 13 TMG), BT-Drucks. 18/4096, S. 34.

In der Tat war die Pflicht der Webseiten-Betreiber, ihre Nutzer durch angemessene Authentifizierungsverfahren zu schützen, bisher nicht ausdrücklich gesetzlich geregelt. Sie wurde allerdings aus § 13 Abs. 4 S. 3 TMG hergeleitet[518] und ergab sich zudem aus § 9 BDSG, aus § 823 Abs. 1 BGB und, als vertragliche Nebenpflicht, aus dem Vertrag mit dem Nutzer.

Unklar ist das Verhältnis des § 13 Abs. 7 Nr. 2 lit. a) TMG zu § 9 BDSG, der die Pflicht zum Schutz personenbezogener Daten umfassend regelt. Es ist unklar, ob und welche Sonderregel hier getroffen werden soll.

Die nach § 13 Abs. 7 TMG gebotenen Schutzmaßnahmen werden nicht näher beschrieben. Es wird auch aus der Gesetzesbegründung nicht klar, welche Pflicht mit der „Berücksichtigung des Standes der Technik" gemeint ist. In der Gesetzesbegründung findet sich die Aussage, dass Authentifizierungsverfahren nach den Technischen Richtlinien des BSI „jedenfalls als dem Stand der Technik gemäß hinreichend sicher anzusehen" seien.[519] Ob dies impliziert, dass „Berücksichtigung des Standes der Technik" gleichbedeutend sein soll mit Sicherheit „gemäß dem Stand der Technik", bleibt unklar.

Interessant ist, dass die Technischen Richtlinien des BSI wohl als Maßstab für den Stand der Technik fungieren sollen. Eine solche Funktion der Technischen Richtlinien des BSI ist bisher weder vom Gesetz angeordnet noch in Rechtsprechung oder Literatur anerkannt. Es ist letztlich auch unklar, welche konkrete Bedeutung die Richtlinien haben sollen. Insoweit sind weitere Arbeiten erforderlich, um Rechtssicherheit herzustellen.

6.3.1.2.3 Durchsetzungsmechanismen

Der Gesetzesentwurf sieht keine spezifische Regelung zur Durchsetzung der Pflicht nach § 13 Abs. 7 TMG vor. Das TMG enthält generell keine Regelung für Verstöße gegen seine Regelungen, so dass stets die allgemeinen Regelungen des Zivilrechts maßgeblich sind. Inwieweit diese zu einer wirkungsvollen Durchsetzung der Pflicht nach § 13 Abs. 7 TMG führen, ist kaum abzusehen. § 13 Abs. 7 TMG ist kein Schutzgesetz im Sinne von § 823 Abs. 2 BGB, jedoch wird nicht selten eine Haftung nach § 823 Abs. 1 BGB in Betracht kommen, ebenso eine Haftung wegen Verletzung vertraglicher Schutzpflichten, da § 13 Abs. 7 TMG eine vertragliche Schutzpflicht der Betreiber von Websites regelt. Allerdings treffen hier die allgemeinen Probleme der Regelung durch zivilrechtliche Haftung (oben 5.4.1.5) in besonderem Maße zu: Die Geschädigten müssten im Rahmen eines Zivilprozesses darlegen und nachweisen, dass der gebotene Sicherheitsmaßstab nicht eingehalten wurde und dass dieser kausal für eine Verletzung dieser Rechtsgüter war. Schon die erste Voraussetzung wird in aller Regel eine unüberwindbare Hürde darstellen, da der Sicherheitsmaßstab, wie dargestellt, unklar ist. Auch das Kausalitätserfordernis dürfte eine erhebliche Hürde darstellen, da oft nicht feststellbar sein wird, dass die Schädigung bei angemessener Sicherheit vermieden worden wäre.

Denkbar ist, dass der Verbandsklage nach dem UWG im Bereich des § 13 Abs. 7 TMG eine Bedeutung zukommen könnte, da § 13 Abs. 7 TMG wohl als marktverhaltensrelevante Norm i. S. des § 4 Nr. 11 UWG anzusehen ist. Die in § 13 Abs. 7 TMG geregelten Anforderungen an die Authentisierung können erhebliche Bedeutung für die Nutzerfreundlichkeit eines elektronischen Marktplatzes oder Webshops haben, so dass die Anforderungen an die Schutzmaßnahmen beim Log-In eine erhebliche Bedeutung für den Wettbewerb haben. Ob dieses Instrument in der Praxis einmal genutzt wird, ist freilich nicht absehbar.

Öffentlich-rechtliche Mechanismen, etwa eine behördliche Aufsicht, sieht das Gesetz nicht vor. Insbesondere erhält das BSI weder Aufgaben noch Befugnisse, aufsichtsrechtlich tätig zu werden. Eine aufsichtsrechtliche Kontrolle ist nach geltendem Recht zwar bereits nach Datenschutzrecht gegeben, da die in § 13 Abs. 7 TMG betroffenen Unternehmer in aller Regel personenbezogene Daten verarbeiten und somit das datenschutzrechtliche Instrumentarium zur Verfügung steht. Diese ist aber, wie dargestellt, bisher weitgehend wirkungslos.

6.3.1.2.4 Zwischenergebnis

Letztlich bleibt die Regelung des TMG inhaltlich unklar. Es ist nicht erkennbar, ob hier eine punktuelle Reglung getroffen werden soll oder eine allgemeine Pflicht zur Wahrung hinreichender IT-Sicherheit. Offen ist, inwieweit die Regelung über die § 9 BDSG hinausgehen soll und es ist fragwürdig, warum ein Schutz gegen Störungen zur rechtlichen Pflicht gemacht wird. Schließlich ist der Inhalt der Pflicht offen.

518 Jandt/Schaar/Schulz, in Roßnagel Recht der Telemediendienste (2012), § 13 TMG Rn. 109; wohl auch: Müller-Broich, Telemediengesetz, 2012, § 13 TMG Rn. 7.

519 Begr. RegE zu Art. 4 Nr. 1 lit. a IT-SicherheitsG (§ 13 TMG), BT-Drucks. 18/4096, S. 35.

Angesichts des extrem weiten Anwendungsbereichs der Pflicht, die Millionen von Anbietern betrifft, sind diese Mängel des Gesetzes äußerst bedauerlich.

Inwieweit § 13 Abs. 7 TMG für die I4.0 von Bedeutung ist, ist unklar. Es ist insbesondere unklar, ob und in welchen Fällen die Norm auf die für I4.0 charakteristische Kooperation anwendbar ist. Anzunehmen ist, dass diese von Art. 13 Abs. 7 TMG nicht erfasst wird, so dass die Norm für I4.0 letztlich nicht gilt.

6.3.1.3 Die Regelung zu kritischen Infrastrukturen

Im Vordergrund der aktuellen Diskussion zum IT-Sicherheitsgesetz stehen die Regeln zum Schutz kritischer Infrastrukturen.

6.3.1.3.1 Der Anwendungsbereich der Regeln zu kritischen Infrastrukturen

Das IT-Sicherheitsgesetz soll, genau wie die NIS-Richtlinie, zwar umfassend zu Verbesserungen der IT-Sicherheit beitragen, adressiert aber einen spezifischen Bereich der Wirtschaft, die Betreiber kritischer Infrastrukturen und die durch die besonderen Gesetze erfassten Unternehmen im Bereich der Energieversorgung, Telekommunikation und Telemedien. Dabei gehören die durch die Regeln zur Energieversorgung und Telekommunikation erfassten Bereiche sachlich zu den kritischen Infrastrukturen, während die Regelung zu den Telemedien, wie dargestellt, eine völlig andersartige Struktur hat.

Der Anwendungsbereich ist jedoch in den einzelnen Gesetzen durchaus unterschiedlich geregelt. Neu ist der Bereich der kritischen Infrastruktur, der im BSI-Gesetz geregelt ist.

Der Begriff der kritischen Infrastruktur ist in § 2 Abs. 10 BSI-G durch zwei Merkmale geregelt. Es handelt sich um Einrichtungen in besonderen Sektoren, die enumerativ aufgeführt sind und etwa „Informationstechnik und Telekommunikation“, „Gesundheit“, und „Ernährung“ umfassen. Als weiteres Merkmal müssen die Einrichtungen „von hoher Bedeutung für das Funktionieren des Gemeinwesens“ sein. Dies wird näher bestimmt durch die Anforderung, dass ihr „Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit“ zur Folge hätte.[520]

Industrie und Dienstleistungen sind (bis auf das Finanz- und Versicherungswesen) aus dem Anwendungsbereich ausgenommen. Dies ist im Hinblick auf „Industrie 4.0“ erstaunlich. Gravierend sind die Mängel des zweiten Abgrenzungsmerkmals: Der Begriff der „erheblichen Versorgungsengpässe“ ist arg ungenau, mehr noch der Begriff der „öffentlichen Sicherheit“, der aus dem Polizeirecht bekannt ist, hier aber nach der Gesetzesbegründung völlig anders zu verstehen ist und eine Gefahr von Leib, Leben, Gesundheit und Eigentum von „Teilen der Bevölkerung“ meint.[521]

Die Definition soll durch eine Rechtsverordnung näher bestimmt werden. Ob die Regelung verfassungsgemäß ist, ist in der Literatur umstritten.

Inhaltich ist die Regelung insoweit nicht überzeugend, als ein hinreichendes Maß an IT-Sicherheit auch für die übrigen Bereiche erforderlich ist. Verständlich wird diese Beschränkung aber vor dem Hintergrund, dass das Gesetz letztlich nur in Bezug auf die Meldepflichten sachliche Änderungen bringt (dazu unten). Der Anwendungsbereich weicht von der Definition des NIS-Richtlinienentwurfs zumindest insoweit ab, als dass die Richtlinie den Bereich der „Informationstechnik und Telekommunikation“ nicht nennt.

Das BSI-G enthält in § 8c Ausnahmen für die besonderen Pflichten bei kritischen Infrastrukturen. Nach § 8c Abs. 1 BSI-G sind Kleinstunternehmen mit weniger als zehn Mitarbeitern ausgenommen. Nach § 8c Abs. 2 Nr. 1 bzw. Abs. 3 Nr. 1 BSI-G sind Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste ausgenommen, da diese nach dem TKG vergleichbaren Bestimmungen unterliegen.

Die für Telekommunikation ausdrücklich genannte Ausnahme wird in § 8c Abs. 2 Nr. 4, Abs. 3 Nr. 4 BSI-G erweitert. Danach gelten die Pflichten nicht, wenn die Betreiber der

520 § 2 Abs. 10 BSIG-E lautet: „Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die
1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und
2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt.“

521 Begr. RegE zu Art. 1 Nr. 8 a) IT-SicherheitsG = § 10 Abs. 1 BSIG, BT-Drucks. 18/4096, S. 31.

kritischen Infrastruktur nach anderen Gesetzten schon vergleichbaren Pflichten unterliegen, der § 8a BSI-G soll also subsidiär sein.

Allerdings ist die Reichweite dieser Subsidiarität unklar. Tatsächlich bestehen nach § 823 Abs. 1 BGB und nach § 9 BDSG bereits vergleichbare Pflichten. Gegenüber diesen allgemeinen Regelungen soll aber die Subsidiarität nicht eingreifen.

6.3.1.3.2 Die materiellen Schutzpflichten der Betreiber kritischer Infrastrukturen

Das IT-Sicherheitsgesetz setzt im Bereich der kritischen Infrastrukturen auf zwei Instrumente: § 8a BSI-G regelt materielle Pflichten der Betreiber kritischer Infrastrukturen in Bezug auf IT-Sicherheit. § 8b BSI-G regelt eine Meldepflicht der Betreiber kritischer Infrastrukturen bei IT-Sicherheitsvorfällen. Die beiden Instrumente sind letztlich voneinander unabhängig. Für die Zwecke dieser Untersuchung sind vor allem die materiellen Schutzpflichten von Interesse.

(1) Die Regelung des IT-Sicherheitsgesetzes

Die zentrale Norm in Bezug auf die materiellen Schutzpflichten ist § 8a Abs. 1 S. 1 BSI-G[522], der die Betreiber kritischer Infrastrukturen zu IT-Sicherheit verpflichtet. Allerdings handelt es sich hierbei nicht um eine allgemeine Pflicht zur IT-Sicherheit. Wie aus dem Wortlaut deutlich wird, geht es um die Vermeidung von Störungen, die für die Funktionsfähigkeit der kritischen Infrastrukturen maßgeblich sind.

Damit wird das Ziel des Gesetzes, der Schutz der Funktionsfähigkeit der kritischen Infrastruktur, unmittelbar zum Maßstab der gesetzlichen Pflicht. Zugleich wird deutlich, dass die Pflicht nicht auf Individualschutz, sondern auf institutionellen Schutz abstellt. Dies bedeutet für die hier interessierende Fragestellung, dass sich aus dem künftigen § 8a BSI-G keine unmittelbaren Pflichten und wohl auch kein Maßstab für die individualschützenden Pflichten zur Gewährleistung von IT-Sicherheit ergibt.

Hinsichtlich der inhaltlichen Anforderungen ist § 8a Abs. 1 S. 1 BSI-G eine Generalklausel, die auf „angemessene" Vorkehrungen verweist. Diese Regelung entspricht zahlreichen Parallelnormen, etwa dem § 9 Abs. 1 S. 1 BDSG, der ebenfalls angemessene Maßnahmen verlangt – freilich mit einem anderen Schutzziel.

(2) Der Stand der Technik im IT-SicherheitsG

Das IT-SicherheitsG verweist an mehreren Stellen auf den „Stand der Technik". So verpflichtet etwa § 8a Abs. 1 S. 2 BSI-G[523] die Betreiber kritischer Infrastrukturen, den Stand der Technik einzuhalten. Außerdem verpflichtet § 13 Abs. 7 S. 2 TMG Diensteanbieter nach TMG, bei den verpflichtenden technischen und organisatorischen Vorkehrungen nach § 13 Abs. 7 S. 1 TMG[524] den Stand der Technik zu berücksichtigen. Gleiches gilt nach § 109 S. 3 TKG[525] für Maßnahmen nach § 109 Abs. 2 S. 2 TKG zur Sicherung gegen unerlaubte Zugriffe und zur Schadensbegrenzung.

Diese Bezugnahme hat in der Diskussion über das IT-SicherheitsG eine recht prominente Rolle gespielt. So wurde etwa berichtet, das Gesetz verpflichte zur IT-Sicherheit nach dem Stand der Technik.[526] In allen Fällen bezieht sich die Bezugnahme auf den Stand der Technik auf die Angemessenheit der technischen und organisatorischen Vorkehrungen. Allerdings ist unklar, was damit gemeint ist. Offenbar soll die Bezugnahme auf den Stand der Technik zu einer Konkretisierung der Anforderungen führen. Allerdings ist schon der Begriff des Standes der Technik seinerseits ausfüllungsbedürftig.

522 § 8a Abs. 1 S. 1 BSIG-E lautet: „Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind."

523 § 8 Abs. 1 S. 2 BSI-G lautet: „Dabei soll der Stand der Technik eingehalten werden."

524 § 13 Abs. 7 S. 2 TMG lautet: „Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen."

525 § 109 S. 3 TKG-E lautet: „Bei Maßnahmen nach Satz 2 ist der Stand der Technik zu berücksichtigen."

526 Siehe etwa BITKOM, BITKOM begrüßt IT-Sicherheitsgesetz („Das Gesetz verpflichtet die Betreiber kritischer Infrastrukturen, ihre IT-Sicherheit zu verbessern und auf dem neuesten Stand der Technik zu halten"), abrufbar unter: https://www.bitkom.org/Presse/Presseinformation/Bitkom-begruesst-IT-Sicherheitsgesetz.html; Roos, Kampfansage an Hacker („Die entsprechenden Vorkehrungen müssen dem Stand der Technik entsprechen [...]."), abrufbar unter http://www.lto.de/recht/hintergruende/h/gesetzgebung-regierungsentwurf-it-sicherheitsgesetz-hacker-angriffe/; Schminkler, IT-Sicherheitsgesetz – zahnloser Tiger („Betreiber von Webseiten und Providern sollen verpflichtet werden, IT-Sicherheit, nach dem Stand der Technik' zu gewährleisten."), abrufbar unter https://www.tagesschau.de/inland/it-sicherheitsgesetz-101.html

Im Bereich des § 13 Abs. 7 TMG wird die Bezugnahme auf den Stand der Technik zudem auf eine „Berücksichtigung“ abgeschwächt. Offenbar soll das Gesetz keine strikte Bindung an den Stand der Technik regeln. Es ist aber unklar, was die Bezugnahme auf den Stand der Technik dann regeln soll. Der Stand der Technik in dem Sinne, wie er hier wohl auch zu verstehen sein soll, also als die Maßnahmen, die für die Zielerreichung geeignet und in der Praxis erprobt sind, kann insoweit ein Indiz für die Angemessenheit der Maßnahmen sein. Die Bezugnahme kann aber auch lediglich ein Hinweis darauf sein, dass sich die Anforderungen entsprechend dem technischen Fortschritt ändern. Die Bezugnahme auf den Stand der Technik in § 13 Abs. 7 TMG ist daher nicht weiterführend. Im Rahmen des § 8a BSI-G soll offenbar eine deutlichere Bindung an den Stand der Technik erfolgen. Allerdings ist insoweit das Verhältnis zur Angemessenheit der Maßnahme in Abs. 1 S. 1 unklar, die in Abs. 1 S. 3 eigenständig definiert wird. Maßgeblich ist letztlich Abs. 1 S. 1, die die Pflicht unmittelbar enthält. Möglicherweise ist Abs. 1 S. 2 deshalb als „soll“-Vorschrift formuliert.

(3) Selbstregulierung

§ 8a Abs. 2 BSI-G führt eine hochinteressante Möglichkeit zur Bestimmung der Pflichten nach § 8a Abs. 1 BSI-G ein. Danach können Betreiber kritischer Infrastrukturen und ihre Branchenverbände Sicherheitsstandards zu Gewährleistungen der Anforderungen nach Abs. 1 vorschlagen, und das BSI kann auf Antrag die Eignung der Standards feststellen. Das Gesetz nennt keine Rechtsfolge einer solchen Feststellung, aber es ist offensichtlich, dass die Wahrung der vom BSI festgestellten Standards als Erfüllung der in Abs. 1 geregelten Pflichten ausreichen soll.

Damit initiiert das IT-Sicherheitsgesetz eine Selbstregulierung, genauer, eine Ko-Regulierung, im Bereich der IT-Sicherheit, die möglicherweise Vorbildcharakter auch für weitere Gebiete der Sicherheit haben kann. Der entscheidende Vorteil dieser Ko-Regulierung liegt in der Möglichkeit, die Expertise der Wirtschaft für die Feststellung geeigneter Sicherheitsanforderungen zu nutzen.

Die Möglichkeit der Wirtschaft, branchenspezifische Standards für IT-Sicherheit festzulegen, besteht zwar auch unabhängig von einer gesetzlichen Regelung. Ein Pferdefuß der Selbstregulierung ist, wie dargestellt, die Unklarheit hinsichtlich der rechtlichen Bedeutung der Selbstregulierung, es fehlt in aller Regel an klaren gesetzlichen Anreizen. Diesem Manko will der Gesetzgeber nun abhelfen. Die Sorge, die von der Wirtschaft entwickelten Sicherheitsstandards könnten inhaltlich zu niedrig sein, soll durch das Erfordernis einer Feststellung durch das BSI, im Einvernehmen mit anderen Aufsichtsbehörden, genommen werden.

Ob dieser Weg letztlich zum Erfolg führt, wird entscheidend davon abhängen, inwieweit sich übereinstimmende Auffassungen zwischen den Branchenverbänden und den Aufsichtsbehörden über angemessene Maßnahmen ergeben.

(4) Durchsetzungsmechanismen

Das IT-Sicherheitsgesetz führt im Bereich Kritischer Infrastrukturen ein scharfes öffentlich-rechtliches Durchsetzungsinstrument ein: Nach § 8a Abs. 3 S. 1 BSI-G sind die Betreiber Kritischer Infrastrukturen verpflichtet, die Erfüllung der Anforderungen nach Abs. 1 nachzuweisen, etwa durch Prüfungen oder Zertifizierungen. Nach § 8a Abs. 3 S. 4 kann das BSI bei Sicherheitsmängeln die Beseitigung der Mängel verlangen. Auch wenn der Wortlaut dieser Norm auffallend deutlich einen Zusammenhang mit der Feststellung von Sicherheitsmängeln durch Audits aufweist, kann wohl kein Zweifel daran bestehen, dass das BSI auch unabhängig hiervon eine Anordnung zur Beseitigung von Sicherheitsmängeln treffen kann. Allerdings sind die eigenständigen Befugnisse des BSI nicht klar geregelt, so dass offen bleibt, inwieweit das BSI aus eigener Initiative die Sicherheit kritischer Infrastrukturen überprüfen kann.

6.3.1.4 Fazit

Das IT-Sicherheitsgesetz bringt einen Korb sehr heterogener Regeln mit Bezug zur IT-Sicherheit. Die vorweggenommene Umsetzung der NIS-Richtlinie wird dabei mit punktuellen, eigenständigen Regelungen verbunden.

Im Bereich der kritischen Infrastrukturen wird ein institutioneller Schutz angestrebt, der vor allem durch eine Ko-Regulierung durch BSI und die Wirtschaft erreicht werden soll. Auch wenn die Einzelheiten noch vage sind, ist dies zumindest ein zukunftweisender Schritt. Im Bereich der konkreten Sicherheitspflichten enthält das Gesetz darüber hinaus keinen erkennbaren Fortschritt.

Das Gesetz bringt darüber hinaus im neuen § 13 Abs. 7 TMG eine Norm für Sicherheit von Websites, die für die Wirtschaft insgesamt von Bedeutung ist. Leider ist die Norm unklar und inhaltlich nicht uneingeschränkt überzeugend.

Für den Bereich der I4.0 bringt das IT-Sicherheitsgesetz sehr wenig, da die Industrie nur in wenigen Bereichen als

kritische Infrastruktur gilt und damit weitgehend aus dem Anwendungsbereich der §§ 8a, b BSIG herausfallen dürfte. Für den Bereich der Industrie gilt daher im Wesentlichen nur § 13 Abs. 7 TMG, während die bisherigen Defizite des gesetzlichen Rahmens für IT-Sicherheit nicht angegangen werden. Insbesondere wird I40 im Sinne einer IT-basierten Kooperation von Industrieunternehmen durch das IT-Sicherheitsgesetz nicht erfasst.

Letztlich bringt das IT-Sicherheitsgesetz, neben dringend benötigten zusätzlichen Stellen für das BSI, vor allem viel Diskussionsbedarf und bestätigt die Notwendigkeit weiterer Forschung zum rechtlichen Rahmen von IT-Sicherheit.

6.3.2 Zertifizierung

6.3.2.1 IT-Sicherheit und Zertifizierung

Ein traditioneller und im Bereich der IT-Sicherheit zugleich neuer Ansatz zur Gewährleistung von Sicherheit ist die Zertifizierung. Zertifizierungen sind ein traditionelles Mittel im Bereich der Sicherheit und werden auch in der IT-Sicherheit seit einiger Zeit verwendet. Bisher kaum erprobt und daher neu sind Ansätze, die eine Verbindung zwischen rechtlichen Sicherheitsanforderungen im Bereich der IT und Zertifizierungen schaffen: Zertifizierung kann die tatsächliche Einhaltung hinreichender IT-Sicherheitsmaßnahmen bestätigen. Dadurch kann IT-Sicherheit in zweifacher Weise gefördert werden: Zum einen kann ein Anreiz geschaffen werden, tatsächliche Maßnahmen der IT-Sicherheit vorzunehmen, kann Vertrauensschutz in Bezug auf die zertifizierte Sicherheit gewährleistet werden, der auch sehr konkrete rechtliche Folgen haben kann. Die schärfste Rechtsfolge der Zertifizierung ist die Bindung der Betriebserlaubnis an die Zertifizierung, wie es etwa im Fall der „TÜV-Plakette“ für Kfz der Fall ist.

Der Anreiz zur tatsächlichen Gewährleistung ist umso stärker, je stärker die Vorteile des Zertifikats sind. Daher kann gerade von rechtlich gebotenen oder geförderten Zertifizierungen ein besonders starker Anreiz zur Verbesserung von Sicherheit ausgehen.

Die Zertifizierung hat nicht zuletzt im Bereich der IT-Sicherheit Tradition. Die Zertifizierung gehört zu den Kernaufgaben des BSI, das Zertifizierung etwa nach BSI-Grundschutz anbietet. Die Voraussetzungen und rechtlichen Wirkungen der Zertifizierung durch das BSI sind jedoch nur in wenigen Einzelfällen gesetzlich geregelt. Auch im Übrigen haben IT-Sicherheits-Zertifizierungen der Praxis große Bedeutung. Prüfunternehmen, wie etwa die TÜV-Gesellschaften erteilen in erheblichem Maße Zertifikate mit Bezug zu IT-Sicherheit, etwa nach der ISO/IEC 270xy-Familie. Allerdings lässt der ISO-Standard zum einen eine freie Wahl des Zertifizierungsgegenstands („scope“) zu und zum anderen gelten hinsichtlich der Intensität der Überprüfung keine einheitlichen Vorgaben, so dass auch insoweit nur eingeschränkt von einer einheitlichen Zertifizierung gesprochen werden kann.

Eine umfassende gesellschaftliche Regelung von Voraussetzungen und Regeln reiner Zertifizierungen mit Bezug zur IT-Sicherheit besteht bisher nicht. Nur in Einzelfällen verweist das Gesetz auf Zertifizierungen mit Schwerpunkt in der IT-Sicherheit. So verweist etwa § 8a Abs. 2 BSIG-E auf Zertifikate, mit denen Betreiber Kritischer Infrastrukturen die Einhaltung der gebotenen Maßnahmen der IT-Sicherheit nachweisen können.

6.3.2.2 Probleme der Zertifizierung

Die Gewährleistung von Sicherheit durch Zertifizierung hat bisher gerade im Bereich der IT-Sicherheit mit Herausforderungen zu kämpfen, die die Wirksamkeit dieser Instrumente stark beeinträchtigen.

6.3.2.2.1 Arten von Zertifizierung

Zertifizierungen in den unterschiedlichsten Ausprägungen sind weit verbreitet, auch in der Informationstechnologie. Der Begriff des Zertifikats im weiteren Sinne meint die Wissensbekundung der zertifizierenden Stelle über das Vorhandensein bestimmter Eigenschaften, kann aber auch eine Bewertung im Sinne einer Qualitätsbewertung enthalten, wie es durchaus häufig der Fall ist. Der Begriff des Zertifikats umfasst daher technische wie sonstige Prüfbestätigungen ebenso wie Gütesiegel jeglicher Art. Im Hinblick auf rechtliche Wirkungen von Zertifizierungen bietet es sich an, zwischen Compliance-Zertifizierungen und Gütesiegeln zu unterscheiden.[527] Dabei ist mit dem Begriff der Compliance-Zertifizierung die Bestätigung über die Erfüllung gesetzlicher Anforderungen durch den zertifizierten Gegenstand gemeint.[528] Als Gegenbegriff soll hier der

527 Borges, in Schweighofer/Kummer/Hötzendorfer (Hrsg.), Kooperation, Tagungsband IRIS 2015, 529, 533.
528 Borges, in Schweighofer/Kummer/Hötzendorfer (Hrsg.), Kooperation, Tagungsband IRIS 2015, 529, 533.

Begriff der (schlichten) Zertifizierung oder des Gütesiegels verwendet werden. Auch der Begriff des Gütesiegels ist nicht verbindlich definiert. Gemeint sind Zertifizierungen über die Einhaltung von Qualitätsmerkmalen, die aber nicht notwendig einer gesetzlichen Grundlage bedürfen und in aller Regel auch nicht hierauf beruhen.[529] Compliance-Zertifikate sind aufgrund ihres spezifischen Gegenstands ein Spezialfall des Zertifikats. Die gesetzliche Grundlage und das Verfahren, das zur Erteilung des Zertifikats führt, sind hiervon zunächst unabhängig.

6.3.2.2.2 Unklarheit der Rechtsfolge der Zertifizierung

In den meisten Fällen der gängigen Zertifizierungen, auch im Bereich der IT-Sicherheit, ist die Rechtsfolge der Zertifizierung nicht gesetzlich geregelt. Dies gilt insbesondere auch für die vom BSI vorgenommene Zertifizierung nach BSI-Grundschutz. Anders ist dies nur in den wenigen Fällen, in denen eine Zertifizierung ausdrücklich angeordnet ist oder vom Gesetz belohnt wird. Ein Beispiel für die Belohnung ist der genannte § 8a Abs. 2 BSIG, wonach die Betreiber kritischer Infrastrukturen den Nachweis der Sicherheit durch eine Zertifizierung erbringen können.

Die rechtliche Regelung der Rechtsfolgen der Zertifizierung ist auch bei der Compliance-Zertifizierung nicht notwendig. Jedoch verleiht erst die gesetzlich geregelte Rechtsfolge der Compliance-Zertifizierung ihre Wirksamkeit: Da das Zertifikat die Erfüllung gesetzlicher Anforderungen anzeigt, ist es umso wertvoller, je stärker das Vertrauen in das Zertifikat und damit in die Erfüllung der gestellten Anforderungen geschützt ist. Eine Compliance Zertifizierung, die keine rechtliche Folge auslöst, ist in dieser spezifischen Funktion weitgehend wertlos und kann letztlich nur als Gütesiegel verwendet werden, mit dem um Vertrauen im Markt geworben werden kann. Für diese Zwecke aber sind Gütesiegel mit differenzierten Qualitätsbewertungen (z. B. „gut“, „4 Sterne“) besser geeignet als die Aussage einer Compliance-Zertifizierung, die wesensnotwendig nur die Erfüllung oder Nichterfüllung der gesetzlichen Anforderungen als Kernaussage enthält.

Die Klarstellung der Rechtsfolge ist daher für die spezifische Zielsetzung der Compliance-Zertifizierung von entscheidender Bedeutung. Bisher fehlt es daran aber meist. Vielmehr ist die rechtliche Bedeutung der Zertifizierung oft unklar.

6.3.2.2.3 Unklarheit der Voraussetzungen

Für die Compliance-Zertifizierung ist eine klare Regelung für die Voraussetzungen der Zertifizierung entscheidend. Eine klare Rechtsfolge kann einem Zertifikat nur beigemessen werden, wenn Gegenstand und Voraussetzungen der Zertifizierung klar und überprüfbar feststehen, denn nur dann kann das Gesetz ein Vertrauen in das Zertifikat mit rechtlichen Folgen belegen.

Bisher besteht eine gesetzliche Regelung der Voraussetzungen einer Zertifizierung nur in Ausnahmefällen. Die soeben dargestellte Unklarheit hinsichtlich der Rechtsfolge realisiert hieraus unmittelbar. Dieses Problem gilt auch für die verbreiteten ISO/IEC-27001-Zertifikate, da Gegenstand und etliche Parameter der Prüfung von der zertifizierenden Stelle – regelmäßig in Absprache mit dem Auftraggeber – festgelegt werden.

6.3.2.3 Beispiel „Datenschutz-Zertifizierung“

Ein interessantes Beispiel für die genannten Schwierigkeiten und die Möglichkeiten, diese zu überwinden, bietet die Datenschutz-Zertifizierung. Hier hat sich in den letzten Jahren, nicht zuletzt im Zusammenhang mit Cloud Computing, eine intensive Diskussion und weitreichende Entwicklung ergeben, die auch für IT-Sicherheit allgemein von Interesse ist, da sich die Zertifizierung auf die Datensicherheit nach § 9 BDSG bezieht.

Da diese Entwicklung gerade für I4.0 von Bedeutung sein kann, werden die Grundlinien dieser aktuellen Entwicklung zur Zertifizierung nachfolgend skizziert.

6.3.2.3.1 Ausgangslage: Kontrollpflicht in der Auftragsdatenverarbeitung

Die Datenschutz-Zertifizierung wird als Compliance-Zertifizierung derzeit für die datenschutzrechtliche Auftragsdatenverarbeitung diskutiert. Diese ist die datenschutzrechtliche Grundlage für die Nutzung von IT-Diensten externer Anbieter. Dies gilt sowohl für traditionelles IT-Outsourcing wie für moderne IT Dienstleistungen, namentlich Cloud Computing.

529 Borges, in Schweighofer/Kummer/Hötzendorfer (Hrsg.), Kooperation, Tagungsband IRIS 2015, 529, 533.

Bei der Auftragsdatenverarbeitung ist die durch den Dienstleister erfolgende Datenverarbeitung zulässig, wenn die in § 11 BDSG geregelten Voraussetzungen der Auftragsdatenverarbeitung erfüllt sind. Danach muss die Auftragsdatenverarbeitung auf einem schriftlichen Vertrag zwischen Auftraggeber und Auftragnehmer beruhen, der die in § 11 Abs. 2 S. 2 Nr. 1 BDSG geregelten Elemente enthält und ein Weisungsrecht des Auftraggebers vorsieht. Außerdem muss der Auftraggeber den Dienstleister gemäß § 11 Abs. 2 S. 1 BDSG sorgfältig auswählen und sich gemäß § 11 Abs. 2 S. 4 BDSG von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen. Diese in § 9 BDSG geregelten Maßnahmen betreffen die Sicherheit der Datenverarbeitung, einschließlich des Schutzes gegen unbefugten Zugriff.

Die Pflicht des Auftraggebers nach § 11 Abs. 2 S. 4 BDSG wird zutreffend als eine Pflicht zur Kontrolle des Auftragnehmers angesehen, die auch eine Kontrolle der technischen Maßnahmen vor Ort, d. h. eine Inspektion des Rechenzentrums und der Rechner, auf denen die Datenverarbeitung stattfindet, einschließt. Diese Pflicht, nicht zuletzt die Erforderlichkeit einer Kontrolle vor Ort, ist jedoch für viele potenzielle Nutzer von IT-Dienstleistungen, insbesondere von Cloud Computing, nicht in zumutbarer Weise zu erfüllen.[530] Bei kleinen Unternehmen fehlt es meist bereits an der erforderlichen Sachkunde, so dass für diese Kontrolle ein Dienstleister eingeschaltet werden müsste.[531] Vor allem aber ist die Kontrollpflicht, wenn sie durch jeden Nutzer von IT-Dienstleistungen durchgeführt wird, häufig ineffizient.[532] Dies gilt insbesondere beim Cloud Computing: Dieselbe Datenverarbeitungsanlage des Cloud-Anbieters müsste durch eine Vielzahl von Cloud-Nutzern kontrolliert werden, jeder Cloud-Nutzer müsste eine Vielzahl von Datenverarbeitungsanlagen überwachen.[533]

6.3.2.3.2 Lösung: Zertifizierung statt Überwachung durch alle Auftraggeber

Als geeignete Lösung für das Problem der Überwachung bei der Auftragsdatenverarbeitung, insbesondere beim Cloud Computing, wird verbreitet die Erfüllung der Kontrollpflicht durch eine Zertifizierung angesehen. Danach erfolgt die in § 11 Abs. 2 S. 4 BDSG gebotene Kontrolle durch einen unabhängigen Dritten, der für die Cloud-Nutzer die Überprüfung vornimmt und die Einhaltung der rechtlich gebotenen Maßnahmen durch ein Zertifikat oder Testat bezeugt.[534]

In der aktuellen Diskussion kommt dem Thesenpapier „Datenschutzrechtliche Lösungen für Cloud Computing“ der Arbeitsgruppe „Rechtsrahmen des Cloud Computing“[535] besondere Bedeutung zu.[536] Die Arbeitsgruppe, die mit Vertretern aus Wissenschaft, Praxis und insbesondere Datenschutzaufsichtsbehörden besetzt ist[537], beschreibt in diesem Papier in insgesamt zehn Thesen das Konzept einer datenschutzrechtlichen Zertifizierung einschließlich der rechtlichen Bedeutung des Zertifikats (Testats) und der wesentlichen Merkmale des Zertifizierungsverfahrens.

Das Konzept sieht im Kern vor, dass der Auftraggeber die Pflicht zur Überprüfung des Auftragnehmers dadurch erfüllen kann, dass er ein Testat prüft, das die Gewährleistung der datenschutzrechtlichen Anforderungen durch den Cloud-Anbieter bestätigt.[538] Das Thesenpapier verwendet den Begriff des Testats[539], offensichtlich um eine begriffliche Nähe zur Bestätigung rechtlicher Anforderungen, etwa dem Testat nach § 322 HGB, zu suchen und um sich von Gütesiegeln abzugrenzen.

530 Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“, Thesenpapier – Datenschutzrechtliche Lösungen für Cloud Computing, These 8, S. 18; BITKOM-Leitfaden Cloud Computing – Evolution in der Technik, Revolution im Business, https://www.bitkom.org/Bitkom/Publikationen/Leitfaden-Cloud-Computing.html, S. 52; Borges, DuD 2014, 164 (166); Gola/Schomerus, BDSG Bundesdatenschutzgesetz – Kommentar, München, 11. Auflage (2012), § 11 RN 21.

531 Borges, DuD 2014, 164 (166); Brennscheidt , Cloud Computing und Datenschutz, 2013; Schuster/Reichl, CR 2010, 38 (42).

532 Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“, Thesenpapier – Datenschutzrechtliche Lösungen für Cloud Computing, These 8, S. 18; Borges, DuD 2014, 164 (166).

533 Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“, Thesenpapier – Datenschutzrechtliche Lösungen für Cloud Computing, These 8, S. 18; Borges, DuD 2014, 164 (166); Selzer, DuD 2013, 215 (216).

534 Borges, in Schweighofer/Kummer/Hötzendorfer (Hrsg.), Kooperation, Tagungsband IRIS 2015, S.529, 533.

535 Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“, Thesenpapier – Datenschutzrechtliche Lösungen für Cloud Computing. Siehe dazu Borges, DuD 2014, 165 (166 ff.).

536 Borges, in Schweighofer/Kummer/Hötzendorfer (Hrsg.), Kooperation, Tagungsband IRIS 2015, S.529, 533.

537 Siehe auch Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“, Thesenpapier – Datenschutzrechtliche Lösungen für Cloud Computing, S. 25.

538 Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“, Thesenpapier – Datenschutzrechtliche Lösungen für Cloud Computing, These 5, S. 11.

539 Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“, Thesenpapier – Datenschutzrechtliche Lösungen für Cloud Computing, S. 12 ff.

Das Konzept enthält wesentliche Grundlagen der Zertifizierung. So sieht das Konzept der AG Rechtsrahmen vor, dass die Zertifizierung nur durch eine unabhängige Stelle erfolgen kann[540], die eine hinreichende fachliche und persönliche Eignung aufweist.[541] Die Eignung der zertifizierenden Stelle soll durch eine Akkreditierung nachgewiesen werden müssen.[542] Die ordnungsgemäße Durchführung der Zertifizierung soll darüber hinaus durch eine zivilrechtliche Haftung der Zertifizierungsstelle für fehlerhafte Prüfungen und Zertifizierungen gesichert werden.[543] Das Konzept zielt auf eine gesetzliche Regelung der Zertifizierung ab, die in der europäischen Datenschutz-Grundverordnung erfolgen soll.

6.3.2.3.3 Das Konzept zur Datenschutz-Zertifizierung

Im Rahmen des Trusted Cloud-Programms, insbesondere im Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“[544] sind umfangreiche Arbeiten zur Datenschutz-Zertifizierung erfolgt, deren Ergebnisse im April 2015 veröffentlicht wurden.[545] Dies sind vor allem das Konzept zum Zertifizierungsverfahren („Datenschutzrechtliche Lösungen für Cloud Computing“, Oktober 2012) und insbesondere das im April 2015 veröffentlichte „Trusted Cloud-Datenschutzprofil für Cloud-Dienste“ (TCDP). Dazu gehören auch weitere Grundlagen zu Elementen der Zertifizierung (Arbeitspapier „Modulare Zertifizierung von Cloud-Diensten“, 2014, Thesenpapier „Datenschutz-Zertifizierung durch private Stellen“, 2015; Arbeitspapier „Modularer Aufbau von Cloud-Diensten“, 2014; Arbeitspapier „Schutzklassen in der Datenschutz-Zertifizierung“, 2015, Thesenpapier „Eckpunkte eines Zertifizierungsverfahrens für Cloud-Dienste“, 2015).

In den Ergebnispapieren werden einige Anforderungen an das Zertifizierungsverfahren sowie an die Prüf- und Zertifizierungsstelle ausgeführt. Danach soll die Prüfung und Zertifizierung im Rahmen eines Verfahrens erfolgen, das durch einen freiwilligen Antrag des Betreibers des zu prüfenden Cloud-Dienstes eingeleitet wird und eine Prüfung sowie die Entscheidung über die Vergabe und ggf. die Erteilung eines Zertifikats einschließt. Die zentrale Aussage des Zertifikats, die Bestätigung über die Erfüllung der datenschutzrechtlichen Anforderungen, ist im Konzept präzise festgelegt. Wesentliche Elemente des Verfahrens, etwa die Pflicht zur Veröffentlichung des Zertifikats, die Haftung für Fehler in der Prüfung und Zertifizierung, sind im Konzept genannt.

Ein Kernelement des Konzepts ist die Festlegung einheitlicher Voraussetzungen für die Erteilung des Zertifikats, insbesondere im Bereich der Prüfanforderungen. Hier wurde das Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP) entwickelt, das die gesetzlichen Anforderungen des BDSG an die Auftragsdatenverarbeitung für die Besonderheiten von Cloud-Diensten spezifiziert. Das TCDP beruht auf dem ISO/IEC-Standard 27018[546] und macht sich dadurch das Instrumentarium des international anerkannten ISO/IEC-Standards 27002[547] zunutze, den der ISO 2718-Standard um Cloud- und insbesondere datenschutzspezifische Anforderungen erweitert.

Das Konzept des Trusted Cloud-Programms beschreibt damit eine datenschutzrechtliche Compliance-Zertifizierung für Datensicherheit nach BDSG.

6.3.2.4 Notwendige gesetzliche Regelung für Compliance-Zertifizierung

Gütesiegel wie Compliance-Zertifikate können auch ohne gesetzliche Grundlage vergeben werden. Allerdings fehlt es in diesem Fall meist an einem transparenten Prüfverfahren und Prüfstandard. Entsprechend kann es nicht verwundern, wenn im Beispiel der Datenschutz-Zertifizierung bei den Datenschutz-Aufsichtsbehörden derzeit eine erhebliche Skepsis gegenüber den herkömmlichen Zertifizierungen herrscht. So weist die von den Arbeitskreisen Technik und Medien der Konferenz der Datenschutzbeauftragten herausgegebenen Orientierungshilfe Cloud Computing darauf

540 Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“, Thesenpapier – Datenschutzrechtliche Lösungen für Cloud Computing, These 5, S. 12.
541 Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“, Thesenpapier – Datenschutzrechtliche Lösungen für Cloud Computing, These 8, S. 17.
542 Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“, Thesenpapier – Datenschutzrechtliche Lösungen für Cloud Computing, These 8, S. 18.
543 Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“, Thesenpapier – Datenschutzrechtliche Lösungen für Cloud Computing, These 8, S. 18.
544 Siehe zum Pilotprojekt auch die weiterführenden Informationen auf https://www.trusted-cloud.de/projekt.
545 Die Ergebnispapiere sind abrufbar unter https://www.trusted-cloud.de/forschung
546 ISO/IEC 27018:2014 Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
547 ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls –

hin, dass eine Zertifizierung nach ISO/IEC 27001 einen „wichtige[n] Baustein für einen Prüfnachweis“ darstelle, eine umfassende datenschutzrechtliche Prüfung aber nicht zertifiziert werde. Daher seien weitere Nachweise erforderlich.[548]

Compliance-Zertifizierungen benötigen daher aus Gründen der Rechtssicherheit regelmäßig eine gesetzliche Regelung. Dies wird am Beispiel der Auftragsdatenverarbeitung besonders sichtbar. So kann die Überprüfungspflicht nach § 11 Abs. 2 Nr. 4 BDSG nach herrschender Ansicht der Literatur bereits nach den geltenden Normen des BDSG durch das Vertrauen auf das Testat eines geeigneten Zertifizierers erfüllt werden.[549] Da diese Möglichkeit aber im BDSG nicht ausdrücklich angeordnet ist, besteht insoweit Rechtsunsicherheit.[550] Daher sieht das Konzept der AG „Rechtsrahmen des Cloud Computing“ vor, dass diese Wirkung des Zertifikats im Gesetz ausdrücklich festgelegt wird.[551]

Die gesetzliche Festlegung einer solchen Rechtsfolge ist aber nur sinnvoll, wenn auch hinsichtlich der Voraussetzungen für die Erteilung eines solchen Zertifikats Klarheit besteht. Entsprechend fordert die AG „Rechtsrahmen des Cloud Computing“ eine umfassende rechtliche Regelung auch der Voraussetzungen der Zertifizierung.[552]

Die Datenschutz-Grundverordnung (DSGVO) wird voraussichtlich eine gesetzliche Regelung zur Zertifizierung enthalten. Zwar enthält der Entwurf der EU-Kommission zur DSGVO[553] keine Aussage darüber, ob die Überprüfung durch eine Zertifizierung ersetzt werden kann. Allerdings enthält der Entwurf in Art. 39 eine – sehr allgemeine – Bezugnahme auf Zertifizierungen. Im Gesetzgebungsverfahren zur DSGVO sind jedoch wesentlich weitergehende Vorschläge zur datenschutzrechtlichen Zertifizierung erarbeitet worden. So sieht der am 12. März 2014 verabschiedete Entwurf des Europäischen Parlaments zur DSGVO eine umfangreiche Regelung zur Zertifizierung in Art. 39 DSGVO vor.[554] Auch der Ministerrat befürwortet eine intensivere Regelung der Zertifizierung in der DSGVO. Im aktuellen Entwurf der italienischen Ratspräsidentschaft vom 03. Oktober 2014[555] wird die Ergänzung des Art. 39 durch einen Art. 39a vorgeschlagen, in dem die Anforderungen an die Zertifizierung und das zugrundeliegende Zertifizierungsverfahren näher geregelt werden.

6.3.2.5 Chancen der IT-Sicherheits-Zertifizierung

Die Untersuchung der Zertifizierung zeigt, auch wenn sie nur insoweit beispielhaft erfolgen konnte, dass die IT-Sicherheits-Zertifizierung, die im geltenden Recht nur punktuell eingesetzt wird, möglicherweise erhebliche Chancen bietet, wenn die rechtlichen Rahmenbedingungen geregelt werden.

Leider fehlt es bisher an Konzepten zu einer breitflächigen IT-Sicherheits-Zertifizierung. Die im Rahmen des Trusted Cloud-Programms geleisteten Arbeiten belegen aber, dass es durchaus möglich ist, ein Konzept zur sicherheitsbezogenen Zertifizierung mit breitem Anwendungsbereich zu entwickeln. Auch das IT-Sicherheitsgesetz setzt auf Zertifizierung, leider ohne den rechtlichen Rahmen hierfür zu bieten. Es ist offensichtlich, dass eine Verbindung der Konzepte Chancen verspricht, nicht nur im Bereich der Kritischen Infrastrukturen, sondern auch darüber hinaus, ggf. insbesondere für die I4.0.

548 Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe Cloud Computing, Version 2.0, Stand 09.10.2014, Ziff. 3, S. 11.

549 Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“, Thesenpapier – Datenschutzrechtliche Lösungen für Cloud Computing, These 8, S. 18; Borges, in Schweighofer/Kummer/Hötzendorfer (Hrsg.), Kooperation, Tagungsband IRIS 2015, S. 529, 534; Brennscheidt Cloud Computing und Datenschutz, 2013, S. 112; Gola/Schomerus, BDSG, § 11 RN 21; Weichert, DuD 2010, 679 (683).

550 Borges, in Schweighofer/Kummer/Hötzendorfer (Hrsg.), Kooperation, Tagungsband IRIS 2015, S. 529, 534.

551 Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“, Thesenpapier – Datenschutzrechtliche Lösungen für Cloud Computing, These 8, S. 18.

552 Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“, Thesenpapier – Datenschutzrechtliche Lösungen für Cloud Computing, These 8, S. 18.

553 Siehe Vorschlag für Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), 25.1.2012, KOM (2012) 11 endg., 2012/0011 (COD), Änderungsanträge 237 f., S. 155 f. sowie Änderungsantrag 51, S. 46, zu Erwägungsgrund 77.

554 Legislative Entschließung des Europäischen Parlaments vom 12.03.2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD) (Ordentliches Gesetzgebungsverfahren: erste Lesung).

555 Ratsdokument Nr. 13772/14 vom 03.10.2014, http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2013772%202014%20INIT

6.3.3 Fazit

In diesem Abschnitt wurden zwei aktuelle Ansätze zur Weiterentwicklung des rechtlichen Rahmens für IT-Sicherheit untersucht. Das IT-Sicherheitsgesetz gibt Impulse für die Entwicklung der IT-Sicherheitsregulierung, indem etwa eine breitflächige gesetzliche Pflicht zur IT-Sicherheit ausgesprochen wird und indem in einem Teilbereich Instrumente wie Aufsichtsbefugnisse für IT-Sicherheit und Entwicklung von Branchenstandards für IT-Sicherheit, erprobt werden können.

Jedoch ist das IT-Sicherheitsgesetz auf einen kleinen Teilbereich der Wirtschaft beschränkt – umfasst insbesondere nicht die I4.0 – und lässt damit den weitaus größten Teil von IT-Anwendungen außen vor. Auch inhaltlich regelt das IT-Sicherheitsgesetz nur Einzelaspekte. Diese Lückenhaftigkeit des IT-Sicherheitsgesetzes belegt letztlich sehr deutlich den Bedarf einer Weiterentwicklung des rechtlichen Rahmens für IT-Sicherheit.

Im Bereich der Zertifizierung zeigt sich derzeit im Bereich des Datenschutzes eine hochinteressante Entwicklung, die Potenzial auch für die IT-Sicherheit allgemein besitzt: Die auf einer gesetzlichen Regelung beruhende Zertifizierung von IT-Sicherheit und insbesondere die Herausbildung von transparenten, öffentlichen Standards für IT-Sicherheit erscheinen geeignet, eine Verbesserung von IT-Sicherheit in der Fläche zu erreichen. Auch insoweit fehlt es derzeit aber an einem tragfähigen Konzept, so dass auch hier erhebliche Anstrengungen erforderlich sind. Die Nutzung der Erkenntnisse aus der Datenschutz-Zertifizierung könnte hier aber einen guten Einstieg bilden.

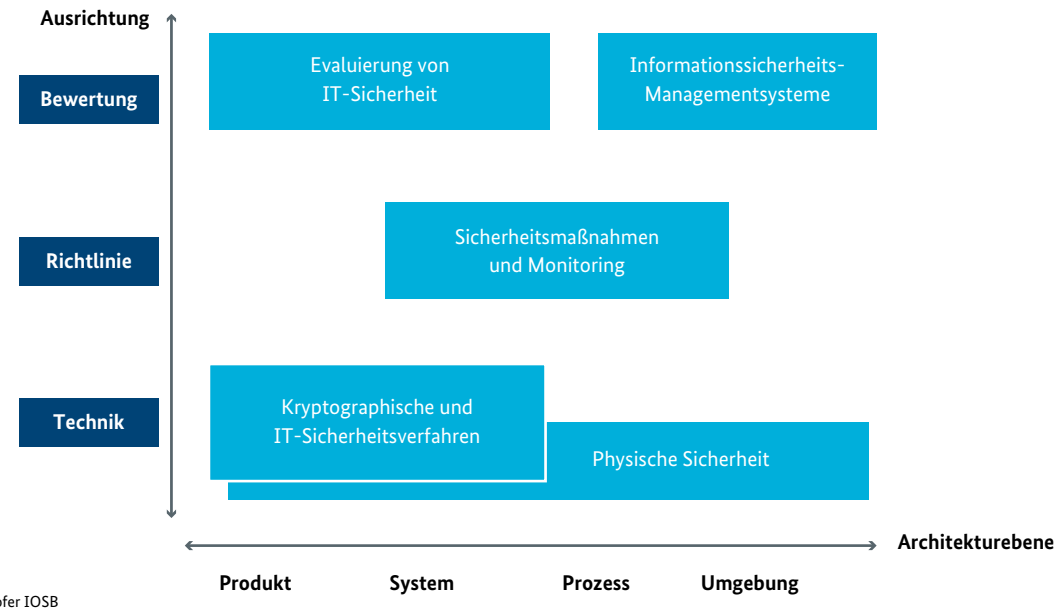
6.4 Standards und Normen

6.4.1 Einteilung und Beziehung der Standards untereinander

Der Bereich der IT-Sicherheitsstandards zeichnet sich durch eine hohe Zahl an de-jure- und de-facto-Standards aus unterschiedlichsten Standardisierungs-, Normungs- und Industriegremien aus (siehe Abbildung 6-1). Es gibt allerdings keine über die verschiedenen Gremien und Branchen allgemein akzeptierte Struktur bzw. Klassifikation der Standardisierungslandschaft, was eine Bewertung der Standards und Normen, insbesondere auch für deren Nutzbarkeit in I4.0, erschwert. Es ist Aufgabe eines I4.0-Referenzmodells, diese Klassifikation zu definieren und dann im Rahmen von I4.0-Referenzarchitekturen dazu passende IT-Sicherheitsstandards auszuwählen.

Abbildung 6–1 zeigt eine Einteilung der Standards nach Dr. Walter Fumy[556], dem Chairman der ISO/IEC JTC1/SC 27.

Abbildung 6–1: Einteilung von IT-Sicherheitsstandards nach Fumy



Quelle: Fraunhofer IOSB

556 Vergl. „Kompass der IT-Sicherheitsstandards“ – Auszüge als Sonderdruck zur it-sa 2013, BITKOM 2013.

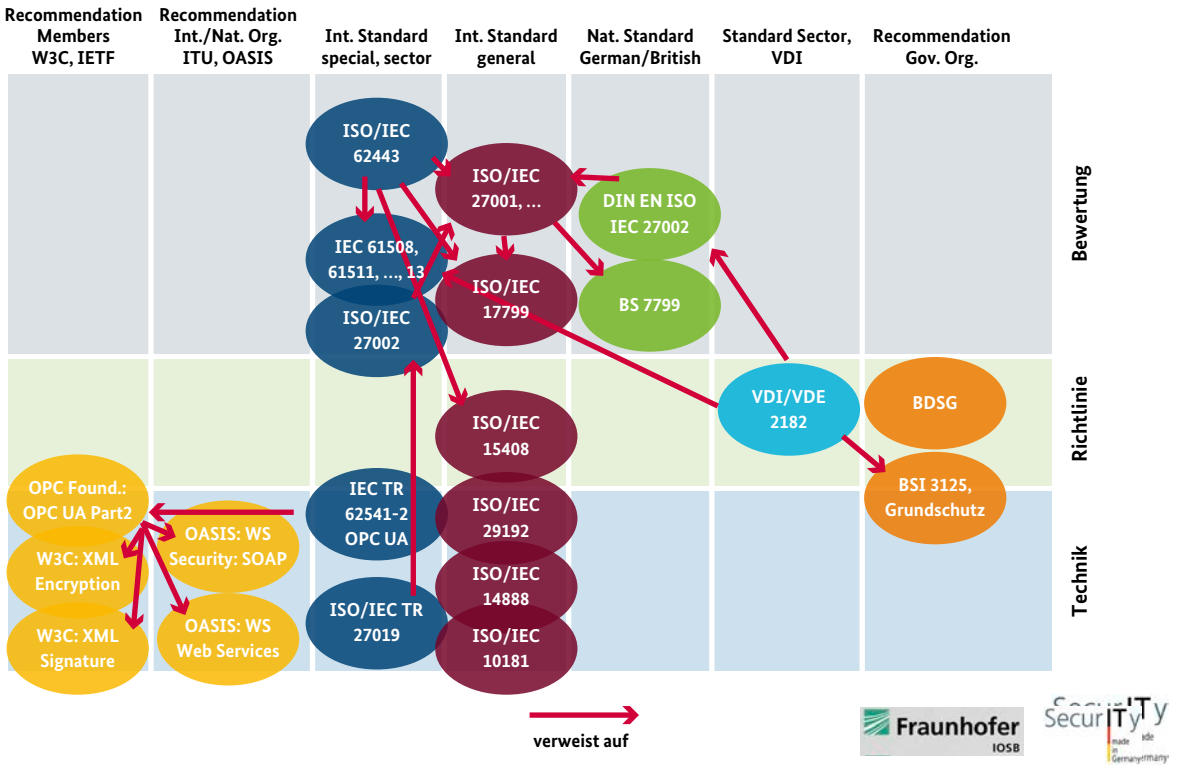
Dieser unterscheidet die folgenden drei Gruppen von IT-Sicherheitsstandards, je nach Zielstellung und Zweck des Standards:

- **Bewertung** der IT-Sicherheit von IT-Systemen: Diese Gruppe bezeichnet Standards, welche die IT-Sicherheit von bestehenden oder entstehenden IT-Systemen nach allgemein akzeptierten Kriterien bewerten. Darunter fällt insbesondere auch der Bereich der organisatorischen und technischen Managementsysteme für Informationssicherheit (ISMS)[557] gemäß ISO/IEC 270xy.
- **Richtlinie** zur IT-Sicherheit von IT-Systemen: Diese Gruppe beinhaltet Richtlinien und Empfehlungen zur Umsetzung von IT-Sicherheitsmaßnahmen und deren Überwachung (Monitoring).
- **Technik** zur Gewährleistung der IT-Sicherheit von IT-Systemen: Diese Gruppe bezieht sich auf technische Verfahren zur Umsetzung von IT-Sicherheit auf technischer Ebene, wie z. B. Verschlüsselung (kryptografische Verfahren), Authentifizierung und Autorisierung.

Ausgehend von dieser Strukturierung zeigt Abbildung 6–2 eine Auswahl der für I4.0 wesentlichen IT-Sicherheitsstandards, deren organisatorische Herkunft (vgl. Kapitel 3.2) und deren Referenzbeziehungen untereinander, also inhaltlichen Abhängigkeiten zwischen den IT-Sicherheitsstandards.

Als wesentliches Ergebnis zeigt sich eine klare Trennung (d.h. keine wesentlichen Referenzen) zwischen den Standards der Gruppen „Bewertung“ und „Richtlinie“ und den Standards der Gruppe „Technik“, insbesondere für den

Abbildung 6–2: Referenzbeziehungen zwischen den wesentlichen IT-Sicherheitsstandards für Industrie 4.0



Legende:

BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
DIN	Deutsches Institut für Normung e.V.
IACS	Industrial Automation Control Systems
IEC	International Electrotechnical Committee
OASIS	Organization for the Advancement of Structured Information Standards
W3C	World Wide Web Consortium
IETF	Internet Engineering Task Force
ISMS	Informationssicherheits-Managementsysteme
ISO	International Standardization Organization
ITU	International Telecommunication Union
NIST	National Institute of Standards and Technology
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e.V.
VDI	Verein Deutscher Ingenieure e.V.

Quelle: Fraunhofer IOSB

557 Vergl. „BSI Standard 100-1“ Managementsysteme für Informationssicherheit (ISMS), Bundesamt für Sicherheit in der Informationstechnik (BSI), 2008.

Bereich der industriellen Produktion. Damit fehlt eine Durchgängigkeit von der organisatorischen auf die technische Ebene, d.h. es gibt als Ergebnis eines ISMS-Prozesses keine unmittelbaren Empfehlungen für den Einsatz von Standards auf der technischen Ebene.

6.4.2 Relevanz von Standards für Industrie 4.0

Industrielle Produktion gemäß I4.0-Konzepten erfordert durchgängige IT-Lösungen zur Kopplung der Prozesse in den zu unterstützenden Wertschöpfungsketten. Diese Durchgängigkeit, ob vertikal über die Ebenen der klassischen Automatisierungspyramide hinweg, oder horizontal in Wertschöpfungsnetzwerken über Unternehmensbereiche und Unternehmen hinweg, ist nur über klar definierte Schnittstellen zu erreichen, mit ihren funktionalen, datenorientierten und nicht-funktionalen Aspekten, insbesondere auch den IT-Sicherheitsaspekten. Aus diesem Grund sind internationale Standards essenziell für das Funktionieren von Wertschöpfungsnetzwerken im Rahmen von I4.0, da diese Netzwerke grundsätzlich global zu verstehen sind. Die Ambitionen der I4.0-Gremien gehen derzeit genau in diese Richtung, indem an Referenzmodellen und sich daraus ableitenden Referenzarchitekturen gearbeitet wird, um den Rahmen für eine derartige Standardisierung zu schaffen. Mit der Definition des Referenzarchitekturmodells Industrie 4.0 (RAMI4.0)[558] wurde ein erster Schritt in diese Richtung gemacht. Die Beachtung von IT-Sicherheit ist eine wesentliche grundsätzliche Forderung über alle Dimensionen des RAMI4.0 hinweg. Ferner wurde kürzlich die Referenzarchitektur IIRA[559] des IIC veröffentlicht, in welcher speziell der IT-Sicherheit eine wesentliche Rolle zugeschrieben wird. Diese starke Rolle fehlt derzeit bei RAMI4.0.

I4.0-Standards können aus pragmatischen und markttechnischen Gründen nicht vollständig neu definiert werden, sondern müssen sich an bestehenden IT-Standards, insbesondere aus dem Anwendungsfeld des Internet, orientieren. Diese müssen auf ihre Tauglichkeit für industrielle Produktionsumgebungen hin untersucht und ggf. angepasst werden. Dies gilt insbesondere für IT-Sicherheitsstandards, da diese verträglich mit anderen nicht-funktionalen Anforderungen, wie z.B. Echtzeit, Ausfallsicherheit und Wartbarkeit sein müssen.

6.4.3 OPC Unified Architecture

Zur Umsetzung der Industrie 4.0 wird eine sichere und vertrauliche Kommunikation der beteiligten Geräte und Komponenten benötigt. Das in diesem Zusammenhang immer wieder genannte Kommunikationsprotokoll OPC UA wird deshalb vom BSI seit Januar 2015 untersucht.

Die Spezifikationsanalyse wurde im Juli 2015 abgeschlossen, aktuell wird die Referenz-Implementierung der OPC Foundation nach Sicherheitsaspekten analysiert.

Generell besitzt die OPC UA Spezifikation sog. „Security by Design“; es wurden keine systematischen Fehler in der Spezifikation gefunden.

Die für die Sicherheit relevanten Teile der Spezifikation wurden intensiv untersucht, in deren Folge viele kleinere Verbesserungsvorschläge, beispielsweise in der Konsistenz der verschiedenen Teile der Spezifikation, aber auch weitere Hinweise und Ratschläge der Sicherheitsgruppe der OPC Foundation mitgeteilt wurden.

Dazu gehören auch ein Abgleich der Definitionen mit ISO2700X und Vorschläge zur Ergänzung der in der Spezifikation genannten Bedrohungen (beispielsweise „Message Flooding“ erweitern um ein weitergefasstes „Denial of Service-Angriffe“).

Durch die lange Lebensdauer der Spezifikation können Teile, die rapiden sicherheits-technischen Veränderungen unterworfen sind, wie kryptographische Verfahren, nicht mehr zeitgemäß sein. Die OPC Foundation ist sich dieser Problematik bewusst und arbeitet an Verbesserungen.

Aktuell wird die Analyse der Referenzimplementierung mit statischen und dynamischen Verfahren (fuzzing) durchgeführt.

Aus den Ergebnissen werden Vorgaben und Empfehlungen für Hersteller und Integratoren abgeleitet; auch werden die Standardeinstellungen einzelner Konfigurationsparameter auf Plausibilität überprüft, um die Funktionsweise von OPC UA für Industrie 4.0 weiter zu verbessern.

558 Referenzarchitekturmodell Industrie 4.0 (RAMI4.0), VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik, 2015.
559 Industrial Internet Architecture Version 1.5, Industrial Internet Consortium, 2015.

6.4.4 Fazit

Die Bewertung lässt sich wie folgt zusammenfassen:

- Im Rahmen der Arbeiten zu einem I4.0-Referenzmodell sollte eine Strukturierung des Themas IT-Sicherheit vorgenommen werden und damit die Klassifikation der notwendigen IT-Sicherheits-Standardisierungsarbeiten erfolgen. Eine erste Übersicht dazu kann aus der Deutschen Normungs-Roadmap IT-Sicherheit des DKE, Kap. 4.3, entnommen werden.[560]

- Zahlreiche IT-Sicherheits-Standards aus der Gruppe „Bewertung“ und „Richtlinie“ sind auch auf den Bereich der industriellen Produktion übertragbar, bedürfen allerdings der Fokussierung auf das Zusammenspiel von IT-Sicherheitsanforderungen und Schutzzielen mit anderen nicht-funktionalen Anforderungen wie Ausfallsicherheit, Echtzeit und Verfügbarkeit.

- Eine belastbare Bewertung der Relevanz bestehender technischer IT-Sicherheitsstandards für den Bereich industrielle Produktion/I4.0 ist erst möglich anhand der Struktur und den ausgewählten Technologien von I4.0-Referenzarchitekturen.

- Eine mögliche I4.0-Referenzarchitektur auf der Basis von IEC/TR 62541-2 OPC UA[561] bringt auf der technischen Ebene eine Reihe von bestehenden IT-Sicherheitsstandards aus den Internet-Standardisierungsgremien (OASIS, IETF, W3C) mit sich. Deren Angemessenheit für die industrielle Produktion ist individuell abzuprüfen hinsichtlich der jeweiligen Sicherheitsanforderungen und Schutzziele aus einem ISMS-Prozess. Eine allgemeine Bewertung des möglichen Schutzniveaus von OPC UA wird derzeit im Rahmen einer Studie des BSI untersucht (siehe 6.4.3).

6.5 Zusammenfassung

Der in diesem Kapitel fortgesetzte interdisziplinäre Ansatz resultiert in einem breit gefächerten Spektrum von technischen, organisatorischen und rechtlichen Konzepten zur Erzielung eines angemessenen Schutzniveaus für I4.0. Dabei wurden einzelne vorhandene Konzepte aus anderen technischen, organisatorischen und rechtlichen Anwendungsfeldern im Hinblick auf deren Übertragbarkeit für I4.0 betrachtet. So wurden bspw. technische Aspekte, wie die Absicherung von Informationsströmen, Daten-, Know-how- und Piraterie-Schutz adressiert, Konzepte zur Überwindung organisatorischer Hemmnisse vorgestellt sowie rechtliche Fragestellungen zur Exportkontrolle näher analysiert und vertragliche oder legislative Lösungsoptionen aufgezeigt. So wie die einzelnen Disziplinen im Kontext von I4.0 miteinander verschränkt sein werden, standen auch hier entsprechende Wechselwirkungen im Vordergrund der Betrachtungen. Die resultierenden Konzepte berücksichtigen neben der Integration von Technik in bestehende Prozesse bspw. auch die Rolle des Menschen in von I4.0 beeinflussten Prozessen, sowie das Vertrauen von KMU in die Technik, in die Kooperationspartner und die I4.0-Vision.

Ferner konnte durch den Rückgriff auf die Erfahrungen mit Betreibern und Integratoren auch die Akzeptanz neuer Technologien im Kontext industrie- und sektorenspezifischer Rahmenbedingungen und besonderer Anforderungen bewertet werden. Aus den bestehenden Kooperationen des Bundesamts für Sicherheit in der Informationstechnik (BSI) mit der Industrie konnte hier ein hohes Maß an Fachwissen bezüglich der technischen Umsetzbarkeit von Sicherheitstechnologien eingebracht werden. Es ist festzustellen, dass viele der Technologien aus dem Feld der klassischen IT technisch bewährt und in der Regel wirtschaftlich einsetzbar sind. Bei der Abschätzung der Handlungsempfehlungen wurden aber nicht nur diese technischen Aspekte betrachtet. Es wurden zudem nach Möglichkeit, abgeleitet aus der klassischen IT, bewährte und wirtschaftlich darstellbare Technologien auf die IT-Sicherheitslösungen abgebildet. Obwohl eine abschließende Wirtschaftlichkeitsberechnung im klassischen Sinne in Ermangelung belastbarer Zahlen aus den Fallbeispielen nicht erfolgen konnte, erscheint eine wirtschaftliche Übertragung der gefundenen Konzepte auf die Produktionsumgebungen durchaus realisierbar.

Mit der abschließenden Bewertung von Standards und Normen komplettieren die in diesem Kapitel vorgestellten Konzepte die notwendige Basis für die Entwicklung von Handlungsvorschlägen im nachfolgenden Kapitel.

560 Koordinierungsstelle IT-Sicherheit im DIN (KITS): Normungsroadmap IT Sicherheit, Version 2.0, 12/2014.
561 IEC TR 62541-2:2010 OPC Unified Architecture – Part 2: Security Model, https://webstore.iec.ch/publication/7174, abgerufen am 16.07.2015.

7. Ableitung von Handlungs-vorschlägen

Das Kapitel 7 fasst die wichtigsten Risiken und Herausforderungen zusammen, ebenso wie die identifizierten Handlungs- und Lösungsmöglichkeiten. Es enthält eine Betrachtung hinsichtlich der Abwägung von Kosten und Nutzen von IT-Sicherheit sowie die identifizierten Handlungsvorschläge als zentrales Ergebnis der Studie.

7.1 Identifizierte Risiken und Herausforderungen

Die nachfolgenden Kapitel fassen die in den Kapiteln 4, 5 und 6 identifizierten Risiken und Herausforderungen für die Industrie 4.0 (I4.0) im Kontext von IT-Sicherheit zusammen, sowohl aus der technischen, organisatorischen als auch aus der rechtlichen/Regulierungssicht.

7.1.1 Herausforderungen der Regulierung der IT-Sicherheit

Die Analyse der gegenwärtigen Regulierung der IT-Sicherheit hat gezeigt, dass die verschiedenen Regulierungsinstrumente im Bereich der IT-Sicherheit spezifische Stärken, aber auch Schwächen aufweisen, die nicht zuletzt für die I4.0 von Bedeutung sind.

Dabei lässt sich feststellen, dass für die beiden Kernaufgaben der Regulierung, der Formulierung materieller Anforderungen zum einen sowie der Durchsetzung normativer Anforderungen zum anderen, auch bei der IT-Sicherheit unterschiedliche Instrumente geeignet sind.

7.1.1.1 Materielle Anforderungen

Die Gesetzgebung spielt derzeit im Bereich der IT-Sicherheitsregulierung eine eher geringe Rolle (5.4.3.1.3). Hinsichtlich der materiellen Anforderungen könnte die Gesetzgebung bei den Grundlagen, etwa Ziele und Prinzipien der IT-Sicherheit, und den Verhaltensanforderungen, ansetzen. In diesem Bereich ist die Gesetzgebung aber bestenfalls am Anfang.

Bei der Formulierung konkreter technischer Anforderungen, die bei der Gesetzgebung strukturell bestenfalls eingeschränkt geeignet ist, hat sich der Gesetzgeber in einzelnen Fällen, etwa bei der elektronischen Signatur und beim elektronischen Identitätsnachweis, recht weit vorgewagt. Die Geeignetheit dieses Ansatzes ist allerdings sehr umstritten, da der Einsatz in der Praxis sowohl der elektronischen Signatur als auch des elektronisches Identitätsnachweises bisher weit hinter den Erwartungen zurückgeblieben ist (5.4.3.1.2).

Das IT-Sicherheitsgesetz (6.3.1.) markiert hier insoweit eine Änderung, als es den Willen des Gesetzgebers zum Ausdruck bringt, im Bereich der IT-Sicherheit tätig zu werden.

Es bringt jedoch auf dem Gebiet der technischen Anforderungen nichts Neues, da der zentrale Begriff des gesamten Gesetzes, der „Stand der Technik“, nur in der Gesetzesbegründung definiert wird und die Regelung viel zu vage ist (6.3.1.2.2; 6.3.1.3.2).

Das IT-Sicherheitsgesetz hat für die I4.0 schon deshalb bestenfalls eine eingeschränkte Bedeutung, weil es auf „kritische Infrastrukturen“ beschränkt ist und daher nur einen Teil der Industrie erfasst. Daher kann vom IT-Sicherheitsgesetz jedenfalls in seiner derzeitigen Konzeption kein wesentlicher Beitrag für einen flächendeckenden Sicherheitsgewinn für die I4.0 ausgehen.

Die Rechtsprechung ist bei der Formulierung von Verhaltensanforderungen, ihrem traditionellen Kerngebiet, auch im Bereich der IT-Sicherheit aktiv und hat hier in einigen Punkten Akzente gesetzt (5.4.3.2.1). Im Bereich technischer Anforderungen, in dem die Rechtsprechung strukturell nur eingeschränkt leistungsfähig ist, bleibt sie erwartungsgemäß blass (5.4.3.2.2).

Behördliche Kontrolle durch Maßnahmen der Aufsicht, etwa Verwaltungsakten, hat für die Breite der IT-Sicherheit unmittelbar keine Breitenwirkung (5.4.3.3). Es fehlt bereits an zuständigen Behörden, sowie an einer klaren Aufgabenzuweisung und einem Konzept für diesen Aspekt (5.4.3.3). Auch nach dem IT-Sicherheitsgesetz kann das BSI nur in kleinen Teilbereichen aktiv werden (6.3.1.2.3).

Die Vertragspraxis (5.4.3.), ein starkes Element der IT-Sicherheit, führt derzeit nicht zu einer klaren Formulierung von einheitlichen Anforderungen an IT-Sicherheit. Prägende Musterverträge gibt es nicht, soweit erkennbar, auch im Übrigen keine einheitliche Vertragsgestaltung (5.4.3.4.1.2).

Für die Formulierung technischer Anforderungen haben Standards unter den verschiedenen Instrumenten wohl die größte Bedeutung (5.4.3.5). Standards wie die ISO/IEC 270xy-Familie und die BSI-Grundschutz-Standards und Maßnahmenkataloge, die Anforderungen an IT-Sicherheit formulieren sind in den technischen Fachkreisen anerkannt. Allerdings kann man hier bei weitem nicht von einer flächendeckenden Anwendung in der Praxis sprechen. Ebenso ist – mangels hinreichender praktischer Umsetzung und mangels Gerichtsentscheidungen – unklar, welche Bedeutung den

Standards für die Erfüllung rechtlicher Pflichten zukommt (5.4.3.5.2).

Kodizes und andere Instrumente der Selbstbindung haben im Bereich der IT-Sicherheit keine nennenswerte Bedeutung (5.4.3.6).

Zertifizierungen werden im Bereich der IT-Sicherheit derzeit häufig eingesetzt und sind künftig wohl ein zunehmend genutztes Instrument (5.4.3.7). Allerdings fehlt es an flächendeckend genutzten Standards für die Zertifizierung von IT-Sicherheit. Vor allem fehlt es an anerkannten Standards für die Durchführung von Zertifizierungen einschließlich der Prüfintensität (5.4.3.7.2). Zudem verwenden Zertifizierungsstellen derzeit noch überwiegend eigene, nicht transparente Anforderungen, wodurch der Wert von Zertifizierung für die Regulierung von IT-Sicherheit sehr stark eingeschränkt wird. Zwar mag das bei den vom BSI anerkannten Prüfstellen anders sein. Diese betreffen aber nur einen kleinen Teil der in der Praxis erfolgenden Zertifizierung.

7.1.1.2 Durchsetzung materieller Anforderungen

Die Durchsetzung von materiellen Anforderungen an IT-Sicherheit lässt sich weitgehenden Fehlens gesetzlicher Normierung der IT-Sicherheit derzeit nicht verlässlich bewerten. Es spricht aber einiges für das Bestehen erheblicher Defizite.

So weist bei den datenschutzrechtlichen Anforderungen an IT-Sicherheit nach § 9 BDSG, die seit 1991 gelten, ein auffälliges Fehlen an behördlichen Maßnahmen zum Vollzug der Anforderungen auf erhebliche Durchsetzungsdefizite hin (5.4.3.1.5) sind. Auch dies hängt vermutlich mit der Unklarheit über die konkreten Anforderungen zusammen.

Die Rechtsprechung ist bei der Durchsetzung von IT-Sicherheit blass, insbesondere bei der Durchsetzung. technischer Anforderungen an IT-Sicherheit (5.4.3.2.3).

Die Durchsetzung von IT-Sicherheit durch behördliche Aufsicht (5.4.3.3) lässt sich derzeit nicht verlässlich beurteilen, da es teilweise schon an einer zuständigen Behörde fehlt. Auch soweit umfassende Zuständigkeiten bestehen, wie im Bereich der datenschutzrechtlichen Anforderungen an IT-Sicherheit, werden ausweislich der Tätigkeitsberichte generell nicht viele Aufsichtsverfahren zu Maßnahmen von IT-Sicherheit durchgeführt.

Die Durchsetzung von IT-Sicherheit durch Zertifizierung (5.4.3.7) lässt sich derzeit kaum sicher beurteilen. Es ist zu vermuten, dass die Zertifizierung zu einer erheblichen Verbesserung von IT-Sicherheit führt. Für eine genaue Untersuchung fehlt es derzeit aber oft schon an der Grundlage, einem öffentlichen Prüfstandard mit breiter Anwendung in der Praxis. Insbesondere fehlt es an einer klaren rechtlichen Verknüpfung von Zertifizierung und Erfüllung rechtlicher Anforderungen an IT-Sicherheit, die bisher nur in eher seltenen Einzelfällen besteht (5.4.3.7.3).

7.1.1.3 Ergebnis: Notwendigkeit der Weiterentwicklung der IT-Sicherheitsregulierung

Als Gesamtergebnis der Analyse ist festzustellen, dass die Regulierung der IT-Sicherheit derzeit noch am Anfang steht. Sowohl hinsichtlich der materiellen Anforderungen als auch hinsichtlich der Durchsetzung von Normen bestehen Defizite. Klassische Regulierungen (Gesetzgebung, Rechtsprechung) sind im Bereich der IT-Sicherheit nur eingeschränkt leistungsfähig, so dass Bedarf nach Ausgleich durch andere Instrumente besteht. Hier zeigen sich Möglichkeiten, etwa durch Standards und Zertifizierungen, die aber bestenfalls im Ansatz bestehen und noch nicht im notwendigen Maß zur Verfügung stehen.

Dieser Befund ist nicht erstaunlich, da die Notwendigkeit von IT-Sicherheit letztlich erst seit wenigen Jahren ins Bewusstsein der Öffentlichkeit getreten ist und sich erst in jüngerer Zeit eine Bedrohungslage entwickelt hat, welche die Notwendigkeit von IT-Sicherheit unmissverständlich vor Augen führt.

Diese Ergebnisse gelten in besonderer Weise für die I4.0, da in der industriellen Produktion IT-Sicherheit zumeist durch weitest gehende technische Abschottung gewährleistet wurde und das Bewusstsein für IT-Sicherheitsrisiken durch aktuelle technologische Entwicklungen erst noch wachsen muss. Insoweit ist besonders problematisch, dass sich auch die Selbstregulierungsmechanismen einschließlich der Zertifizierung bisher noch nicht auf die besonderen Anforderungen an die I4.0 einstellen konnten.

Dies zwingt zu dem Schluss, dass die Regulierung der IT-Sicherheit, gerade im Hinblick auf die I4.0, der Weiterentwicklung bedarf.

7.1.2 Herausforderungen Technik

In den Kapiteln 4, 5 und 6 wurden die wesentlichen Herausforderungen technischer Art aufgezeigt. Eine Vielzahl von Bedrohungen und zugehörige IT-Sicherheitsmaßnahmen basierend auf Best Practices und Standards wurden untersucht. Technische Implementierungshindernisse bestehender Empfehlungen für IT-Sicherheitsmaßnahmen können deren Umsetzung in Wertschöpfungsnetzwerken der I4.0 verhindern. Bestehende Konzepte (Zonierung) sind somit nicht mehr im gleichen Maße wie in der heutigen Industrie 3.x anwendbar bzw. wirkungsvoll. Neue Konzepte, insbesondere im Umgang mit sensiblen Informationen bei der notwendigen Weitergabe an Wertschöpfungsnetzwerkpartner sind eine daraus resultierende Handlungsmöglichkeit.

7.1.3 Herausforderungen Organisatorisch

In den Kapiteln 5.2 und 5.3 wurden die wesentlichen Herausforderungen organisatorischer Art aufgezeigt.

Es hat sich gezeigt, dass viele der organisatorischen Sicherheitsmaßnahmen, die heute für das industrielle Umfeld empfohlen und dort auch vielfach bereits umgesetzt sind, auch für die I4.0 geeignet sind. Es ist allerdings zu beachten, dass durch die Überwindung von Unternehmensgrenzen zahlreiche neue Schnittstellen entstehen und neue Prozesse etabliert werden müssen. Diese müssen jeweils einzeln für sich und für ihre Auswirkungen auf andere Prozesse hin untersucht werden, um geeignete organisatorische Maßnahmen umsetzen zu können. Die Gefahren, die von einer fehlenden oder mangelhaften Umsetzung der Maßnahmen ausgehen, sind im I4.0-Kontext als deutlich größer einzuschätzen, zumal es mehr Akteure im Wertschöpfungsnetzwerk gibt und zwischen diesen eine wesentlich größeren Menge an sensiblen Daten (und Unternehmensgeheimnissen) ausgetauscht wird.

7.1.4 Herausforderungen Recht

In den Studienkapiteln 5.4 wurden die wesentlichen Herausforderungen rechtlicher Art bei Implementierung von IT-Sicherheitsmaßnahmen aufgezeigt.

Aus der rechtlichen Perspektive ist deutlich geworden, dass die Fragestellungen, die derzeit in der juristischen Literatur vermehrt betrachtet werden (v.a. Datenschutz), nur teilweise die faktischen Probleme der KMU bei der Umsetzung von I4.0 betreffen: Vordringlich sind hier strukturelle Maßnahmen im Rechtsraum nötig um Unsicherheiten über konkrete Anforderungen zu beseitigen, wirksame Erlaubnisnormen und Durchsetzungsmechanismen zu schaffen, zu einer einheitlichen Vertragspraxis zu gelangen und Standards und Zertifikate zu etablieren auf deren Basis die Unternehmen ihre Leistungen anbieten und weiterentwickeln können.

7.2 Handlungs- und Lösungsmöglichkeiten

In den Studienkapiteln 5 und 6 wurden die wesentlichen Handlungs- und Lösungsmöglichkeiten aufgezeigt. Die folgenden Abschnitte fassen dies kurz zusammen und erläutern besonders relevante Punkte.

7.2.1 Handlungsmöglichkeiten aus technischer Sicht

Wie eingangs beschrieben, resultieren die in Kapitel 6 vorgestellten neuartigen Sicherheitskonzepte aus einer Prüfung von einzelnen vorhandenen Konzepten aus anderen Anwendungsfeldern im Hinblick auf deren Übertragbarkeit für I4.0.

Für den technischen Teil wurden dazu zunächst die in Kapitel 4 entwickelten Bedrohungs- und Risikomodelle herangezogen, auf deren Basis eine Auswahl von Sicherheitskomponenten in Abhängigkeit von zu schützenden Werten und Angriffsvektoren erfolgte. Die vorgestellten Konzepte umfassen nicht nur technische Aspekte, wie z. B. die Absicherung von Informationsströmen zwischen, sowie die Datenquellen und Datensenken selbst, sondern adressieren auch Fragestellungen des Daten-, Know-how- und Piraterie-Schutzes. Dies resultierte in einem breit gefächerten Spektrum von Konzepten zur Erzielung eines angemessenen Schutzniveaus durch Industrial Rights Management, der Verwendung hardware-basierter Sicherheitsanker, Production Line IT-Security Monitoring sowie der Integration von Safety und Security. Wie schon in Kapitel 6.5 festgestellt, konnte in Ermangelung belastbarer Zahlen aus den Fallbeispielen keine abschließende Wirtschaftlichkeitsberechnung erfolgen. Eine wirtschaftliche Übertragung der gefundenen Konzepte auf Produktionsumgebungen erscheint jedoch durchaus realisierbar. Ferner wurde Wert darauf gelegt, dass auch Praxiserfahrungen sowohl hinsichtlich der Sicherheit beim Betreiber als auch beim Integrator und der Sicherheit in einzelnen Produkten bei der Ausarbeitung der Konzepte Berücksichtigung fanden. Aus den bestehenden Kooperationen des Bundesamts für Sicherheit in der Informationstechnik (BSI) mit der Industrie

konnte hier ein hohes Maß an Fachwissen bezüglich der technischen Umsetzbarkeit von Sicherheitstechnologien eingebracht werden.

7.2.1.1 Security

Sicherheit („Security“) kann weder verordnet werden (siehe z. B. Signaturgesetz, DE-Mail-Gesetz), noch kann sie durch Standards erzwungen werden. Vielmehr ist Sicherheit das Ergebnis eines komplexen Regelungsprozesses, in dem die Sicherheit des Ist-Zustands analysiert und durch Ergreifen zusätzlicher Maßnahmen in einen sichereren Soll-Zustand überführt werden soll. Hierzu sind die nachfolgend aufgeführten Maßnahmen erforderlich.

Da heutige ICS-Systeme mit hoher Wahrscheinlichkeit in gleicher oder veränderter Form auch in I4.0 eingesetzt werden, muss dieser Regelungsvorgang bereits heute angestoßen werden, um mit einem adäquaten Sicherheitsniveau in I4.0 starten zu können.

7.2.1.1.1 Forensische Analyse gemeldeter Sicherheitsvorfälle (reaktiv)

Angriffe auf ICS-Systeme finden täglich statt: In seinem Bericht für das US-Fiskaljahr 2014 listet das amerikanische ICS-Cert 245 gemeldete Angriffe auf kritische ICS-Infrastrukturen auf[562], die Dunkelziffer dürfte weitaus höher liegen.

Nur bei etwa der Hälfte dieser Vorfälle konnte aufgeklärt werden, wie die Angreifer ins ICS-System eingedrungen sind. Heutige Anomalie-Erkennungssysteme helfen bei der Aufklärung dieser Vorfälle (und der anschließenden Verbesserung der Systemsicherheit) nicht, da sie nur bekannte Angriffsmuster zuverlässig erkennen.

Hier ist also zunächst eine forensische Ermittlung der verwendeten Angriffsmuster gemeldeter Sicherheitsvorfälle gefordert, die dann neue Muster in die Anomalie-Erkennung einspeisen kann.

Im Kontext eines Wertschöpfungsnetzwerkes wird die forensische Analyse eines Sicherheitsvorfalls in vielen Fällen viele Komponenten und Systeme bei unterschiedlichen (technische und personelle Ausstattung) Partnern in möglicherweise unterschiedlichen Rechträumen betreffen, hierauf muss sich die Forensik ebenso wie die Hersteller von entsprechenden Werkzeugen, Hersteller von Anomalie-Erkennungssystemen sowie deren Betreiber einstellen.

7.2.1.1.2 Penetration Testing (proaktiv)

Eine forensische Analyse kann Vorfälle nur erkennen, wenn der Schaden bereits eingetreten ist. Unerkannte, neue Angriffsvektoren können somit großen Schaden anrichten und die Reputation ganzer Industrien (Automobilindustrie!) beeinträchtigen, bevor sie erkannt und neutralisiert werden.

Auch ist die Beseitigung eines einmal erfolgreichen Angriffs („Advanced Persistent Threat (APT)“, vgl. Jahresbericht BSI 2014) manchmal mit enormen Aufwand verbunden, wie der Hackerangriff auf den Deutschen Bundestag und ähnliche APT-Angriffe zeigen.

Daher ist es sinnvoll, die tatsächliche Sicherheit eines Systems vor einem Angriff zu testen. Dies kann durch kontrollierte Penetration Tests (Pentests), die von spezialisierten Firmen durchgeführt werden, erfolgen.

Sinnvoll ist allerdings die Festlegung eines organisatorischen Rahmenwerks, wie mit den Ergebnissen eines solchen Pentests umgegangen werden soll. Ohne solche Regularien besteht die Gefahr, dass erkannte Sicherheitslücken aus Kostengründen nicht geschlossen werden. Insofern sollten Penetrationstests Teil eines übergeordneten Sicherheitsmanagements sein.

7.2.1.1.3 Definition formaler Sicherheitsziele

Um die Sicherheit eines Systems bewerten zu können, muss man zunächst einmal definieren, was „Sicherheit“ im Kontext des untersuchten Systems überhaupt bedeutet. Ohne eine solche Definition könnte ein Zustand des Systems als sicher angesehen werden, der kritische Schwachstellen besitzt, und gravierende Angriffe erlaubt.

Dies ist z. B. das Problem bei Sicherheitszertifizierungen: Um die Folgekosten einer Zertifizierung niedrig zu halten,

562 News-Meldung “US industrial control systems attacked 245 times in 12 months”, http://www.v3.co.uk/v3-uk/news/2399334/us-industrial-control-systems-attacked-245-times-in-12-months, abgerufen am 08.07.2015.

werden kritische Stellen des Systems oft von der Evaluierung ausgenommen. Dadurch kann man mit geringem Aufwand ein System als „sicher“ zertifizieren, obwohl es gravierende Schwachstellen besitzt.

7.2.1.1.4 Formale Analyse vorgeschlagener Sicherheitsmechanismen

In der Materialwissenschaft, der Raumfahrt, der Pharmazie und vielen weiteren industriellen Bereichen werden zuerst Computersimulationen durchgespielt, bevor ein Stoff oder Antrieb real produziert wird.

Dies ist auch für die IT-Sicherheit sinnvoll, da der Rollout einer Sicherheitsmaßnahme äußerst kostspielig sein kann. Daher sollte die Wirksamkeit dieser Sicherheitsmaßnahme vorher sorgfältig analysiert werden.

Hierfür stehen in der Forschung verschiedene Hilfsmittel bereit: Reduktionsbasierte Beweise für kryptographische Mechanismen und Protokolle, und automatisierte Analysetools zur Analyse der Sicherheit komplexer Systeme.

Als Vorbedingung zum Einsatz dieser Tools müssen die Sicherheitsziele des Systems formal definiert sein (s. o.).

7.2.2 Handlungsmöglichkeiten aus betrieblich/organisatorischer Sicht

Im organisatorischen Teil von Kapitel 6 wurden Konzepte zur Überwindung organisatorischer Hemmnisse vorgestellt, welche neben der Integration von Technik in bestehende Prozesse auch die Rolle des Menschen in von der I4.0 beeinflussten Prozessen, sowie das Vertrauen von KMU in die Technik, in die Kooperationspartner und die Vision von I4.0 berücksichtigen.

Exemplarisch für die Integration von Technik in bestehende Prozesse seien hier die Nutzung von Best-Practice-Berichten, neu zu entwickelnden Bewertungs- und Entscheidungsunterstützungsmodellen und die Sensibilisierung für die sich ändernde Bedrohungslage genannt. Für die Rolle des Menschen steht eine Weiterbildung und Sensibilisierung der Mitarbeiter und die Einführung von Assistenzsystemen, sowie für das Vertrauen in I4.0 das Begreifen des Wandels als zentrales Innovationsthema im Unternehmen und eine gesteuerte Entwicklung und Kommunikation top-down. Weiterhin erscheint die schrittweise Näherung an I4.0 ein wesentlicher Aspekt zu sein, der z. B. durch die Durchführung von Pilotprojekten in vertrauter Umgebung bzw. Kooperationsbeziehungen erreicht werden kann.

7.2.3 Handlungsmöglichkeiten aus rechtlicher Sicht

Im rechtlichen Teil von Kapitel 6 wurden Fragestellungen, wie z. B. zur Datensicherheit, näher analysiert und vertragliche oder legislative Lösungsoptionen aufgezeigt. Durch den Rückgriff auf die Erfahrungen mit Betreibern und Integratoren wurde auch die Akzeptanz dieser Technologien im Kontext Industrie- und Sektoren-spezifischer Rahmenbedingungen und besonderer Anforderungen bewertet. Hierbei wurde insbesondere auf das IT-Sicherheitsgesetz sowie rechtliche Fragen bezüglich notwendiger Zertifizierungen eingegangen.

7.2.3.1 Chancen durch Konzept zur Verbindung der Instrumente

Die Analyse des gegenwärtigen Zustands der IT-Sicherheitsregulierung zeigt, dass die Möglichkeiten der verschiedenen Instrumente zur Regulierung von IT-Sicherheit noch bei weitem nicht in vollem Umfang genutzt werden, und dass es insbesondere an einer schlüssigen Verbindung der einzelnen Elemente fehlt. Daher ist es notwendig, durch ein schlüssiges Konzept zur Regulierung von IT-Sicherheit das Potential der einzelnen Instrumente besser zu nutzen und vor allem die notwenige Verknüpfung der einzelnen Elemente herzustellen.

Ziel und Leitlinie der Regelung von IT-Sicherheit muss dabei Gewährleistung eines hinreichenden Maßes an IT-Sicherheit in allen Bereichen der digitalen Gesellschaft sein. Besonders wichtig ist dies im Bereich der I4.0, bei der Angriffe zu erwarten sind und zu hohem Schadenspotential führen können.

Kern des Konzepts muss es dabei sein, eine Verbindung der stärksten Instrumente im Bereich der materiellen Anforderungen mit jeden Durchsetzungsinstrumenten herzustellen, die für die Durchsetzung dieser Interessen am besten geeignet sind.

7.2.3.2 Materielle Anforderungen an IT-Sicherheit

Bei den materiellen Anforderungen an IT-Sicherheit hat sich gezeigt, dass grundlegende Fragen sowie Verhaltensanforderungen durch Gesetzgebung, konkrete technische Anforderungen besser durch Selbstregulierungsmechanismen, insbesondere Standards in Verbindung mit

Zertifizierungen, geregelt werden können. Entsprechend sollte die Weiterentwicklung der IT-Sicherheitsregulierung diese Instrumente nutzen.

7.2.3.2.1 Gesetzgebung

Die Gesetzgebung kann vor allem im Bereich von Grundlagen der IT-Sicherheit und von Verhaltensanforderungen wirken.

Im Bereich der Grundlagen sollten die bisherigen Defizite beseitigt werden. Auch wenn es hierzu aus heutiger Sicht noch weiterer Forschung bedarf, erscheint es notwendig, die Aufgaben einer allgemeinen Regelung zu Grundlagen der IT-Sicherheit anzugehen. Das IT-Sicherheitsgesetz, das in Teilen noch recht rudimentär wirkt, sollte so schnell wie möglich – und nach Vorbereitung durch Forschung und Diskussion in Fachkreisen – zu einer allgemeinen Regelung ausgebaut werden.

Insbesondere erscheint es notwendig, die Grundlagen für den erfolgreichen Einsatz anderer Instrumente zu legen. Dies betrifft vor allem die Zertifizierung. Hier hat sich im Bereich des Datenschutzes in Bezug auf IT-Sicherheit eine sehr interessante Entwicklung ergeben, die als Vorbild dienen kann. Das Ziel einer Datenschutz-Zertifizierung auf gesetzlicher Grundlage wurde im Datenschutzrecht schon seit längerem diskutiert und in § 9a BDSG bereits ansatzweise geregelt, die beabsichtigte gesetzliche Regelung durch ein Datenschutzaudit-Gesetz ist aber bisher gescheitert.

In jüngster Zeit hat sich im Hinblick auf die Anforderungen an die IT-Sicherheit aber eine sehr dynamische und vielversprechende Entwicklung ergeben, an derer die Bundesregierung erfolgreich mitgewirkt hat. Im Bereich der Auftragsdatenverarbeitung, welche die datenschutzrechtliche Grundlage des Cloud Computing darstellt, verlangt das BDSG von Auftraggeber eine Überprüfung der technischen und organisatorischen Maßnahmen zur Gewährleistung von IT-Sicherheit. Hier hat sich die Erkenntnis durchgesetzt, dass die Kontrolle der technischen und organisatorischen Maßnahmen am besten durch eine Zertifizierung erfolgen kann. So haben der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. und die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. im Jahre 2013 eine Gesellschaft zur Zertifizierung von Auftragsdatenverarbeitungsdiensten gegründet und einen Prüfungsstandard herausgegeben, der der Zertifizierung zugrunde liegen soll.

In jüngster Zeit wurden im Rahmen des Trusted Cloud-Programms im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) von der sog. Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ und dem Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ Grundlagen für eine Datenschutz-Zertifizierung erarbeitet. Bereits in ihrem Ausgangspapier hat die AG Rechtsrahmen, wegen der Unsicherheit in Bezug auf die Grundlagen und Rechtsfolgen der Zertifizierung, eine gesetzliche Reglung der Zertifizierung gefordert. In dem aktuellen Papier zum Zertifizierungsverfahren sind weitere Kernelemente der erforderlichen gesetzlichen Regelung genannt und Regelungsvorschläge unterbreitet.

Die Entwürfe des Europäischen Parlamentes und des Ministerrats zur Datenschutz-Grundverordnung sehen, wenngleich nur in Grundzügen und divergierend, eine gesetzliche Regelung zur Zertifizierung vor.

Diese Entwicklung ist überaus wichtig und relevant für die IT-Sicherheits-Regulierung insgesamt. Das Datenschutzrecht erfasst einen großen Bereich der Datenverarbeitung überhaupt, ist also der Sache nach schon fast eine allgemeine Regelung der IT. Zugleich umfasst das Datenschutzrecht durch die Anforderungen des § 9 BDSG an die technischen und organisatorischen Maßnahmen zur IT-Sicherheit jedenfalls große Teile der IT-Sicherheit.

Die Entwicklung der Zertifizierung und ihre gesetzliche Grundlage im Datenschutzrecht muss daher schon wegen ihrer faktischen Bedeutung für die IT-Sicherheit beachtet werden. Umso mehr ist es erforderlich, diesen Ansatz zu stärken und in Bezug zu einer Regelung der IT-Sicherheit insgesamt zu stellen. Damit könnten sich widersprechende Regeln vermieden werden und zugleich die Chancen der bisherigen Arbeit im Bereich der datenschutzrechtlichen IT-Sicherheit für die Regulierung der IT-Sicherheit insgesamt genutzt werden.

Konkret sollte eine gesetzliche Regelung zur IT-Sicherheits-Zertifizierung erfolgen, die Voraussetzungen, Verfahren und rechtliche Bedeutung der Zertifizierung regelt. Dabei sollte die Möglichkeit der Zertifizierung nicht staatlichen Stellen, etwa dem BSI, vorbehalten sein, sondern, ebenso wie im Konzept der datenschutzrechtlichen Zertifizierung, durch Unternehmen möglich sein. Umso mehr bedarf es einer klaren gesetzlichen Grundlage für die genannten Aspekte. Anders als im Bereich des Datenschutzes kann der nationale Gesetzgeber hier selbst tätig werden.

Die sektorspezifische Regulierung der IT-Sicherheit muss daneben weiterentwickelt werden. Angesichts der fortschreitenden Bedeutung der IT, beispielsweise im Automobilbereich, ist eine Überarbeitung und Weiterentwicklung der gesetzlichen Anforderungen an Sicherheit in der automobilbezogenen IT, und entsprechend auch im Rahmen der Prüfung und Zertifizierung von Kraftfahrzeugen, unumgänglich.

Eine unmittelbare Reglung technischer Anforderungen durch Gesetz erscheint auch im Bereich der IT-Sicherheit, nicht oder nur in Teilbereichen, sinnvoll.

7.2.3.2.2 Entwicklung prüffähiger Standards

Die größten Potentiale zur Formulierung technischer Anforderungen an IT-Sicherheit liegen bei der Formulierung von Standards.

Neben der gesetzlichen Regelung der Zertifizierung ist auch bei den Standards selbst eine Weiterentwicklung erforderlich. Insoweit kann der Staat jedoch allenfalls Rahmenbedingungen setzen, da Standards nach der bisherigen Erfahrung vor allem dann erfolgreich sind, wenn sie aus den beteiligten Verkehrskreisen hervorgehen.

Der Staat kann darüber hinaus aber auch die Entwicklung von Standards fördern, wie dies etwa im Bereich der Standards für Datenschutz-Zertifizierung geschehen ist. Hier wurde im Rahmen des Trusted Cloud-Programms des BMWi ein prüffähiger Datenschutz-Standard für Cloud-Dienste, das Trusted Cloud-Datenschutzprotokoll für Cloud-Dienste (TCDP) erarbeitet. Das TCDP ist insoweit besonders interessant, als es gesetzliche Anforderungen – hier des BDSG – in prüffähige Anforderungen umsetzt und zugleich auf dem ISO/IEC 27018-Standard und dem ISO/IEC 27002-Standard aufsetzt, wodurch international bekannte Standards genutzt werden.

Es ist daher zu erwägen, auch die Entwicklung von Sicherheits-Standards für die I4.0 zu fördern.

7.2.3.2.3 Vertragliche Anforderungen

Vertragliche Anforderungen können in erheblichem Maß zur Bestimmung von Anforderungen an IT-Sicherheit beitragen. Erforderlich ist dazu aber eine Grundlage. Auch insoweit kommt der Entwicklung von Grundlagen, etwa durch gesetzliche Verhaltensregeln oder durch technische Standards, auf die Bezug genommen werden kann, entscheidende Bedeutung zu.

Die Entwicklung von Musterverträgen kann möglicherweise ebenfalls gute Impulse liefern. Ob die Regierung, hierzu, wie es die EU-Kommission derzeit für Vertragsbedingungen im Cloud Computing versucht, gute Beiträge leisten kann, lässt sich nicht verlässlich abschätzen. Da die Vertragsfreiheit einen Kern der Privatautonomie ausmacht, spricht einiges dafür, die Entwicklung von Musterverträgen und Musterklauseln im Kern den beteiligten Wirtschaftskreisen zu überlassen. Insoweit ist allerdings eine gewisse Skepsis angezeigt, da sich im unterschiedliche Verständnisse bei US-amerikanischen und deutschen Unternehmen in Bezug auf vertragliche Regeln zu bestehen scheinen. Dies könnte die Bildung einheitlicher Vertragsbedingungen entscheidend erschweren. Zugleich wären sie aber äußerst hilfreich.

Die Entwicklung von Musterverträgen oder -klauseln zur IT-Sicherheit verspricht nicht zuletzt im Hinblick auf die Internationalität der Informationstechnologie und der IT-Dienste große Chancen, wenn es gelingt, gemeinsame Positionen der Wirtschaft in diesem Aspekt zu entwickeln.

7.2.3.3 Durchsetzungsmechanismen

7.2.3.3.1 Behördliche Aufsicht

Die Notwendigkeit einer Stärkung der behördlichen Aufsicht für IT-Sicherheit erscheinen angesichts der bestehenden Unvollständigkeit des Systems aus wissenschaftlicher Sicht offensichtlich. Dies gilt insbesondere im Hinblick auf I4.0. Bei der Weiterentwicklung der behördlichen Aufsicht sollten insbesondere die institutionellen Defizite des gegenwärtigen Zustands, etwa das Fehlen von zuständigen Behörden und Aufgaben, behoben werden. Dabei sollte am IT-Sicherheitsgesetz angesetzt werden. Die Möglichkeit behördlicher Anordnungen bei Mängeln der IT-Sicherheit sollte letztlich flächendeckend möglich sein und nicht auf Branchen oder vorgeblich besonders wichtige Bereiche beschränkt sein.

Die Beschränkung auf „kritische Infrastrukturen“ ist im Hinblick auf I4.0 zu überprüfen. Jedenfalls Teilbereiche der I4.0 sollten in das Regime des IT-Sicherheitsgesetzes einbezogen werden. Eine generelle Bezeichnung von I4.0 als „kritische Infrastruktur“ wiederum würde freilich über das Ziel hinausschießen. Die Formulierung einer sachgerechten Beschränkung bedarf der fachlichen Vorbereitung.

Bei der Weiterentwicklung der behördlichen Aufsicht sollten die Möglichkeiten der Zusammenwirkung bestehender Aufsichtsbehörden ausgelöst werden. Hierzu dürften aber noch vorbereitende Arbeiten erforderlich sein. Insbesondere ist sorgfältig zu prüfen, bei welchen Behörden diese Aufsicht angesiedelt sein sollte. Eine Alleinzuständigkeit des BSI für die Aufsicht im Bereich der IT-Sicherheit ist offensichtlich nicht sinnvoll, da die Aufsicht der gesamten Wirtschaft und der gesamten Verwaltung das BSI überfordern würde. Insbesondere ist die Zusammenarbeit bei IT-Sicherheit und IT-Sicherheit im Datenschutz auch auf der Ebene der Aufsicht abzustimmen.

Die Einschätzungen aus der Praxis, die im Rahmen dieser Studie nicht flächendeckend ermittelt werden konnte, divergieren. In den seitens der Beteiligten und des Beirats übermittelten Stellungnahmen lehnen teilweise jegliche weitere Regulierung, damit wohl auch stärkere Aufsichtsbefugnisse für Behörden, an. Andere hingegen betonen, dass die Durchsetzung von Sicherheitsanforderungen gewährleistet werden müsse.

7.2.3.3.2 Rechtsprechung

Die Rechtsprechung kann ihre Kraft zur Durchsetzung normativer Anforderungen an die IT-Sicherheit nur entfalten, wenn klare Ansprüche und Klagebefugnisse zur Verfügung stehen. Da es hieran bisher mangelt, sind diese zu schaffen. Insoweit wird der Gesetzgeber gefragt sein, da nicht erkennbar ist, dass sich diese aus der Praxis hinreichend dynamisch entwickeln. Auch insoweit werden aber Vorarbeiten erforderlich sein. Derzeit lässt sich kaum abschätzen, ob zusätzliche Verbandsklagebefugnisse sinnvoll wären. Zu beachten ist, dass sich, soweit eine gesetzliche Regelung der IT-Sicherheit erfolgt, möglicherweise schon nach derzeitiger Gesetzeslage das die Instrumentation des Wettbewerbsrechts anwendbar ist. Dies wäre jedenfalls der Fall, wenn diese Gesetze als marktverhaltensregelnde Normen i.S. des § 4 Nr. 11 UWG angesehen wird.

Ein wesentliches Hindernis ist insoweit das Fehlen klarer Ansprüche von Betroffen bzw. Geschädigten und die Schwierigkeit eines Nachweises der Kausalität im Fall von Rechtsverletzungen. Insoweit wäre ggf. durch Erleichterung von Darlegungen oder Beweislast in Bezug auf IT-Sicherheit zu denken, ähnlich wie es bei der Produkthaftung der Fall ist. Auch solche Maßnahmen bedürfen freilich der fachlichen Vorbereitung.

7.2.3.3.3 Zertifizierung

Die Zertifizierung von IT-Sicherheit bietet wie dargestellt, große Chancen für die Gewährleistung von IT-Sicherheit. Diese sollte ausgebaut werden. Insoweit ist, wie dargestellt, eine gesetzliche Klärung der rechtlichen Bedeutung von Zertifizierung erforderlich. Weiterhin bedarf einer gesetzlichen Regelung des Zertifizierungsverfahrens. In beiden Aspekten hat die aktuelle Entwicklung der Datenschutz-Zertifizierung wesentliche Vorarbeiten hervorgebracht, die als Impuls für die Regulierung der IT-Sicherheit insgesamt genutzt werden können (s. o.).

Unabdingbar und zentral ist aus wissenschaftlicher Sicht die Schaffung eines gesetzlichen Rahmens für IT-Sicherheits-Zertifizierungen. Bei der Diskussion um die Datenschutz-Zertifizierung hat sich als zentrale Schwierigkeit gezeigt, dass die Anforderungen an die Stelle, die Zertifizierungen mit rechtlicher Wirkung erteilen können, ebenso wie Anforderungen an das Verfahren der Zertifizierung, nicht hinreichend geklärt sind. Daher fordern Aufsichtsbehörden und Unternehmen eine gesetzliche Regelung dieser Elemente der Datenschutz-Zertifizierung. Dieselbe Forderung ist auch an die Zertifizierung von IT-Sicherheit generell zu stellen. Es ist daher ein gesetzliche Regelung von Voraussetzungen, Verfahren und rechtlicher Wirkung der IT-Sicherheits-Zertifizierung dringend geboten.

7.2.3.3.4 Unterstützung und Flankierung der Selbstregulierung

Die größte Bedeutung für die IT-Sicherheit dürfte auch künftig der Selbstregulierung zukommen. Dies gilt uneingeschränkt auch für die I4.0. Allerdings ist die Entwicklung bisher noch völlig am Anfang. Erforderlich ist daher eine Förderung der Entwicklung von Selbstregulierungsmechanismen für die I4.0.

Der vom IT-Sicherheitsgesetz vollzogene Ansatz in § 8a Abs. 2 BSI-Gesetz könnte dabei ein geeigneter Ausgangspunkt sein. Allerdings sollte ein deutlicherer Anreiz zur Wahrung von Sicherheitsstandards geschaffen werden. Insbesondere sollte im Gesetz eindeutig bestimmt werden, dass die Wahrung der vom BSI anerkannten branchenspezifische Ansatz die gesetzlichen Anforderungen, soweit sie vom Standard abgedeckt sind, erfüllt, da sonst Rechtsunklarheit entstehen kann. Durch eine solche Klarstellung könnte sich für die Wirtschaft ein wichtiger Anreiz zur Schaffung von sicherheitsbezogenen Pflichten ergeben. Allerdings müssen auch insoweit noch fachliche Grundlagen (Klärung Verhältnis zu

allgemeinen Regeln, Verfahren zur Bildung und Geltungsbereich von Standards der Praxis etc.) gelegt werden.

Ein wesentlicher Ansatzpunkt ist dabei die Forschung zur Regelung von IT-Sicherheit in der I4.0, die im Rahmen dieser Studie nur angesprochen, aber nicht vollzogen werden kann (dazu unten), damit die Grundlagen geklärt werden können.

Die Formulierung von Musterverträgen oder -klauseln kann letztlich nur durch die Praxis erfolgen. Hier kann der Staat unterstützen, etwa durch Initiierung von Prozessen zur Diskussion und Entwicklung von angemessenen Regeln (dazu auch unten).

Für die Entwicklung von Kodizes für I4.0 ist es derzeit noch zu früh. Hier sind weitere Forschungsarbeiten erforderlich.

7.2.3.4 Forschung und Weiterentwicklung der IT-Sicherheitsregulierung für Industrie 4.0

Die Analyse hat gezeigt, dass Regulierung von IT-Sicherheit generell noch am Anfang ist. Daher ist insofern Erforschung und Weiterentwicklung der IT-Sicherheits-Regulierung notwendig. Dies gilt angesichts der erheblichen Gefährdungen der vernetzen Entwicklung und Produktion in besonderer Weise für die I4.0.

Notwendig erscheint ein Forschungsprogramm, um die dringend benötigte interdisziplinäre Forschung zu den Chancen und Anforderungen an IT-Sicherheits-Regulierung in kurzer Zeit zu etablieren. Dabei sollten die Bedürfnisse der I4.0 explizit adressiert werden.

7.2.3.5 Handlungsempfehlungen im Bereich des Vertragrechts

Die spezifischen Implementierungshindernisse für die I4.0 im Bereich der vertraglichen Regelung zur IT-Sicherheit betreffen vor allem die materiellen Regeln. Die schwierigen Fragen des anwendbaren Rechts können durch Rechtswahl überwiegend geklärt werden und werden in der Praxis entsprechend gelöst.

Bei den materiellen vertraglichen Regeln zur IT-Sicherheit in der I4.0 herrscht derzeit große Unsicherheit. Dies beruht wesentlich auf den allgemeinen Problemen der Regulierung von IT-Sicherheit, die hier in vollem Umfang relevant werden. Entsprechend ist für die Handlungsempfehlungen uneingeschränkt auf die allgemeinen Handlungsempfehlungen zur IT-Sicherheits-Regulierung zu verweisen.

Bei den materiellen vertraglichen Regeln zur IT-Sicherheit in der I4.0 herrscht derzeit große Unsicherheit. Dies beruht wesentlich auf den allgemeinen Problemen der Regulierung von IT-Sicherheit, die hier in vollem Umfang relevant werden. Entsprechend ist für die Handlungsempfehlungen uneingeschränkt auf die allgemeinen Handlungsempfehlungen zur IT-Sicherheits-Regulierung zu verweisen.

7.2.3.6 Handlungsempfehlungen im Bereich des Haftungsrechts

Im Bereich der außervertraglichen Haftung steht die I4.0 vor der Herausforderung, dass erhebliche Schadens- und Haftungsrisiken bestehen, über deren sachgerechte Eingrenzung und Allokation derzeit noch weitgehend Unsicherheit besteht. Auch insoweit handelt es sich im Wesentlichen um allgemeine Probleme der Regulierung von IT-Sicherheit, so dass auch insoweit auf die allgemeinen Handlungsempfehlungen verwiesen werden kann. Besonderes Gewicht sollte dabei auf die Formulierung geeigneter Verhaltenspflichten gelegt werden. Insoweit ist, wie dargestellt, auch der Gesetzgeber in der Pflicht.

Ein Schwerpunkt der Weiterentwicklung sollte auch im Hinblick auf die außervertragliche Haftung bei der Entwicklung geeigneter vertraglicher Regeln zwischen den Kooperationsbeteiligten liegen, da der Schwerpunkt der Schadensrisiken bei Kooperationsbeteiligten liegt und die Schutzpflichten ebenso wie die Risikoverteilung zwischen den Kooperationsbeteiligten vertraglich geregelt werden kann.

Das Erfordernis gesetzlicher Maßnahmen, etwa gesetzlicher Haftungsbegrenzungen, kann derzeit nicht sicher beurteilt werden. Daher sind, vor einer etwaigen Einleitung gesetzgeberischer Maßnahmen, fachliche Vorarbeiten erforderlich.

7.2.3.7 Handlungsempfehlungen im Bereich des Datenschutzrechts

7.2.3.7.1 Schaffung neuer datenschutzrechtlicher Legitimationen für den Datenumgang und -austausch

Die bisher gängigen datenschutzrechtlichen Erlaubnistatbestände sind zur Legitimation des Datenumgangs und -austauschs zwischen den Partnern im Rahmen von I4.0 nur bedingt geeignet und unterliegen erheblichen Rechtsunsicherheiten. Die Schaffung neuer Erlaubnistatbestände ist daher aus unserer Sicht zumindest zweckmäßig, wenn nicht sogar geboten.

Insofern könnten einerseits neue gesetzliche Erlaubnistatbestände geschaffen werden, die eindeutig auf eine partnerübergreifende, automatisierte Zusammenarbeit ausgerichtet sind und im Rahmen von I4.0 als Legitimation herangezogen werden können. Die Schaffung eines solchen Erlaubnistatbestandes auf deutscher Ebene wird gleichwohl erheblichen Schwierigkeiten unterliegen, da die datenschutzrechtlichen Normen auf den Vorgaben der EU-DatenschutzRL basieren, die eine spezielle Erlaubnis für solche Zusammenhänge nicht vorsieht. Die avisierte DS-GVO sieht derzeit indes noch Gestaltungsmöglichkeiten bezüglich eines eigenständigen nationalen Beschäftigtendatenschutzes vor[563], sodass zumindest nach dessen Inkrafttreten eine Schaffung entsprechender Erlaubnistatbestände durch die nationalen Gesetzgeber in Betracht gezogen werden sollte. Alternativ könnten entsprechende Erlaubnistatbestände auch unmittelbar in die EU-Datenschutz-Grundverordnung aufgenommen werden, was sich aufgrund des Umstandes, dass I4.0 über Ländergrenzen hinweg zum Einsatz kommen soll, ohnehin empfehlen dürfte.

Solange es an entsprechenden gesetzgeberischen Gestaltungen fehlt, sollte zumindest ein Anforderungskatalog entwickelt und veröffentlicht werden, aus dem hervorgeht, in welchen Fällen Nutzer von I4.0 davon ausgehen dürfen, dass der Austausch von personenbezogenen Beschäftigten- und Kundendaten in der Produktionskette erlaubt ist. Dies sollte mit der Erstellung von Mustervertragsklauseln einhergehen, bei deren Abschluss Partner in einer Produktionskette davon ausgehen dürfen, dass der Datenaustausch aus vertraglich ordnungsgemäß ausgestaltet ist. Diese sollten von dem Düsseldorfer Kreis[564] in Kooperation mit Branchenverbänden (insbes. VDMA) entwickelt werden, um eine größtmögliche Praxisrelevanz bei gleichzeitig maximaler Verbindlichkeit sicherzustellen.

Insgesamt sollten eindeutige Kriterien mit Regelbeispielen dafür vorgegeben werden, wann Unternehmen davon ausgehen dürfen, dass der Austausch von personenbezogenen Kunden- und Beschäftigtendaten über die existierenden Erlaubnistatbestände (derzeit §§ 28, 32 BDSG) legitimiert ist.

Eine weitere Möglichkeit besteht darin, Mustereinwilligungserklärungen zu schaffen, die der Legitimierung im Rahmen von automatisierten Produktionsprozessen dienen können. Als Beispiel können hier die zwischen dem Düsseldorfer Kreis und der Versicherungswirtschaft ausgehandelten Einwilligungs- und Schweigepflichtentbindungserklärungen dienen.[565] Dies könnte analog wiederum über eine Kooperation zwischen Branchenverbänden (z. B. VDMA) und Düsseldorfer Kreis gelöst werden.

7.2.3.7.2 Schaffung eines einheitlichen Rechtsrahmens/ einheitlicher Standards für grenzüberschreitenden Datenverkehr

Weiterhin empfehlen wir, wie derzeit in dem DS-GVO-E vorgesehen, einen einheitlichen rechtlichen Standard für länderübergreifenden Datenverkehr – jedenfalls soweit dies möglich ist, also jedenfalls innerhalb der EU – einzuführen, um bezüglich des grenzüberschreitenden Datenverkehrs Rechtsunsicherheiten zu vermeiden. Hierbei sollte allerdings darauf geachtet werden, dass die prozessualen Anforderungen an den Datenschutz gerade für mittelständische Unternehmen nicht überspannt werden. Die derzeit im DS-GVO-E vorgesehenen Anforderungen in Bezug auf Datenschutzrisikoanalysen, -folgenabschätzungen und Compliance-Reviews[566] sollten daher noch einmal kritisch hinterfragt werden, da diese gerade im Zusammenhang mit I4.0 wirtschaftlich unauflösbare Herausforderungen schaffen können, nicht zuletzt aufgrund der erheblichen Bußgelder, die im Falle von Verstößen drohen.

Überdies müssen den Anwendern unverzüglich Vertragsklauseln an die Hand gegeben werden, bei denen sie davon ausgehen können, dass der multinationale Datenaustausch im Rahmen von I4.0 nicht deshalb rechtswidrig ist, weil es an einem angemessenem Datenschutzniveau bei den datenempfangenden Partnern in Drittstaaten fehlt. Insoweit kommt entweder eine klare Stellungnahme der Aufsichtsbehörden dahingehend in Betracht, dass EU-Standardvertragsklauseln stets, also auch bei bestehenden Verarbeitungsbezügen zu den USA, als hinreichende Garantien i.S.v. § 4c Abs. 2, Hs. 2 BDSG zu qualifizieren sind. Alternativ kommt der Entwurf eigenständiger Musterklauseln durch den Düsseldorfer Kreis in Betracht, bei deren Abschluss Unternehmen von einem hinreichenden Datenschutzniveau bei dem jeweiligen Datenempfänger ausgehen dürfen; aufgrund des multinationalen Bezuges von I4.0 dürfte es sich bei

563 S. Art. 82 DS-GVO-E.
564 Inoffizieller Zusammenschluss der Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich.
565 Abrufbar unter https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2012/index.php
566 Vgl. hierzu Behling/Abel/Behling, Praxishandbuch Datenschutz im Unternehmen, 1. Aufl. 2014, Kap. 1 Rn. 46 ff.

dem Entwurf solcher eigenständigen Musterklauseln allerdings empfehlen, die Abstimmung mit der Artikel-29-Datenschutzgruppe und wichtigen Handelspartnern (wie z. B. China oder USA) zu suchen.

Ohnehin ist zu empfehlen, das Modell der derzeitigen EU-Standardvertragsklauseln dahingehend zu überdenken, als diese den multilateralen Abschluss originär nicht vorsehen. Prototypisch müsste derzeit daher ggfs. eine Vielzahl von EU-Standardvertragsklauseln zwischen Nutzern von I4.0 abgeschlossen werden, wenn die Produktions- und Verarbeitungskette Drittstaatenbezüge aufweist. Da sich dies bereits unter Praktikabilitätsaspekten als schwierig erweist, sind deutlich flexiblere Standardvertragsklauseln erforderlich, die auch komplexe Datenverarbeitungen mit zahlreichen Partnern in einem internationalen Netzwerk abbilden können. Dabei wäre es wünschenswert, dass solche Standardvertragsklauseln nicht nur die datenschutzrechtlichen Fragen regeln, sondern auch Fragen zum Umgang mit Betriebs- und Geschäftsgeheimnissen, dies zumindest im Sinne eines Minimalkonsenses, damit gerade mittelständische Partner von I4.0 ein Vertragswerk nutzen können, bei dem sie ohne umfangreiche Rechtsberatung unterstellen können, dass sie vor rechtlichen und tatsächlichen Risiken möglichst umfassend geschützt sind. Insoweit kommt etwa eine Kooperation von Branchenverbänden (insbes. VDMA), Düsseldorfer Kreis, Artikel-29-Datenschutzgruppe sowie Rechtsexperten aus der unternehmerischen Praxis und Beratung in Betracht.

Schließlich benötigen die Partner von I4.0 einen klaren Orientierungsrahmen für die wirtschaftliche Implementierung von hinreichenden technisch-organisatorischen Maßnahmen. Hier kann das in dem DS-GVO-E bereits vorgesehene sog. Europäische Datenschutzsiegel ggfs. einen Beitrag leisten.

7.2.3.8 Handlungsempfehlungen im Bereich des WTO-Rechts

Aus dem WTO-Recht ergeben sich keine unmittelbaren Handlungsempfehlungen.

7.2.3.9 Handlungsempfehlungen im Bereich des gesetzlichen Geheimnisschutzes

Im Bereich des Geheimnisschutzes empfehlen wir von gesetzgeberischer Seite eine länderübergreifende Vereinheitlichung der Schutzstandards, wobei diesbezüglich mit der neuen Geheimnisschutzverordnung bereits ein Anfang geschafft sein dürfte, was es dann indes noch im Einzelnen bei einem Inkrafttreten zu eruieren gilt. Gleichwohl kann zwischen den Partnern auch Abhilfe geschaffen werden, indem „Non Disclosure Agreements“ (NDA) oder ähnliche Vereinbarungen erfolgen, wobei diese sich auch dazu äußern sollten, in welchem Umfang der Umgang mit Betriebs- und Geschäftsgeheimnissen der jeweils anderen Partner erlaubt ist, um die eingangs erläuterten Rechtswidrigkeitsrisiken bei deren Übermittlung und Empfang zu vermeiden. Mustervereinbarungen können, wie zuvor ausgeführt[567], an dieser Stelle gerade dem Mittelstand helfen, an I4.0 teilzunehmen.

7.2.3.10 Handlungsempfehlungen im Bereich des Exportkontrollrechts

Im Bereich des Exportkotrollrechts sind nicht unmittelbar Handlungen bspw. von gesetzgeberischer Seite erforderlich, da nur in Einzelfällen rechtliche Implementierungshindernisse aus dem Exportkontrollrecht resultieren dürften. Gleichwohl würde es sich anbieten, bspw. im Rahmen einer juristischen Arbeitsgruppe solche exportkontrollrechtlichen Beschränkungen dezidiert herauszuarbeiten, die gemeinhin im Rahmen von I4.0 maßgeblich werden können (z. B. bzgl. Verschlüsselungstechnologien) und deshalb möglicherweise als Hindernis für die Nutzung von I4.0 wirken. Insoweit sollte in Betracht gezogen werden, seitens des Gesetzgebers exportrechtliche Privilegierungen bezüglich solcher Technologien vorzusehen, die – wie gerade das Verschlüsselungsthema zeigt – für eine vertrauensvolle und niederschwellige Nutzung von I4.0 unabdingbar sind.

7.3 Kosten-Nutzen-Betrachtungen

Im Umfeld der Diskussionen über die IT-Sicherheit in der I4.0 darf auch die Frage nach den Kosten und den Aufwendungen für die angestrebten Maßnahmen nicht vernachlässigt werden. Allerdings ist die Materie zu komplex und die Anzahl der Akteure auf verschiedenen Ebenen zu hoch, um eine klassische Kosten-Nutzen-Analyse vornehmen zu können.

Bei einer Kosten-Nutzen-Analyse werden Kosten und Nutzen in, soweit erforderlich abgezinsten, Geldeinheiten gemessen und miteinander verglichen. Eine Abzinsung ist

567 Vgl. zuvor Ziff. 3.3.1.3.

dann notwendig, wenn Kosten und Nutzen, die in mehr als einer Zeitperiode anfallen, berücksichtigt werden sollen. Falls Kosten und Nutzen nicht sicher eintreten, werden deren Erwartungswerte ermittelt. Ein Projekt oder eine Investition ist dann vorteilhaft, wenn das Ergebnis der Analyse positiv ist. Bei gegebenem Budget sind jene Projekte umzusetzen, die das beste Gesamtergebnis, also die beste Rentabilität der eingesetzten Mittel, erbringen.

Die praktischen Erfahrungen der letzten Jahre haben gezeigt, dass es sehr problematisch ist, die tatsächliche Schadenshöhe bei Angriffen auf IT-Systeme zu beziffern, auch wenn es hierzu Beispiele gibt.[568] Da die potenzielle Schadenshöhe gleichzeitig den gegebenenfalls durch IT-Sicherheitsmaßnahmen realisierbaren Nutzen (nämlich die Vermeidung des Schadens) darstellt ist das Vornehmen einer zuverlässigen Bewertung auf monetärer Basis schwierig. Darüber hinaus entstehen im Zusammenhang mit Kosten-Nutzen-Betrachtungen häufig dann Probleme, wenn nicht am Markt gehandelte Güter (z. B. Menschenleben, Zeit) oder schwer zu quantifizierender qualitativer Nutzen (z. B. Image, Kundenzufriedenheit, Qualität, Mitarbeiterzufriedenheit) bewertet werden müssen. Eine Objektivierung des Nutzens in Form von nur scheinbar messbaren monetären Einheiten ist daher sehr anfällig für subjektive Interpretationen oder Manipulationen durch den Ersteller dieser Vergleichsrechnung. Aus diesen Gründen trägt das Instrument der Kosten-Nutzen-Analyse nur wenig zur Verbesserung der Nachvollziehbarkeit und somit der Transparenz bei der Auswahl von Projekten und der Durchführung von Investitionen im Bereich der IT-Sicherheit bei.

Geeigneter erscheinen daher die Instrumente der Risikoanalyse und des Risikomanagements und daraus folgend die Auswahl der geeigneten IT-Sicherheitsmaßnahmen. So kann auch der Tatsache Rechnung getragen werden, dass Art und Umfang der benötigten Sicherheitsmaßnahmen wesentlich von Faktoren, wie beispielsweise dem Abhängigkeitsgrad des Unternehmens von bestimmten Assets, von besonderen Verfügbarkeitsnotwendigkeiten oder von der Durchdringung mit IT, beeinflusst werden und die Schadenswahrscheinlichkeit nicht in jeder Konstellation gleich ist. Darüber hinaus ist Sicherheit auch immer eine Frage der Bereitschaft Risiken einzugehen und damit eine Frage des persönlichen Ermessens oder der Risikofreudigkeit der Verantwortlichen. Berücksichtigt werden müssen darüber hinaus auch gesetzliche und regulatorische Anforderungen.

Auch im Rahmen der Risikoanalyse ist es möglich und sinnvoll, die dem Risiko gegenüberstehenden Aufwendungen zu betrachten, um eine transparente Entscheidung für oder gegen eine aktive Prävention zu treffen. Im Kontext von IT-Sicherheitsprojekten spielen vor allem Personal- und Sachkosten eine wichtige Rolle. Im Hinblick auf Personalkosten sind etwa die Kosten für Personal in den Bereichen Wartung und Schulung zu berücksichtigen, aber auch jene für IT-Sicherheitsverantwortliche, die direkt mit der Planung und Umsetzung von Maßnahmen betraut sind. Bei den Sachkosten handelt es sich meist fast ausschließlich um Kosten für die Anschaffung und den Betrieb von Hard- und Software.

Eine additive Methode zur Risikoanalyse, die auch die Kostenseite abbilden kann, ist ROSI (Return on Security Investment). Angelehnt an die Berechnung des ROI (Return on Investment) aus dem klassisch-betriebswirtschaftlichen Bereich werden beim ROSI nicht nur die Kosten, die für eine IT-Sicherheitsmaßnahme selbst anfallen, betrachtet, sondern auch die Kosten der wahrscheinlichen Schäden sowie die Reduzierung der Kosten der wahrscheinlichen Schäden durch die Umsetzung der IT-Sicherheitsmaßnahme. Weitere auf die IT-Sicherheit zugeschnittene Methoden basieren auf Konzepten aus der Investitionsrechnung und Entscheidungstheorie (z. B. Kapitalwert, interner Zinsfuß, Analytischer Hierarchieprozess) bzw. auf der Balanced Scorecard sowie Konzepten wie Wert im Risiko (VaR)[569].

Auch wenn diese Methoden oder Kombinationen davon die eine oder andere Verbesserung im Hinblick auf die Betrachtung der Wirtschaftlichkeit von IT-Sicherheitsprojekten bringen, bleibt das zentrale Problem der Quantifizierung von Nutzen weitgehend ungelöst.

Ein pragmatischer Ansatz zur Umgehung der Schwierigkeiten könnte die Orientierung an Best-Practice-Ansätzen sein. Investitionen in IT-Sicherheit würden dann umgesetzt, wenn sie sich auch in anderen ähnlichen Kontexten bewährt haben. Es würde angenommen werden, dass sie sich unter anderem auch deshalb bewährt haben, weil sie sich im Vergleich zu Alternativen als wirtschaftlicher

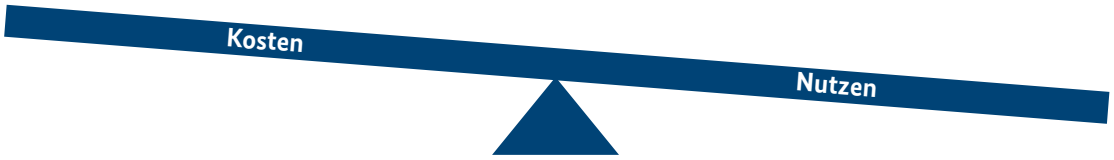
568 Sony 2011, vgl. Spiegel Online v. 03.06.2011 (abrufbar unter http://www.spiegel.de/netzwelt/web/erneuter-datenklau-hacker-lieben-sony-a-766391.html).

569 Demetz, L., Bachlechner, D. 2013. "To Invest or Not to Invest? Assessing the Economic Viability of a Policy and Security Configuration Management Tool," Economics of Information Security and Privacy. Berlin/Heidelberg: Springer, S. 25–47.

Abbildung 7–1: Kosten-Nutzen-Faktoren im Kontext von IT-Sicherheit

- Mechanische und elektronische Auf-/Umrüstung von Maschinen und Anlagen
- IT-Hardware
- Software-Anpassung (MES/PMS, Steuerungen, Kommunikation, Einbindung Dritter etc.)
- Software Neuinvestition (Kommunikation, Verschlüsselung etc.)
- Konnektivität
- Zusätzlicher Personalaufwand intern
- Personalkosten extern (DL)
- Know-how-Einkauf
- Qualifizierung Mitarbeiter
- Neueinstellungen
- Mitarbeit Gremien etc.
- Rechtsberatung/Vertragsgestaltung
- Risikoabschätzung
- Umstrukturierung
- Pilotprojekte
- Assistenzsysteme
- Umsetzung von Standards
- Versicherung neuer Risiken

- Flexibilisierung der Produktion
- Abfangen von Kapazitätsspitzen
- Konzentration auf Kernkompetenzen
- Auslastung von Maschinen
- Verringerung von menschl. Kommunikationsaufwand
- Verringerung körperl. Belastungen am Arbeitsplatz
- Schnelleres Lernen von Arbeitern
- Kundenbindung
- Transparente Informationsflüsse
- Frühzeitiges Entdecken von Angriffen
- Schäden vermeiden
- Erkennen von Anomalien
- Know-How-Verlust vermeiden
- Vertrauen in I4.0 aufbauen
- Menschl. Fehlverhalten vermeiden
- Auf Marktänderungen vorbereitet sein
- Gewinnung von Fachpersonal über Vorreiterstellung
- Bestehende Kooperationen stärken – gemeinsam wachsen
- Von schnellen IT-Innovationszyklen profitieren?
- Ggf. Möglichkeiten der Patentierung



Quelle: Fraunhofer ISI

erwiesen haben oder zumindest als wirtschaftlicher eingeschätzt wurden.

Zur Verbesserung der wirtschaftlichen Transparenz von IT-Sicherheitsmaßnahmen in Unternehmen erscheinen Maßnahmen in zwei Bereichen sinnvoll: Zum einen die Ergänzung der Risikoanalyse um eine Betrachtung der Aufwendungen, die über die reinen Investitionskosten für Hard- und Software hinausgehen und zum anderen der Weiterentwicklung der Methoden und Tools zur Nutzenbewertung, wie z. B. der Nutzwertanalyse für IT-Sicherheitsmaßnahmen, von Szenariotechniken oder von multikriteriellen Bewertungssystemen. Im Rahmen eines fokussierten Forschungs-programms sollte die Weiterentwicklung entsprechender Methoden vorangetrieben werden.

Wichtig ist, dass IT-Sicherheit und vor allem die Auswahl von konkreten Projekten und Investitionen aus der Sphäre des Nebulösen herausgelöst und vermehrt im Lichte betriebswirtschaftlicher Überlegungen diskutiert wird. Es muss dort Transparenz geschaffen werden, wo es möglich ist. Gleichzeitig müssen Unternehmen und Dienstleister aber der Versuchung widerstehen, nicht zurechenbare oder nicht quantifizierbare Faktoren um jeden Preis berechenbar machen zu wollen.

7.4 Handlungsvorschläge

Zusammen mit der abschließenden Bewertung von Standards und Normen komplettieren die in Kapitel 6 der Studie vorgestellten technischen, organisatorischen und rechtlichen Konzepte die notwendige Basis für die Entwicklung von den im Folgenden genannten Handlungsvorschlägen. Zusammen mit den in den Kapiteln 4 und 5 identifizierten Bedrohungen, Risiken und verfügbaren IT-Sicherheitskonzepten werden konkrete Handlungsvorschläge formuliert, welche der Politik bzw. dem Gesetzgeber und den Anwendern dabei helfen sollen, für konkrete Szenarien zu erkennen, an welchen Stellen Handlungsbedarf besteht und welche Maßnahmen möglich sind, um vorhandenen Risiken und Bedrohungen sowie rechtlichen und organisatorischen Hemmnissen zu begegnen.

Dieses Kapitel enthält eine strukturierte Liste mit allen in der Studie identifizierten konkreten Handlungsvorschlägen, die geeignet sind, die IT-Sicherheit in der Industrie 4.0 zu steigern. Als Zieladressatenkreis werden Entscheider in Unternehmen, in Wirtschafts- und Förderpolitik sowie in Standardisierungsorganisationen erachtet.

Die Handlungsvorschläge sind daher den primären Zieladressatenkreisen zugeordnet, auf konkretere Zielgruppen wird in den ausführlichen Handlungsvorschlägen hingewiesen.

Primäre Zielgruppen sind Entscheider in

- Unternehmen und Branchenverbänden,
- Politik/Gesetzgeber und Aufsichts- und Regulierungsbehörden (Wirtschafts- und Förderpolitik)
- sowie Standardisierungs- und Normierungsorganisationen.

Konkrete bzw. sekundäre Zielgruppen sind: KMU/Industrie als Anwender I4.0, IT-Sicherheitsindustrie (Anbieterseite Sicherheitstechnologie I4.0), Wissenschaft (Forschung/Entwicklung von Sicherheitstechnologie I4.0).

Eine Vielzahl von Handlungsvorschlägen muss kurzfristig im Zeitraum von wenigen Jahren angegangen werden. Hier sind sowohl die Wirtschafts- und Förderpolitik, Standardisierungsorganisationen als auch die Unternehmen selbst gefragt.

Die vorgeschlagenen Umsetzungszeithorizonte der Handlungsempfehlungen unterscheiden sich nach kurzfristig (ein bis zwei Jahre), mittelfristig (drei bis fünf Jahre) und langfristig (sechs bis zehn Jahre).

Es folgt eine strukturierte und nach Priorität sortierte Liste mit den in der Studie identifizierten 36 Handlungsvorschlägen hinsichtlich der IT-Sicherheit für die Industrie 4.0, jeweils für die zentralen Schwerpunkte Recht, Betrieblich/Organisatorisch, Technik und Standardisierung.

Handlungsvorschläge Recht:

Im Bereich Recht hat die Studie festgestellt, dass für die Praxis in erster Linie Rechtsunsicherheiten mit Blick auf konzeptionelle, insbesondere regulatorische und vertragsgestaltende Rahmenbedingungen bestehen. Aus diesem Grund identifizieren die Handlungsvorschläge für dieses Themenfeld, in welchen Bereichen und mit Bezug zu welchen konkreten Umständen entsprechende konzeptionelle rechtliche Lösungen benötigt werden (z. B. durch Gesetzesanpassung, Musterklauseln) und welche Akteure (Gesetzgeber, Aufsichtsbehörden, Branchenverbände) diese im Einzelnen ausgestalten können.

Tabelle 7–1: Priorisierte Handlungsvorschläge Recht

Handlungsvorschlag	Kategorie	Zieladressatenkreis	Zeitraum	Priorisierung
Einheitliche rechtliche Pflichten zur IT-Sicherheit und prüffähige Standards	Rechtssicherheit	Politik/Gesetzgeber (Gesetzgebung, Regulierungsbehörden, Verbände)	mittelfristig	1
Rechtssicherheit durch datenschutzrechtliche Rechtsgrundlagen für Datenströme bei I4.0	Rechtssicherheit	Bundesregierung durch entsprechende Gesetzesinitiativen	mittelfristig	2
Rechtlicher Rahmen für IT-Sicherheits-Zertifizierung	Rechtssicherheit	Politik/Gesetzgeber Gesetzgebung	mittelfristig	3
Ausbau behördlicher Kompetenzen und Kooperation im Bereich IT-Sicherheit	Rechtssicherheit	Politik/Gesetzgeber Bundesgesetzgeber, Bundesregierung, BSI, Datenschutzbehörden und Verbände	langfristig	4
Musterklauseln und Mustereinwilligungen für I4.0 hinsichtlich Haftung sowie Datenschutz und Betriebs- und Geschäftsgeheimnisse	Rechtsgestaltung	Erarbeitung durch Aufsichtsbehörden (Düsseldorfer Kreis, Artikel-29-Gruppe) und Branchenverbände	mittelfristig	5
Musterdatenschutzklauseln und -einwilligungen (abhängig von ersteren)	Rechtsgestaltung	Erarbeitung durch Aufsichtsbehörden (Düsseldorfer Kreis, Artikel-29-Gruppe) und Branchenverbände	mittelfristig (Datenschutz-Musterklauseln und -einwilligungen) langfristig (Zertifizierung, Siegel)	5

Tabelle 7–1: Priorisierte Handlungsvorschläge Recht (Fortsetzung)

Handlungsvorschlag	Kategorie	Zieladressatenkreis	Zeitraum	Priorisierung
Musterverträge zur Kooperation und Sicherheitsanforderungen	Rechtsgestaltung	Unternehmen (Betreiber von Produktionsanlagen und Dienstleister) und Branchenverbände	mittelfristig	5
Orientierungsrahmen für angemessene technisch-organisatorische Maßnahmen durch Datenschutzsiegel	Rechtssicherheit	Politik (Bundesregierung)	mittelfristig	6
Herausarbeitung von Hindernissen, die durch (internationales) Exportrecht bei I4.0 gemeinhin entstehen können	Ermittlung von Hindernissen	Analyse durch die Branchenverbände	langfristig	7
Forschung und Konzeption zum Rechtsrahmen für IT-Sicherheit	Rechtssicherheit	Politik (Bundesregierung und Verbände)	mittelfristig	8
Länderübergreifende einheitliche Schutzstandards in Bezug auf Geheimnisschutz	Rechtssicherheit	Initiative durch die europäische Kommission	langfristig (Evaluierung); kurzfristig (Mustervereinbarungen)	9
Muster-Non-Disclosure-Agreements	Rechtsgestaltung	Erarbeitung durch die Branchenverbände	kurzfristig	10

Handlungsvorschläge Betrieblich/Organisatorisch:

Tabelle 7–2: Priorisierte Handlungsvorschläge Betrieblich/Organisatorisch

Handlungsvorschlag	Kategorie	Zieladressatenkreis	Zeitraum	Priorisierung
Einigung auf sinnvolle Vorgaben im Hinblick auf Strukturen und Prozesse (Mindeststandards)	Technikintegration	Politik	kurzfristig	1
Förderung der Entwicklung von Bewertungs- und Entscheidungsunterstützungsmodellen	Technikintegration	Politik	langfristig	2
Top-down-Förderung von Vertrauen in das Konzept und die Vision	Vertrauen	Unternehmen	mittelfristig/ langfristig	3
Konzeption geeigneter Aus- und Weiterbildungsangebote	Faktor Mensch	Politik	mittelfristig	4
Hinterfragen etablierter Strukturen und Prozesse im Rahmen des Risikomanagements	Technikintegration	Unternehmen	kurzfristig	5
Orientierung an Erfahrungsberichten, Best-Practices und Handlungsleitfäden	Technikintegration	Unternehmen	kurzfristig	6
Umsetzung bewährter organisatorischer IT-Sicherheitsmaßnahmen	Technikintegration	Unternehmen	kurzfristig	7
Einsatz von Assistenzsystemen zur Entlastung von Mitarbeitern	Faktor Mensch	Unternehmen	mittelfristig	8
Einsatz von Promotoren zur Förderung von Änderungsprozessen	Faktor Mensch	Unternehmen	mittelfristig/ langfristig	9
Durchführung einer gezielten Personalentwickelung	Faktor Mensch	Unternehmen	mittelfristig/ langfristig	10
Durchführung von Pilotprojekten in einem etablierten Umfeld	Vertrauen	Unternehmen	kurzfristig	11
Bereitstellung einer Plattform zur Diskussion und Aufklärung mit Fokus auf KMU	Vertrauen	Politik	kurzfristig	12
Erforschung von Maßnahmen zur Vermeidung von menschlichem Fehlverhalten im Kontext von Angriffen	Faktor Mensch	Politik	langfristig	13

Handlungsvorschläge Technik:

Tabelle 7–3: Priorisierte Handlungsvorschläge Technik

Handlungsvorschlag	Kategorie	Zieladressatenkreis	Zeitraum	Priorisierung
Entwicklung integrierter Methodik für Safety & Security	Safety & Security	Unternehmen	kurzfristig	1
Verschlüsselung sensibler Daten	Industrial Rights Management	Unternehmen	kurzfristig	2
Integritätsprüfungen	Integritäts-prüfungen und hardware-basierte Sicherheitsanker	Unternehmen	kurzfristig	3
Verwendung hardware-basierter Sicherheitsanker	Integritäts-prüfungen und hardware-basierte Sicherheitsanker	Unternehmen	kurzfristig	4
Entwicklung von Komponenten mit Secure-Plug-&-Work-Fähigkeiten	Safety & Security	Unternehmen/KMU, insb. Forschung & Entwicklung	kurzfristig	5
Aufbau von Public-Key-Infrastruktur oder Single-Sign-On	Schlüsselverwaltung für digitale Verschlüsselung	Unternehmen/KMU, insb. Hersteller von Komponenten und Anlagen	mittelfristig	6
Entwicklung von Anomalie-Erkennungssystemen	Production Line IT-Security Monitoring	Unternehmen/KMU, insb. Hersteller und Betreiber von Produktionsanlagen und Komponenten, Forschung und Entwicklung	mittelfristig	7

Handlungsvorschläge Standardisierung:

Tabelle 7–4: Priorisierte Handlungsvorschläge Standardisierung

Handlungsvorschlag	Kategorie	Zieladressatenkreis	Zeitraum	Priorisierung
Erarbeitung integrierter Standards für Safety & Security	Safety & Security	Standardisierungsorganisationen	mittelfristig	1
Erarbeitung einer Struktur für IT-Sicherheitsstandards	Safety & Security	Standardisierungsorganisationen	mittelfristig	2
Integration technischer Standards mit ISMS-Standards	Safety & Security	Standardisierungsorganisationen	mittelfristig	3
Engineering von sicheren IT-Systemen	Safety & Security	Standardisierungsorganisationen	langfristig	4

7.4.1 Politik/Gesetzgeber und Aufsichts- und Regulierungsbehörden

Ausgehend von den vorliegenden Erkenntnissen werden nachfolgend entsprechende Handlungsvorschläge formuliert die sich primär an die Politik/den Gesetzgeber und somit vorrangig an die Förderpolitik, die Wirtschaftspolitik und Aufsichts- und Regulierungsbehörden richten.

7.4.1.1 Betrieblich-organisatorisch

Technikintegration

Die Vision von I4.0 erweist sich als stark technologiegetrieben. Technische Entwicklungen der letzten Jahre haben die heutige Vision von I4.0 überhaupt erst entstehen lassen. Noch gibt es aber weder Standards noch „die I4.0-Technologie“, so dass Unternehmen bisher weitestgehend alleine auf ihrem Weg zu einer vernetzten und automatisierten industriellen Produktion sind.

7.4.1.1.1 Einigung auf sinnvolle Vorgaben im Hinblick auf Strukturen und Prozesse (Mindeststandards)

Betrifft: Politik. Eine Einigung auf für Unternehmen aller Größen sinnvolle Vorgaben sollte von der Wirtschaftspolitik unterstützt werden. Die Einführung und Durchsetzung von Mindeststandards sollte aber in der Zuständigkeit der Unternehmen bleiben. Die Einbindung von Forschungseinrichtungen und Verbänden liegt nahe.

Feststellung: Neben technischen Standards ist Standardisierung auch im Zusammenhang mit organisatorischen Maßnahmen sinnvoll – vor allem auch im Kontext von organisatorischen IT-Sicherheitsmaßnahmen. Unternehmen müssen sich darauf verlassen können, dass nicht nur aus technischer Sicht von kooperierenden Unternehmen Mindeststandards eingehalten werden, sondern auch im Hinblick auf Strukturen und Prozesse.

Empfehlung: In Abstimmung mit der Industrie sollte die Entwicklung von I4.0-Mindeststandards durch entsprechende gesetzliche Rahmenbedingungen gefördert werden (Ziff. 7.1.1.1). Zu beachten ist bei der Festlegung der Mindeststandards, dass die Standards auch von KMU umsetzbar und mit verhältnismäßigem Aufwand überprüfbar sind. Darüber hinaus erscheint eine Abstimmung auf internationaler Ebene sinnvoll. Der Einsatz von Standardprodukten, wie auch die Umsetzung von standardisierten Strukturen und Prozessen, bietet ein höheres Maß an Sicherheit für strategische Entscheidungen.

Zielzustand: Unternehmen greifen auf bestehende Standards zurück und kehren ab von Insellösungen ab. Unternehmen sind mit Vorgehensweisen zur effektiven Etablierung und Durchsetzung von Mindeststandards vertraut.

Zeitraum: Kurzfristig. Bereits begonnene Standardisierungsprozesse sollten von den Unternehmen und von der Politik unterstützt werden. Darüber hinaus sind bestehende Standardisierungslücken zu schließen.

Rolle des Menschen

Während der Wandel hin zur I4.0 im Hinblick auf die Technikintegration als Evolution verstanden werden kann, kommt es im Hinblick auf die Rolle des Menschen tatsächlich zu etwas, was als Revolution bezeichnet werden könnte. Es kommt zu einem Aufbrechen von Routinen, zum Einbüßen von Privilegien oder Machtempfinden, zu Einschränkungen der erlebten Freiräume und damit zu Unsicherheiten.

7.4.1.1.2 Förderung der Entwicklung von Bewertungs- und Entscheidungsunterstützungsmodellen

Betrifft: Politik. Die Handlungsempfehlung richtet sich primär an die Wissenschaftspolitik. Forschungseinrichtungen und Unternehmen spielen aber im Hinblick auf die erfolgreiche Umsetzung der Empfehlung eine zentrale Rolle.

Feststellung: Entscheidungsunterstützung wird aufgrund der zunehmenden Komplexität und Dynamik im Zusammenhang mit vernetzter und automatisierter industrieller Produktion immer wichtiger. Die konkreten Faktoren, die bei Entscheidungen im Zusammenhang mit organisatorischen IT-Sicherheitsmaßnahmen herangezogen werden sollten, sind heute noch weitgehend unbekannt. Die zentrale Herausforderung besteht darin, dass bei organisatorischen Entscheidungen nicht nur die monetär direkt abbildbaren Faktoren, sondern auch die sogenannten „weichen“ Faktoren entscheidend sind.

Empfehlung: Im Rahmen eines fokussierten Forschungsprogramms sollte die Entwicklung von an die Anforderungen der I4.0 angepassten Bewertungs- und Entscheidungsunterstützungsmodellen vorangetrieben werden. Die Modelle sollen das Treffen von fundierten und rationalen Entscheidungen im Zusammenhang mit organisatorischen IT-Sicherheitsmaßnahmen erleichtern.

Zielzustand: Modelle und Tools zur Entscheidungsunterstützung existieren und können die komplexen Prozesse abbilden.

Zeitraum: Langfristig. Das Aufsetzen und insbesondere die Durchführung eines Forschungsprogramms können der Natur nach nicht kurz- oder mittelfristig erfolgen.

7.4.1.1.3 Konzeption geeigneter Aus- und Weiterbildungsangebote

Betrifft: Politik. Im Zusammenhang mit der Konzeption entsprechender Angebote ist die Unterstützung durch die Bildungspolitik gefragt. Die Anforderungen müssen von den Unternehmen definiert werden. Die Einbindung von Lehreinrichtungen und Verbänden ist unbedingt notwendig.

Feststellung: Der mit I4.0 einhergehende Wandel erfordert nicht nur immer mehr Interdisziplinarität und Arbeit in interprofessionellen Teams, sondern auch umfassendes fachliches und methodisches Wissen. Es mangelt an Aus- und Weiterbildungsangeboten, die die umfassenden Anfor-

derungen der I4.0, insbesondere auch im Hinblick auf IT-Sicherheit, abdecken. Zudem gibt es im Bereich der Industrie einen gravierenden Mangel an ausgebildeten Fachkräften im Bereich IT-Sicherheit. Ohne diese Fachkräfte in den größeren Unternehmen wird ein Know-How-Transfer nicht gelingen.

Empfehlung: In Abstimmung mit der Industrie sollten zunächst die Anforderungen an Mitarbeiter in der I4.0 erhoben und anschließend passende Aus- und Weiterbildungsangebote konzipiert werden. Dabei sollten sowohl die Anforderungen an Mitarbeiter, die mit dem Aufbau und der Betreuung der Produktionsumgebung betraut sind, als auch jene an Mitarbeiter die Anlagen bedienen oder überwachen berücksichtigt werden. Ziel ist u.a. eine Bewusstseinsschärfung auch für die IT-Sicherheitsrisiken.

Zielzustand: Es existiert ein Angebot an interdisziplinären Qualifizierungsmaßnahmen.

Zeitraum: Mittelfristig. Der Markt muss sich über die Nachfrage erst entwickeln. Lehreinrichtungen müssen gefunden werden, die Aus- und Weiterbildung anbieten können und wollen.

7.4.1.1.4 Erforschung von Maßnahmen zur Vermeidung von menschlichem Fehlverhalten im Kontext von Angriffen

Betrifft: Politik. Die Handlungsempfehlung richtet sich primär an die Wissenschaftspolitik. Geeignete Forschungseinrichtungen sind für die erfolgreiche Umsetzung der Empfehlung unerlässlich.

Feststellung: Wie in vielen anderen Bereichen auch scheitert IT-Sicherheit im Kontext der I4.0 häufig am Faktor Mensch. Angreifer nutzen heute nicht nur Systemschwachstellen aus, sie setzen ebenso auf menschliches Fehlverhalten. Besonders in KMU ist das Sicherheitsbewusstsein oft nicht ausreichend ausgeprägt.

Empfehlung: Im Rahmen eines Forschungsprogramms sollte der Faktor Mensch im Rahmen der IT-Sicherheit in der I4.0 gezielt untersucht werden. Dabei sollte der Fokus auf der Entwicklung von Maßnahmen zur Abwehr möglicher Angriffe, die menschliches Fehlverhalten ausnützen oder gezielt auf Social Engineering setzen, liegen.

Zielzustand: Die Rolle des Menschen innerhalb des Konzepts ist gefestigt, zusätzliche Sicherheitsrisiken gehen nicht von den Mitarbeitern aus.

Zeitraum: Langfristig, da ein für einen längeren Zeitraum laufendes Forschungsprogramm aufzusetzen und durchzuführen ist.

Vertrauen

Vertrauen hängt sehr eng mit der Überzeugung zusammen, dass ein angemessenes IT-Sicherheitsniveau gewährleistet werden kann. Für den Erfolg der I4.0 ist nicht nur Vertrauen in die Vision selbst eine zwingende Voraussetzung, sondern auch Vertrauen in die Technik und in mögliche Kooperationspartner.

7.4.1.1.5 Bereitstellung einer Kommunikationsplattform zur Diskussion und Aufklärung mit Fokus auf KMU

Betrifft: Politik. Für die Bereitstellung einer entsprechenden Plattform ist eine intensive Zusammenarbeit von Wirtschaftspolitik, Unternehmen und Verbänden notwendig.

Feststellung: Grundlegendes Vertrauen in das Konzept oder die Vision von Industrie 4.0 kann zu einem gewissen Grad durch eine breite Diskussion und Aufklärung erreicht werden. Eine frühzeitige Erörterung von Bedenken und die Klärung von offenen Fragen sind für den Erfolg der I4.0 unerlässlich. Die bestehende Plattform Industrie 4.0 enthält kaum Möglichkeiten für KMU für einen schnellen oder kurzfristigen Austausch. Das Engagement im Rahmen einer Arbeitsgruppe o.ä. ist für viele KMU jedoch zu zeitaufwändig. Da es oftmals um den Bedarf einer konkreten Problemlösung geht, ist die Nutzung der bestehenden Plattform Industrie 4.0 für KMU nicht zielführend.

Empfehlung: Die Politik sollte unter Einbeziehung von Vertretern der Industrie, der Wissenschaft und der Gesellschaft eine Kommunikationsplattform für die breite Diskussion der industriellen Produktion der Zukunft bereitstellen und damit zu einer umfassenden Aufklärung über Potenziale und Gefahren der I4.0 beitragen.

Zielzustand: Unternehmen können sich über eine gemeinsame Plattform austauschen oder Informationen einholen und erhalten gleichzeitig zielgerichtete Informationen zu neuen technischen, organisatorischen und rechtlichen Entwicklungen.

Zeitraum: Kurzfristig. Es besteht die Notwendigkeit, eine solche Plattform kurzfristig bereitzustellen, da gerade jetzt die Unsicherheit bei KMU am größten ist und daher ein großer Bedarf besteht, sich auszutauschen und von den Erfahrungen anderer zu profitieren.

7.4.1.2 Rechtlich

Im Folgenden werden die in dieser Studie offenkundig gewordenen Feststellungen und Empfehlungen (vgl. Kap. 7.2.3) mit den wesentlichsten Handlungsvorschlägen noch einmal verkürzt strukturiert dargestellt. Dies betrifft insbesondere Handlungsfelder zur Implementierung rechtlicher Rahmenbedingungen zur Zertifizierung von IT-Sicherheit, datenschutzrechtlicher Erlaubnisnormen, Vertragsmuster und sonstige Standardisierungsmöglichkeiten zur Schaffung von Rechtssicherheit und Gestaltungsunterstützung insbesondere für KMU.

Rechtliche Unsicherheiten

Das fehlende Vertrauen und die Angst vor möglichem Kontrollverlust werden nicht ausreichend von einem Rechtsrahmen zur IT-Sicherheits-Zertifizierung aufgefangen. Rechtliche Unsicherheiten bestehen insbesondere auch bei grenzüberschreitenden I4.0 Strukturen mit Blick auf den Geheimnisschutz (Schutz von Betriebs- und Geschäftsgeheimnissen, siehe Kapitel 4.4.6), das Exportrecht (siehe Kapitel 4.4.7) und mit Blick auf die datenschutzrechtliche Zulässigkeit der Übermittlung personenbezogener Daten. Dabei stellen sich den Unternehmen insbesondere Fragen der rechtssicheren Ausgestaltung von Verträgen mit Partnern und Dienstleistern in Bezug auf Datenschutz sowie Betriebs- und Geschäftsgeheimnissen. Hieraus resultiert etwa ein Bedürfnis an Mustern, Rechtsgrundlagen und Standards, die die Netzstrukturen von I4.0 hinreichend berücksichtigen.

7.4.1.2.1 Einheitliche rechtliche Pflichten zur IT-Sicherheit und prüffähige Standards

Betrifft: Politik/Gesetzgeber. Die Handlungsempfehlung richtet sich vor allem an die Gesetzgebung, Regulierungsbehörden und Verbände.

Feststellung: Das IT-Sicherheitsgesetz adressiert neben Anbietern von Telemediendiensten vor allem Betreiber von „kritische Infrastrukturen“ und erscheint insgesamt ausbaufähig. Zudem fehlt es derzeit an ausreichenden Entwicklungen an Standards für konkrete Themen und Bereiche der I4.0.

Empfehlung: Die Bundesregierung sollte evaluieren, ob das IT-Sicherheitsgesetz den tatsächlichen Bedürfnissen Rechnung trägt. Insbesondere sind weitere gesetzliche Maßnahmen zur IT-Sicherheit erforderlich, die auch auf I4.0 anwendbar sind.

Der Staat kann die Entwicklung von Standards fördern, wie dies etwa im Bereich der Standards für Datenschutz-Zertifizierung geschehen ist. Hier wurde im Rahmen des Trusted Cloud-Programms des BMWi ein prüffähiger Datenschutz-Standard für Cloud-Dienste, das Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP) erarbeitet. Das TCDP ist insoweit besonders interessant, als es gesetzliche Anforderungen – hier des BDSG – in prüffähige Anforderungen umsetzt und zugleich auf dem ISO/IEC 27018-Standard und dem ISO/IEC 27002-Standard aufsetzt, wodurch international anerkannte Standards genutzt werden.

Zielzustand: Gesetzliche Vorgaben für Teilbereiche der I4.0 durch IT-Sicherheitsgesetz II.

Zeitraum: Kurz- und mittelfristig. Das IT-Sicherheitsgesetz ist in Kraft getreten. Weitere legislative Maßnahmen sind jedoch nicht ausgeschlossen und werden bereits erwogen. Soweit kurzfristige gesetzliche Maßnahmen erfolgen, sind die Bedürfnisse von I4.0 zu berücksichtigen. Mittelfristig sollte auf der Grundlage des fachlichen Diskurses und der Erfahrung mit dem IT-Sicherheitsgesetz eine Fortentwicklung erfolgen („IT-Sicherheitsgesetz II“).

7.4.1.2.2 Rechtssicherheit durch datenschutzrechtliche Rechtsgrundlagen für Datenströme bei I4.0

Betrifft: Politik/Gesetzgeber. Die Handlungsempfehlung richtet sich vor allem an die Bundesregierung durch entsprechende Gesetzesinitiativen.

Feststellung: Die bisher gängigen datenschutzrechtlichen Erlaubnistatbestände sind zur Legitimation des Datenumgangs von und -austauschs zwischen den Partnern im Rahmen von Industrie 4.0 nur bedingt geeignet und unterliegen erheblichen Rechtsunsicherheiten. Neben Fragen nach allgemeinen Rechtsgrundlagen für die Datenverarbeitungen im Rahmen von Industrie 4.0 bestehen insbesondere Rechtsunsicherheiten bei der Übermittlung von Daten in unsichere Drittstaaten. Die von der EU-Kommission bisher entwickelten

Standardvertragsklauseln sind nicht auf die Besonderheiten der Industrie 4.0 zugeschnitten und sehen etwa keinen multilateralen Abschluss vor.

Empfehlung: Die Bundesregierung sollte sich bei den Verhandlungen zur Europäischen Datenschutzgrundverordnung für die Schaffung klarer und rechtssicherer Erlaubnistatbestände einsetzen, auf die sich Unternehmen auch bei Industrie 4.0 Anwendungen stützen können. Soweit dem nationalen Gesetzgeber Spielräume verbleiben sollten, etwa in Bezug auf das Beschäftigtendatenschutzrecht, sollte der deutsche Gesetzgeber verhältnismäßige Erlaubnistatbestände bei der Verarbeitung von Beschäftigtendaten bei Industrie 4.0 Anwendungen schaffen. Die Datenschutzaufsichtsbehörden sollten im Dialog mit Branchenverbänden Standardvertragsklauseln entwerfen, die die Strukturen und Bedürfnisse der einzelnen Industrie 4.0 Konstellationen flexibel berücksichtigen und den multilateralen Abschluss durch mehrere Unternehmen vorsehen. Entsprechende Standardvertragsklauseln dürften insbesondere für KMU eine Erleichterung darstellen. Dabei sollten auch Vertreter wichtiger Handelspartner, wie etwa die Federal Trade Commission der USA, in die Beratungen miteingebunden werden.

Zielzustand: Rechtssichere Datenverarbeitungen und -übermittlungen zwischen Unternehmen bei Industrie 4.0 Kooperationen, auch in Drittstaaten, aufgrund klarer gesetzlicher und vertraglicher Grundlagen.

Zeitraum: Mittelfristig. Die Bundesregierung kann sich im Rahmen der Verhandlungen über die EU-Datenschutzgrundverordnung für Erlaubnistatbestände einsetzen. Erst wenn der Inhalt der Datenschutzgrundverordnung hinsichtlich der Frage eines nationalen Spielraums feststeht, kann der deutsche Gesetzgeber ein Beschäftigtendatenschutzgesetz erörtern. In Anbetracht der Dauer von Gesetzgebungsverfahren erscheint eine Umsetzung nur mittelfristig möglich. Auch die Ausarbeitung von Standardvertragsklauseln erfordert zunächst einen Dialog zwischen Datenschutzaufsicht und Branchenverbänden. Auch hier muss ein Konsultationsverfahren erfolgen, das voraussichtlich nicht kurzfristig zum Abschluss gebracht werden kann.

7.4.1.2.3 Rechtlicher Rahmen für IT-Sicherheits-Zertifizierung

Betrifft: Politik/Gesetzgeber. Die Handlungsempfehlung richtet sich vor allem an die Gesetzgebung.

Feststellung: Derzeit fehlt es an rechtlichen Grundlagen der IT-Sicherheit und von Verhaltensanforderungen. Dabei könnten IT-Sicherheits-Zertifizierungen Abhilfe schaffen.

Empfehlung: Es sollte eine gesetzliche Regelung zur IT-Sicherheits-Zertifizierung geschaffen werden, die Voraussetzungen, Verfahren und rechtliche Bedeutung der Zertifizierung regelt. Anders als im Bereich des Datenschutzes kann der nationale Gesetzgeber hinsichtlich der Anforderungen an allgemeine IT-Sicherheitszertifizierungen selbst tätig werden.

Zielzustand: Gesetzlicher Rahmen für anerkannte und bindende IT-Zertifizierungen, auf die Unternehmen zurückgreifen können.

Zeitraum: Mittelfristig. Aufgrund der Dauer von Gesetzgebungsvorhaben, sind gesetzliche Rahmenbedingungen nicht kurzfristig umzusetzen. Eine mittelfristige Umsetzung erscheint jedoch denkbar.

7.4.1.2.4 Ausbau behördlicher Kompetenzen und Kooperationen im Bereich IT-Sicherheit

Betrifft: Politik. Die Handlungsempfehlung richtet sich vor allem an den Bundesgesetzgeber, Bundesregierung, BSI, Datenschutzbehörden und Verbände.

Feststellung: Das bisherige System behördlicher Aufsicht für IT-Sicherheit ist unvollständig. Es bestehen institutionelle Defizite, etwa das Fehlen von zuständigen Behörden und Aufgaben.

Empfehlung: Bei der Weiterentwicklung der behördlichen Aufsicht sollten die Möglichkeiten der Zusammenwirkung bestehender Aufsichtsbehörden ausgelöst werden. Eine Alleinzuständigkeit des BSI ist nicht sinnvoll. Vielmehr sollte eine Zusammenarbeit bei IT-Sicherheit und Datensicherheit im Sinne des Datenschutzes auch auf Ebene der Aufsichtsbehörden abgestimmt werden.

Zielzustand: Flächendeckende behördliche Aufsicht zur IT-Sicherheit und behördliche Abstimmungen bei IT-Sicherheit und Datensicherheit im Sinne des Datenschutzes zur Sicherung einheitlicher Anforderungen durch die Regulierungsbehörden.

Zeitraum: Langfristig. Aufgrund der Dauer von Gesetzgebungsvorhaben, ist mit einer kurzfristigen Umsetzung nicht zu rechnen. Auch der Ausbau der behördlichen Kooperation ist ein fortschreitender Prozess, der langfristig anzulegen ist.

7.4.1.2.5 Musterklauseln und Mustereinwilligungen für I4.0 hinsichtlich Haftung sowie Datenschutz und Betriebs- und Geschäftsgeheimnisse

Betrifft: Regulierungsbehörden. Die Handlungsempfehlung richtet sich vor allem an die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und den Düsseldorfer Kreis (informelle Beratungsgremien der deutschen Datenschutzaufsichtsbehörden), die Artikel-29-Gruppe[570] (Beratungsgremium der nationalen Datenschutzaufsichtsbehörden, des europäischen Datenschutzbeauftragten und der Europäischen Kommission) und Branchenverbände.

Feststellung: Derzeit fehlt es an Mustern, die KMU den Umgang mit datenschutzrechtlichen Anforderungen bei I4.0 Netzwerkstrukturen erleichtern. Zudem fehlen Muster, die KMU verwenden können um ihre Betriebs- und Geschäftsgeheimnisse gegenüber anderen Unternehmen bei Einbindung im Rahmen von Zusammenarbeiten bei I4.0 zu schützen.

Empfehlung: In Kooperation mit dem Düsseldorfer Kreis und der Artikel-29-Gruppe sollten Branchenverbände Musterklauseln und Mustereinwilligungen für datenschutzrechtliche Verarbeitungen und Nutzungen speziell für häufige oder branchenübliche I4.0 Netzwerkstrukturen entwerfen. Zudem sollten Branchenverbände in Kooperation mit Experten aus der Praxis Musterklauseln zum Schutz vor Betriebs- und Geschäftsgeheimnissen entwerfen, die den besonderen Konstellationen bei I4.0 Anwendungen Rechnung tragen. Die Entwicklung von Musterverträgen oder -klauseln zur IT-Sicherheit verspricht nicht zuletzt im Hinblick auf die Internationalität der Informationstechnologie und der IT-Dienste große Chancen, wenn es gelingt, gemeinsame Positionen der Wirtschaft in diesem Aspekt zu entwickeln.

Zielzustand: Verfügbare Mustereinwilligungen und Musterklauseln, auf die Unternehmen, insbesondere KMU, hinsichtlich des Datenschutzes und zur Sicherung von Betriebs- und Geschäftsgeheimnissen zurückgreifen können.

Zeitraum: Mittelfristig. Eine Ausarbeitung von Mustern für KMU ist lediglich mittelfristig zu erwarten, da dies einen Abstimmungsprozess zwischen Datenschutzaufsicht und Branchenverbänden erfordert. Sind diese ausgearbeitet, können KMU jedoch zeitnah darauf zurückgreifen.

7.4.1.2.6 Orientierungsrahmen für angemessene technisch-organisatorische Maßnahmen durch Datenschutzsiegel

Betrifft: Politik. Die Handlungsempfehlung richtet sich vor allem an die Bundesregierung.

Feststellung: In der Praxis herrscht Unklarheit, ob die von den verantwortlichen Stellen implementierten technischen und organisatorischen Maßnahmen als angemessen zu qualifizieren sind, da es an einem ausreichenden Orientierungsrahmen für Anwendungen der I4.0 derzeit fehlt.

Empfehlung: Schaffung eines klaren Orientierungsrahmens für die wirtschaftliche Implementierung von hinreichenden technischen und organisatorischen Maßnahmen, z. B. durch das in dem Entwurf der Datenschutzgrundverordnung vorgesehene Datenschutzsiegel.

Zielzustand: Gesetzliche Regelung eines Datenschutzsiegels als Orientierung für angemessene technische und organisatorische Maßnahmen.

Zeitraum: Mittelfristig. Der Entwurf der EU-Datenschutzgrundverordnung sieht bereits jetzt die Einführung eines EU-Rechtsrahmen zur Vergabe von Datenschutzsiegeln vor. Die Bundesregierung kann sich daher bereits im Rahmen der laufenden Verhandlungen im europäischen Gesetzge-

570 Vgl. Artikel 29 und 30 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.
Siehe auch http://ec.europa.eu/justice/data-protection/article-29/index_de.htm

bungsverfahren für diese Regelung einsetzen. Nach Ablauf der Umsetzungsfristen für die EU-Datenschutzgrundverordnung können Datenschutzsiegel dann zur Orientierung und Vereinheitlichung technisch-organisatorischer Maßnahmen beitragen.

7.4.1.2.7 Herausarbeitung von Hindernissen die durch (internationales) Exportrecht bei Industrie 4.0 gemeinhin entstehen können

Betrifft: Politik. Die Handlungsempfehlung richtet sich vor allem an die Bundesregierung.

Feststellung: Da die Entwicklung der Industrie 4.0 sich in der Praxis noch nicht hinreichend konturiert hat, lässt sich zurzeit nicht abschließend feststellen, welche Hindernisse durch das (internationale) Exportrecht entstehen könnten.

Empfehlung: Die Bundesregierung sollte eine Arbeitsgruppe einrichten, die unter Beobachtung der weiteren Entwicklung der Industrie 4.0 dezidiert herausarbeitet, welche Industrie 4.0 Anwendungen in der Praxis gemeinhin Hindernissen durch (internationales) Exportrecht ausgesetzt sind.

Zielzustand: Umfassende Erfassung von Hindernissen durch (internationales) Exportrecht, die durch sich weiterentwickelnde Industrie 4.0 Anwendungen entstehen könnten.

Zeitraum: Langfristig. Die Arbeitsgruppe bedarf einer langfristig angelegten Beobachtung der Entwicklung der Industrie 4.0, bevor etwaige Feststellungen abschließend getroffen werden können.

7.4.1.2.8 Forschung und Konzeption zum Rechtsrahmen für IT-Sicherheit

Betrifft: Politik. Die Handlungsempfehlung richtet sich vor allem an die Bundesregierung, aber auch Verbände.

Feststellung: Diese Studie hat gezeigt, dass die Regulierung von IT-Sicherheit generell noch am Anfang steht. Die Gefährdungen der vernetzten Entwicklung und Produktion im Hinblick auf I4.0 ist noch nicht ausreichend erforscht.

Empfehlung: Notwendig erscheint die Einrichtung und Förderung eines Forschungsprogramms, um die dringend benötigte interdisziplinäre Forschung zu den Chancen und Anforderungen an IT-Sicherheits-Regulierung, insbesondere im Hinblick auf die Bedürfnisse der I4.0, in kurzer Zeit zu etablieren.

Zielzustand: Umfassende Erforschung der sich weiterentwickelnden I4.0-Anwendungen.

Zeitraum: Mittelfristig. Forschungsergebnisse sind kurzfristig nicht zu erreichen. Mittelfristig erscheinen jedoch erste konkrete Ergebnisse denkbar.

7.4.1.2.9 Länderübergreifende einheitlichen Schutzstandards in Bezug auf Geheimnisschutz

Betrifft: Politik. Die Handlungsempfehlung richtet sich vor allem an die Europäische Kommission, die Bundesregierung, aber auch an Branchenverbände.

Feststellung: Eine umfassende Regulierung des Geheimnisschutzes (Schutz von Betriebs- und Geschäftsgeheimnissen) existiert noch nicht. Mit der neuen Geheimnisschutzverordnung[571] ist jedoch bereits ein Anfang geschaffen. Non-Disclosure-Agreements (NDA) sind bei KMU noch nicht ausreichend verbreitet, können den Schutz jedoch verbessern.

Empfehlung: Die Geheimnisschutzverordnung sollte regelmäßig evaluiert werden, um zu prüfen, ob sich in der Praxis Bedürfnisse zeigen, die durch die vorgesehene Regulierung noch nicht abgedeckt sind. Unabhängig davon sollten Branchenverbände Muster-Non-Disclosure-Agreements schaffen, auf die insbesondere KMU zurückgreifen könnten.

Zielzustand: Umfassende gesetzliche Reglung zum Geheimnisschutz und Musterklauseln für Non-Disclosure-Agreements für Industrie 4.0.

Zeitraum: Langfristig. Aufgrund der bereits jetzt bestehenden gesetzgeberischen Aktivitäten, erscheint eine langfristige Beobachtung zur Evaluierung der Regelungen zweckmäßig (Evaluierung).

571 Vorschlag für eine RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung /* COM/2013/0813 final – 2013/0402 (COD) */.

Kurzfristig. Unabhängig vom gesetzlichen Geheimnisschutz können NDAs zeitnah vertraglichen Schutz herstellen. Die Ausarbeitung für spezifische Industrie 4.0 Anwendungen sollte durch die betroffenen Branchenverbände kurzfristig möglich sein und vermag den KMU eine Hilfestellung zu geben, die etwaige gesetzliche Defizite bereits jetzt ausgleichen könnte (Mustervereinbarungen).

7.4.2 Unternehmen und Branchenverbände

Ausgehend von den vorliegenden Erkenntnissen werden nachfolgend entsprechende Handlungsvorschläge formuliert die sich primär an Unternehmen richten und primär Industrieunternehmen/KMU als Anwender von I4.0 betreffen.

7.4.2.1 Betrieblich-organisatorisch

Im Folgenden werden betrieblich-organisatorische Handlungsvorschläge für Unternehmen mit Fokus auf KMU formuliert. Wie in Kapitel 7.5.1.2 wird auch im Folgenden eine Zuordnung von Empfehlungen zu den Kategorien Technikintegration, Rolle des Menschen und Vertrauen in die Technik, Kooperationspartner und das Potenzial der Vision von Industrie 4.0 vorgenommen.

Auch im Hinblick auf Unternehmen gilt, dass die Umsetzung aller Handlungsvorschläge sofort angegangen werden sollte.

Technikintegration

Wie bereits erwähnt, stehen Unternehmen bisher weitestgehend alleine auf ihrem Weg zu einer vernetzten und automatisierten industriellen Produktion da und agieren demensprechend zögerlich. Mangelnde Erfahrung und fehlende Vorhersehbarkeit von Entwicklungen hat häufig Ad-hoc-Maßnahmen und Improvisation zur Folge, wie im Fallbeispiel Automobilbau (siehe Kapitel 4.1.1) beschrieben. Dies macht die Entwicklung und Einhaltung von Richtlinien und Verfahren, die zur Gewährleistung der IT-Sicherheit notwendig sind, schwierig. Prozesse auf Basis von Versuch und Irrtum lassen sich nur schwer mit der Gewährleistung eines bestimmten IT-Sicherheitsniveaus vereinbaren.

7.4.2.1.1 Orientierung an Erfahrungsberichten, Best-Practices und Handlungsleitfäden

Betrifft: Unternehmen. Die Handlungsempfehlung richtet sich vor allem an Betreiber von Produktionsanlagen und Dienstleister mit Fokus auf die I4.0. Der Austausch von Erfahrungen zwischen Unternehmen kann allerdings auch von der Politik durch geeignete Maßnahmen gefördert werden.

Feststellung: Während einige Unternehmen oder Industriezweige bereits auf eine lange Erfahrung mit einer überdurchschnittlich stark vernetzten und automatisierten industriellen Produktion zurückblicken können, stehen andere noch am Anfang. Von einem intensiven Erfahrungsaustausch, vor allem im Bereich der IT-Sicherheit, würden alle Beteiligten profitieren, da die Wahrscheinlichkeit von Zwischenfällen reduziert und das Vertrauen in die Industrie insgesamt gesteigert werden würde.

Empfehlung: Bewährte Mittel um Erfahrungen von einem Unternehmen an ein anderes weiterzugeben sind beispielsweise Erfahrungsberichte (Success-Stories), Best-Practices und Handlungsleitfäden. Im Hinblick auf IT-Sicherheit können diese Mittel Hilfestellungen zu Richtlinien und Verfahren, Methoden und Werkzeugen sowie zu Schulungen und Sensibilisierungsmaßnahmen geben. Unternehmen können mithilfe von Erfahrungsberichten, Best-Practice-Sammlungen und Handlungsleitfäden in ihrer schrittweisen aber kontinuierlichen Annäherung an das Konzept I4.0 bestärkt werden und von Entwicklungen in anderen Unternehmen oder Industriezweigen profitieren.

Zielzustand: Best-Practice-Sammlungen und Handlungsempfehlungen unterstützen Unternehmen bei ihren Entscheidungen.

Zeitraum: Kurzfristig, um die derzeitige Unsicherheit der Unternehmen abzuschwächen.

7.4.2.1.2 Hinterfragen etablierter Strukturen und Prozesse im Rahmen des Risikomanagements

Betrifft: Unternehmen. Die Handlungsempfehlung richtet sich vor allem an Betreiber von Produktionsanlagen und Dienstleister mit Fokus auf die I4.0.

Feststellung: Bei der zunehmenden Vernetzung und Automatisierung der industriellen Produktion kommt das Bewusstsein für die sich durch Technikintegration verän-

dernde Bedrohungslage leicht zu kurz. Einerseits werden etablierte Praktiken nur selten auf ihre Angemessenheit hin überprüft und andererseits werden neue technische Entwicklungen ohne eingehende Prüfung des Nutzen-Risiko-Verhältnisses in bestehende Prozesse integriert.

Empfehlung: Die Bedeutung der integrierten Abschätzung von technischen, rechtlichen und organisatorischen Folgen der Integration neuer Techniken in bestehende Prozesse kann von Unternehmen nicht hoch genug eingeschätzt werden. Einerseits müssen in der industriellen Produktion etablierte Praktiken auf ihre Eignung für die I4.0 und andererseits neue technische Entwicklungen auf ihr Nutzen-Risiko-Verhältnis hin überprüft werden. Es muss klar sein, dass die I4.0 nicht nur mit Vorteilen verbunden sein kann, sondern an einigen Stellen auch Nachteile in Kauf genommen werden müssen.

Zielzustand: Die sich durch den Wandel hin zu Wertschöpfungsnetzwerken im Rahmen von I4.0 verändernde Bedrohungslage wird anerkannt.

Zeitraum: Kurzfristig. Eine Sensibilisierung der Unternehmen und der einzelnen Mitarbeiter muss kurzfristig realisiert werden, da das Potenzial für Angriffe bereits besteht und die Angreifer auch nicht abwarten. Der Prozess zur Analyse und Anpassung gefährdeter Strukturen und Datenflüsse muss unverzüglich angestoßen werden (s. Kap. 6.2.1).

7.4.2.1.3 Umsetzung bewährter organisatorischer IT-Sicherheitsmaßnahmen

Betrifft: Unternehmen. Die Handlungsempfehlung richtet sich vor allem an Betreiber von Produktionsanlagen und Dienstleister mit Fokus auf die I4.0.

Feststellung: Die Grundprinzipien der IT-Sicherheit aus organisatorischer Sicht haben auch in der industriellen Produktion der Zukunft ihre Gültigkeit. Aufgrund der zunehmenden Komplexität und Dynamik im Kontext von I4.0 nimmt die Bedeutung einer umfassenden Planung und transparenten Umsetzung von organisatorischen IT-Sicherheitsmaßnahmen allerdings zu.

Empfehlung: Solange noch keine I4.0-spezifischen Best-Practice-Sammlungen, Leitfäden und Standards existieren, die Fragen der IT-Sicherheit umfassend behandeln, sollten sich Unternehmen bei der Planung und Umsetzung organisatorischer IT-Sicherheitsmaßnahmen an vorhandenen, teils auf die industrielle Produktion spezialisierten Leitfäden und Standards für die IT-Sicherheit orientieren. Zusätzlich ist vor allem im Hinblick auf Richtlinien und Verfahren das Ergreifen von Maßnahmen ratsam, die die Einhaltung derselben sicherstellen.

Zielzustand: Unternehmen warten die kommenden Entwicklungen nicht mehr ab, sondern nutzen die existierenden und bekannten Standards. Anpassungen daran erfolgen iterativ und kontinuierlich.

Zeitraum: Kurzfristig, da die Sicherheitslücken z.T. bereits jetzt bestehen.

Rolle des Menschen

Die digitale Integration und Echtzeitsteuerung von Produktionsprozessen durch dezentrale Rechnereinheiten ermöglicht es zum einen, zukünftig auch mit An- und Ungelernten komplexere Tätigkeiten in der Produktion auszuführen (z.B. durch „geführte“ Arbeit mithilfe von Motion-Capture-Anzügen und Datenbrillen). Zum anderen wird der Bedarf an hoch qualifizierten Beschäftigten vor allem im IT-Bereich steigen, um das digitale Produktionssystem zu steuern, überwachen und anzupassen. Allerdings beruht ein Großteil der Innovationsstärke und Wettbewerbsfähigkeit deutscher Unternehmen auf der herausragenden Beherrschung technischer Herstellungsverfahren und Produktionsprozesse (z. B. Qualität, Flexibilität, Liefertreue) – siehe Kapitel 6.2.2. Daher ist es dringend erforderlich, eine gezielte Personalentwicklung zu betreiben, so dass spezifische Kompetenzen und Erfahrungen auch im Rahmen von I4.0-Produktionssystemen zukünftig weiter genutzt und strategisch weiterentwickelt werden können.

7.4.2.1.4 Einsatz von Promotoren zur Förderung von Änderungsprozessen

Betrifft: Unternehmen. Die Handlungsempfehlung richtet sich vor allem an Betreiber von Produktionsanlagen.

Feststellung: Es ist verständlich, wenn Menschen mit Unbehagen auf Veränderungen reagieren, weil diese mit dem Aufbrechen vertrauter Routinen und dadurch mit Unsicherheiten verbunden sind. Im Hinblick auf die IT-Sicherheit kann dieses Unbehagen zu menschlichem Fehlverhalten, vor allem bei der Umsetzung von Richtlinien und Verfahren, führen – in Extremfällen ist sogar denkbar, dass sich Mitarbeiter gegen das eigene Unternehmen wenden.

Empfehlung: Unternehmen sollten die Neuausrichtung als Chance sehen und den Mitarbeitern auch so vermitteln. In der Praxis hat sich dazu in anderen Bereichen der Einsatz von Promotoren bewährt, die den Änderungsprozess aktiv und intensiv fördern. Auch ein Einsatz von Projektteams und gegebenenfalls einer Pilotumgebung bieten sich zur Überwindung möglicher Hemmnisse an.

Zielzustand: Schaffung einer Innovationskultur in Unternehmen.

Zeitraum: Mittelfristig/langfristig. Die Schaffung und Förderung einer Innovationskultur im Unternehmen ist ein langfristiger Prozess, der jedoch so schnell wie möglich eingeleitet und dann weiterentwickelt werden muss. Der Zielzustand kann jedoch erst langfristig erreicht werden.

7.4.2.1.5 Durchführung einer gezielten Personalentwicklung

Betrifft: Unternehmen. Die Handlungsempfehlung richtet sich vor allem an Betreiber von Produktionsanlagen.

Feststellung: Der mit I4.0 einhergehende Wandel erfordert immer mehr Interdisziplinarität sowie die Arbeit in interprofessionellen Teams. Doch auch die zunehmenden Qualifizierungsbedarfe auf der fachlichen und methodischen Ebene dürfen nicht außer Acht gelassen werden.

Empfehlung: Im Hinblick auf Schulungen sollten sich Unternehmen an multidisziplinären Maßnahmen auf Verbandsebene beteiligen. Diese könnten eine gute Möglichkeit bieten, auch über Unternehmensgrenzen hinweg zu lernen – was vor allem für KMU hilfreich wäre. In solchen Schulungen sollte auch ein Bewusstsein für das notwendige Zusammenwirken von Recht, Organisation und Technik zur Gewährleistung eines angemessenen IT-Sicherheitsniveaus im Kontext von I4.0 vermittelt werden.

Zielzustand: Es existieren multidisziplinäre Qualifizierungsangebote am Markt.

Zeitraum: Mittelfristig. Unternehmen müssen zunächst die Bedarfe definieren und können dann gezielt Qualifizierungsmaßnahmen planen.

7.4.2.1.6 Einsatz von Assistenzsystemen zur Entlastung von Mitarbeitern

Betrifft: Unternehmen. Die Handlungsempfehlung richtet sich vor allem an Betreiber von Produktionsanlagen.

Feststellung: Der Wandel hin zu einer industriellen Produktion der Zukunft reduziert die monotonen Tätigkeiten für Mitarbeiter und erhöht damit die Anforderungen. Gleichzeitig steigt die Komplexität und Dynamik der Produktion im Allgemeinen.

Empfehlung: Vor allem angesichts der Komplexität und Dynamik der Produktion sind geeignete Assistenzsysteme für Unternehmen empfehlenswert. Entsprechende Systeme können vor allem auch im Kontext der Umsetzung von organisatorischen IT-Sicherheitsmaßnahmen hilfreich sein. Gezielte Auswertungen von Ereignissen und kontinuierliche Verbesserungen führen im Idealfall zu lernenden Systemen, die im Zeitverlauf immer besser darin werden, den Menschen zu unterstützen.

Zielzustand: Existenz von Assistenzsystemen zur Entlastung von Mitarbeitern.

Zeitraum: Mittelfristig. Assistenzsysteme können erst entwickelt werden, wenn die Prozesse ausgestaltet und umgesetzt sind.

Vertrauen

Im Hinblick auf das Vertrauen in die I4.0 besteht vor allem bei KMU die Angst vor einem möglichen Kontrollverlust durch die zunehmende Vernetzung und Automatisierung der Produktion.

Beispiel: Der Teilezulieferer befürchtet z. B. als Lieferant ersetzbar zu werden, sobald er seine Baupläne und Fertigungskapazitäten offen legt. Zudem steht die Befürchtung im Raum, über die Informationsebene zusätzlich angreifbar im Rahmen der Industriespionage zu sein.

7.4.2.1.7 Top-down-Förderung von Vertrauen in das Konzept und die Vision

Betrifft: Unternehmen. Die Handlungsempfehlung richtet sich vor allem an Betreiber von Produktionsanlagen.

Feststellung: Unternehmen fällt es mitunter schwer, grundlegendes Vertrauen in das Konzept oder die Vision von I4.0 zu schaffen. Wie eine Veränderung wie der Wandel hin zur industriellen Produktion der Zukunft in einem Unternehmen wahrgenommen wird, hängt unter anderem von der Geschwindigkeit der Veränderung und der Nachvollziehbarkeit der Maßnahmen ab. Im Hinblick auf die I4.0 ist wichtig, dass Möglichkeiten zum Aufbau von Systemvertrauen gefunden werden.

Empfehlung: Ein Ansatz Vertrauen zu schaffen, besteht darin, den Wandel als zentrales Innovationsthema im Unternehmen zu verstehen und auch so zu kommunizieren. Unternehmen sollten das Thema top-down vorantreiben. Positive Erfahrungsberichte aus anderen Unternehmen und Industriezweigen können den Prozess der Vertrauensbildung unterstützen. Eine schrittweise Einführung innerhalb des Unternehmens macht die Entwicklung besser nachvollziehbar und hilft, Hemmnisse und Widerstände abzubauen. Der Prozess kann durch den Aufbau von Systemvertrauen, zum Beispiel durch den Einsatz von zertifizierten Produkten und Prozessen, zusätzlich unterstützt werden.

Zielzustand: Bestehen einer Innovationskultur in Unternehmen.

Zeitraum: Mittelfristig/langfristig, da es sich um ein übergreifendes Thema handelt.

7.4.2.1.8 Durchführung von Pilotprojekten in einem etablierten Umfeld

Betrifft: Unternehmen. Die Handlungsempfehlung richtet sich vor allem an Betreiber von Produktionsanlagen. Die Durchführung von Pilotprojekten kann allerdings auch von der Politik durch geeignete Maßnahmen gefördert werden.

Feststellung: Häufig fehlt es Unternehmen an einem geeigneten Umfeld, um erste Erfahrungen mit neuen technischen Entwicklungen zu sammeln. Vor allem KMU sind auf unbekanntem Terrain sehr zögerlich, da der betriebliche Alltag kaum Raum für Versuch und Irrtum lässt.

Empfehlung: Unternehmen sollten gezielt bestehende Kooperationen nutzen, um I4.0-Pilotprojekte in einem etablierten Umfeld zu testen und um die Kooperationen zu vertiefen. Der betriebliche Alltag, der nicht selten durch hohen Erfolgsdruck geprägt ist, lässt Unternehmen zu wenig Raum, um sich mit rechtlichen und organisatorischen Fragestellungen im Zusammenhang mit neuen technischen Entwicklungen auseinanderzusetzen.

Zielzustand: Unternehmen wagen die Vernetzung mit anderen Unternehmen, da sie die Vorteile auf bekanntem Terrain evaluieren konnten.

Zeitraum: Kurzfristig, da es das Ziel sein muss, so schnell wie möglich Erfahrungen zu sammeln.

7.4.2.2 Rechtlich

Im Folgenden werden die rechtlichen Handlungsvorschläge dargestellt, auf die KMU zurückgreifen sollten. Einige dieser Handlungsvorschläge können von KMU bereits umgesetzt werden, andere sollten umgesetzt werden, sobald entsprechende Muster durch Branchenverbände unter Beteiligung der Aufsichtsbehörden entwickelt worden sind.

Rechtsgestaltung

Aufgrund unbestimmter oder nicht einschlägiger gesetzlicher Erlaubnisnormen stellen sich den Unternehmen Hindernisse bei der Erhebung und Weitergabe von personenbezogenen Daten in I4.0 Strukturen. Weder die derzeitige Gesetzeslage noch die geplante Datenschutzgrundverordnung in ihrer bislang erörterten Form schaffen in diesem Umfeld ausreichende Rechtsklarheit, so dass Unternehmen mit nicht unerheblichen Rechtswidrigkeitsrisiken konfrontiert sind.

Beispiel: Kundendaten. Entscheidet sich der Käufer eines PKW für eine Individuallackierung muss die individuelle Farbcodierung zwischen den beteiligten Rechnern und intelligenten Lackierrobotern im Industrie-4.0-Umfeld des Automobilherstellers ausgetauscht werden. Eine Anonymisierung wird nur schwerlich zu erreichen sein, denn damit das Fahrzeug mit dem individuellen Farbcode mit dem Abschluss der Lackierung dem richtigen Kunden zugeordnet werden kann, müssen Farbcode und Kunde mit einem Zuordnungsmerkmal verknüpft werden. Besonders kritisch wird es, wenn diese Daten grenzüberschreitend an einen Standort oder Kooperationspartner außerhalb des Europäischen Wirtschaftsraumes übermittelt werden müssen.

Die Rechtsunsicherheiten können durch eigene rechtsgestaltende Instrumente wie Einwilligungen der Personen, auf die sich die Daten beziehen, und vertragliche Regelungen mit den Kooperationspartnern reduziert werden. Gerade KMU sind dabei jedoch auf entsprechende Vorlagen und Muster angewiesen, die auf die typische Ausgestaltung für I4.0-Strukturen zugeschnitten sein müssen. Diese können nur durch Branchenverbände in Abstimmung mit den Regulierungsbehörden ausgearbeitet werden.

Auch in Bezug auf den Schutz von Betriebs- und Geschäftsgeheimnissen können Rechtsunsicherheiten bei der Vertragsgestaltung durch entsprechende Muster von Verbänden reduziert werden.

7.4.2.2.1 Musterverträge zur Kooperation und Sicherheitsanforderungen

Betrifft: Unternehmen. Der Handlungsvorschlag richtet sich vor allem an Betreiber von Produktionsanlagen und Dienstleister mit Fokus auf die I4.0. Erarbeitung durch Branchenverbände.

Feststellung: Musterverträge oder -klauseln zur Kooperation in der I4.0 sind bisher kaum verbreitet. Dies hat zur Folge, dass keine einheitlichen Anforderungen an sicherheitsbezogene Pflichten der Beteiligten und technische Anforderungen bestehen.

Empfehlung: KMU sollten – soweit möglich – auf Musterklauseln und -verträge zurückgreifen. Diese sollten durch Verbände, etwa durch Branchenverbände, erarbeitet werden. Ideal wäre es, einen Grundbestand einheitlicher Regeln zu schaffen, der für alle Branchen gilt, und diese durch branchenspezifische Besonderheiten zu ergänzen.

Zielzustand: In der Praxis werden von KMU Musterklauseln und-verträge verwendet, die – soweit sachlich angemessen – einheitliche Anforderungen an IT-Sicherheit stellen und branchenspezifische Besonderheiten enthalten, die von Gerichten als Konkretisierung des gesetzlichen Sorgfaltsmaßstabs anerkannt werden.

Zeitraum: Mittelfristig. Eine Ausarbeitung von Mustern für KMU ist lediglich mittelfristig zu erwarten, da dies einen Abstimmungsprozess erfordert und divergierende Interessen zu berücksichtigen sind. Sind diese ausgearbeitet, können KMU jedoch zeitnah darauf zurückgreifen.

7.4.2.2.2 Musterdatenschutzklauseln und -einwilligungen

Betrifft: Unternehmen. Die Handlungsempfehlung richtet sich vor allem an Betreiber von Produktionsanlagen und Dienstleister mit Fokus auf die I4.0.

Feststellung: Datenschutzbezogene Musterklauseln und -einwilligungen finden kaum Anwendung, was jedoch auch darin begründet liegt, dass derzeit keine auf Industrie 4.0 zugeschnittenen Muster existieren.

Empfehlung: KMU sollten – soweit möglich – auf Musterklauseln und -einwilligungen zurückgreifen. Insbesondere im Bereich des Datenschutzes müssten diese jedoch von Branchenverbänden in Kooperation mit den Datenschutzaufsichtsbehörden zunächst entwickelt werden. Auch sollten KMU von Zertifizierungen und Datenschutzsiegel Gebrauch machen, sobald die rechtlichen Grundlagen durch die Politik geschaffen worden sind.[572]

Zielzustand: In der Praxis werden von KMU Musterklauseln und-einwilligungen verwendet, die auch im Streitfalle von Aufsichtsbehörden anerkannt werden.

Zeitraum: Mittelfristig. Eine Ausarbeitung von Mustern für KMU ist lediglich mittelfristig zu erwarten, da dies einen Abstimmungsprozess zwischen Datenschutzaufsicht und Branchenverbänden erfordert. Sind diese ausgearbeitet, können KMU jedoch zeitnah darauf zurückgreifen (Datenschutz-Musterklauseln und -einwilligungen).

Langfristig. Die rechtlichen Rahmenbedingungen für Zertifizierungen und Siegel erfordern aufgrund der Dauer von Gesetzgebungsprozessen Zeit. Soweit diese jedoch geschaffen und entsprechende Zertifizierungen und Siegel angeboten werden, können diese von KMU zeitnah in Anspruch genommen werden (Zertifizierung, Siegel).

Abhängigkeit zum Handlungsvorschlag „Musterklauseln und Mustereinwilligungen für Industrie 4.0 hinsichtlich Datenschutz und Betriebs- und Geschäftsgeheimnisse“, siehe Kapitel 7.4.1.2.5.

572 Vgl. Handlungsvorschlag in Ziffer 7.4.1.2.5. Dies ist eine notwendige Vorstufe die zunächst umzusetzen wäre.

7.4.2.2.3 Muster-Non-Disclosure-Agreements

Betrifft: Unternehmen. Die Handlungsempfehlung richtet sich vor allem an Betreiber von Produktionsanlagen und Dienstleister mit Fokus auf die I4.0. Erarbeitung durch die Branchenverbände.

Feststellung: KMU machen nicht immer von der Möglichkeit von Non-Disclosure-Agreements Gebrauch. Auf spezifische I4.0-Anwendungen zugeschnittene Muster stehen, soweit ersichtlich, nicht zur Verfügung.

Empfehlung: KMU sollten auf Non-Disclosure-Agreements zurückgreifen. Auch hier können Branchenverbände entsprechende Muster schaffen, auf die KMU sodann zurückgreifen sollten.

Zielzustand: In der Praxis werden von KMU Muster Non-Disclosure-Agreements verwendet, die auf die spezifischen Erfordernisse von I4.0 zugeschnitten sind.

Zeitraum: Kurzfristig. Muster-NDA können für unterschiedliche I4.0-Anwendungen von den betroffenen Branchen zeitnah entwickelt werden und sollten sodann unverzüglich von KMU aufgegriffen werden, um einen entsprechenden Schutz vertraglich abzusichern.

7.4.2.3 Technisch

Ausgehend von den in Kapitel 6 vorgestellten technischen Konzepten, werden im nachfolgenden entsprechende technische Handlungsvorschläge in den Kategorien Safety & Security, Industrial Rights Management, Integritätsprüfungen und hardwarebasierte Sicherheitsanker, Maintenance und Management von Industriekomponenten, Schlüsselverwaltung für digitale Verschlüsselung sowie Production Line IT-Security Monitoring formuliert.

Safety & Security

Zukünftig müssen die Themenbereiche Safety und IT-Security gemeinsam betrachtet werden. Eine integrierte Methodik muss dabei die Sicherheit beider Bereiche gewährleisten. Diese Methodik muss zum einen sicherstellen, dass IT-Security Probleme nicht den Zugriff auf Produktionskomponenten eröffnen. Zum anderen muss der gewünschte und erlaubte Zugriff auf diese Komponenten so organisiert werden, dass hier keine Optionen eröffnet werden, die IT-Systeme zu manipulieren.

Hier gibt es zzt. weder Aktivitäten, eine integrierte Sicht zu erzeugen, noch sind Best-Practice-Ansätze für diesen Einsatzzweck verfügbar. Allerdings können diese Ansätze möglicherweise mit vertretbaren Aufwenden aus den aktuellen Prozessen und Technologien abgeleitet werden.

Beispiel: Durch Beschädigung eines IT-Systems in der Produktion mit Schadsoftware verhält sich das System nicht mehr seiner Spezifikation entsprechend. Möglicherweise bewegen sich mechanische Komponenten wie Roboterarmen schneller als zulässig. Hier erzeugt ein IT-Sicherheitsvorfall ein mögliches Safety-Risiko. Es könnte zu einer mechanischen Havarie kommen und Teile des Systems können Menschen gefährden.

Im Normalfall ist dieses Risiko jedoch durch weitere Maßnahmen beschränkt, wie z. B. die Absicherung solcher Systeme durch räumliche Abtrennung. Auch der Zugang zu diesen Räumen wird heute mit Aktuatorik und Sensorik organisiert, die an IT-Systeme angeschlossen sind. Daher kann diese Absicherung in I4.0 nicht mehr als ausreichend angesehen werden.

7.4.2.3.1 Integrierte Methodik für Safety & Security

Betrifft: Unternehmen. Die Handlungsempfehlung betrifft KMU/Industrie als Anwender von I4.0, unterstützt durch die Wissenschaft (Forschung/Entwicklung von IT-Sicherheitstechnologie für I4.0).

Feststellung: Zukünftig müssen moderne, teiloffene Produktionssysteme (cyber-physische Produktionssysteme) umfassend abgesichert werden, um unbefugten Zugriff (im Sinne von Security) zu unterbinden und gefahrbringende Betriebszustände (im Sinne von Safety) abzuwenden.

Empfehlung: Entwicklung einer integrierten Methodik (Prozesse und Standards) für den Entwurf flexibel vernetzter, zugleich Security- und Safety-kritischer Systeme.

Zielzustand: Zur Gewährleistung von Safety und Security bei Planung, Inbetriebnahme und Betrieb produktionstechnischer Anlagen unter Berücksichtigung der wechselseitigen Implikationen stehen integrierte Methoden oder Leitfäden zur Best Practice bereit.

Zeitraum: Kurzfristig, da Best Practice Guidelines im Gegensatz zur Standardisierung schnell erarbeitet werden können. Im Idealzustand liegen integrierte Standards (siehe 7.4.3.1) vor wenn die integrierte Methodik umgesetzt wird.

Industrial Rights Management

Selbst wenn die Forderung nach Verschlüsselung sensibler Daten zunächst nicht industrie-4.0-spezifisch erscheint, ist es doch als absolutes Neuland für die industrielle Produktion einzustufen. Daher erscheint es dringend geboten, die zzt. verfügbaren Technologien auf ihren Einsatznutzen bezüglich I4.0 zu analysieren, zu bewerten und an entsprechenden Stellen auch einzusetzen.

Dies ist auch bis zu einem gewissen Grad schon heute technologisch umsetzbar, auch wenn die meisten Produktionskomponenten dafür jetzt noch nicht geeignet erscheinen. Zukünftig muss Verschlüsselung als Option wählbar sein und vorhandene Systeme müssen einer Prüfung in Bezug auf ihre optionale Ertüchtigung unterzogen werden.

Beispiel: Im I4.0 Szenario ist es durchaus denkbar, dass ein Produzent von Produkten selbst gar nicht über die notwendige Produktionsinfrastruktur verfügt. Der Vision nach kann das Produkt mit bestehenden Produktionssystemen gefertigt werden, indem diese über die Web-Infrastruktur gesteuert werden. In diesem Fall würden alle Intellectual Property Werte des Produzenten auf nicht firmeneigenen Produktionssystemen verarbeitet werden.

In diesem Fall ist es ganz besonders wichtig, dass diese Daten so gehalten und verarbeitet werden, dass nur die Eigentümer dieser Daten Zugriff haben oder Zugriff erlauben können.

7.4.2.3.2 Verschlüsselung sensibler Daten

Betrifft: Unternehmen. Die Handlungsempfehlung betrifft Hersteller von Produktionsanlagen und Komponenten.

Feststellung: Durch die Auswahl und den Einsatz verschlüsselungsfähiger Protokolle oder auch Datenformate, die eine strukturerhaltende Verschlüsselung ermöglichen (z. B. XML Encryption), können sensible Daten, wie z. B. Produktions- und Fabrikationsdaten, mittels symmetrischer und asymmetrischer Kryptografie geschützt werden.

Empfehlung: Bei der Planung und Entwicklung neuer Komponenten, Systeme und Anlagen sollte, wo immer möglich, eine Verschlüsselung von sensiblen Daten vorgesehen werden.

Zielzustand: Sensible Daten werden generell nur verschlüsselt übertragen und gespeichert.

Zeitraum: Kurzfristig, da diese Maßnahmen unmittelbar in laufende Entwicklungen einfließen sollten.

Integritätsprüfungen und hardwarebasierte Sicherheitsanker

Jede Verschlüsselungstechnologie ist nur so gut, wie die Organisation der Schlüssel es zulässt. Das beste Schloss in der sichersten Tür mit dem perfektesten Schlüssel bringt keine Sicherheit, wenn der Schlüssel erworben oder das Schloss ausgebaut werden kann. Hier müssen flankierende Maßnahmen die Integrität von „Schlüssel, Schloss und Tür“ gewährleisten.

Diese Möglichkeit der Prüfung der Integrität von Industriekomponenten ist daher unmittelbar empfehlenswert und wird auch die Integrität der Schlüssel ermöglichen, die im vorangegangenen Beispiel die Datensicherheit herbeiführen können.

Im Produktionsumfeld können dies hardwarebasierte Sicherheitsanker sein. Diese lassen sich momentan bereits mittels sog. Trusted Computing Modulen (TPM) auf Produktionskomponenten aufbringen. Langfristig wird man hier technische Weiter- oder auch Neuentwicklungen benötigen.

Beispiel: In der I4.0 werden Maschinen viel autonomer miteinander interagieren als wir das heute erleben. Im Zusammenhang mit der bereits erwähnten Interaktion dieser Systeme auch über traditionelle Unternehmensgrenzen hinweg, entsteht durch die Verschränkung der Produktionsumgebungen eine als kritisch anzusehende Infrastruktur. Hier ist es daher besonders wichtig, abzusichern, dass nur autorisierte und auch integre Produktionskomponenten miteinander interagieren. Daher ist eine kontinuierliche Integritätsprüfung aller am Produktionsprozess beteiligten Komponenten erforderlich. Diese Prüfung kann aber nur erfolgen, wenn die Identität und Integrität der Produktionskomponenten sichergestellt werden kann.

7.4.2.3.3 Integritätsprüfungen

Betrifft: Unternehmen. Die Handlungsempfehlung betrifft Hersteller von Produktionsanlagen und Komponenten.

Feststellung: Die Integrität von Hard- und Softwarekomponenten ist eine wichtige Voraussetzung für eine sinnvolle Verwendung von Verschlüsselungstechnologien.

Empfehlung: Bei der Planung und Entwicklung neuer Komponenten, Systeme und Anlagen sollten Möglichkeiten zur Integritätsprüfung während der Boot- und Laufzeit sowie bei Instandhaltungsmaßnahmen geschaffen werden.

Zielzustand: Neue Komponenten besitzen bereits die rudimentäre Fähigkeit, die Integrität ihrer eigenen Firmware, Anwendungen und Konfigurationsparameter zu prüfen.

Zeitraum: Kurzfristig, da entsprechende Chips und Softwarelösung bereits am Markt erhältlich sind.

7.4.2.3.4 Verwendung hardwarebasierter Sicherheitsanker

Betrifft: Unternehmen. Die Handlungsempfehlung betrifft Hersteller von Komponenten.

Feststellung: Hardware-Sicherheitsanker in allen Endgeräten stellen eine sinnvolle Basis für zukünftige Sicherheitskonzepte für Automatisierungskomponenten und Produktionsanlagen dar, ein sinnvolles Schlüsselmanagement vorausgesetzt.

Empfehlung: Bei der Planung und Entwicklung neuer Komponenten sollte ein ‚hardwarebasierter Sicherheitsanker' vorgesehen werden, wie z. B. das in der Office-IT etablierte Trusted Platform Module (TPM). Diese Sicherheitsanker müssen in ein sinnvolles Schlüsselmanagement integriert werden.

Zielzustand: Neue Komponenten werden mit geeigneten hardwarebasierten Sicherheitsankern ausgeliefert, so dass diese für zukünftige Software-Erweiterungen vorbereitet sind.

Zeitraum: Kurzfristig, da entsprechende Produkte (Chips) bereits am Markt erhältlich sind.

Maintenance und Management von Industriekomponenten

Im Kontext der zu erwartenden zunehmenden räumlichen Verteilung der Produktion in I4.0 kommt der sicheren Inbetriebnahme und auch dem sicheren Betrieb von Systemen und Komponenten in der Fläche eine viel größere Bedeutung zu als es gegenwärtig vorstellbar ist.

Allein die Verteilung der Produktion wird eine Maintenance durch Personal vor Ort kaum umsetzbar erscheinen lassen. Hinzu kommt, dass die Anpassung der Systeme wesentlich agiler stattfinden wird.

Hier ist eine Anpassung der digitalen Systeme an Plug-and-Play-Paradigmen, wie sie bereits aus der klassischen IT bekannt sind, direkt empfehlenswert.

Beispiel: Bereits heute kennt man das Paradigma, dass sog. Apps auf Systeme geladen werden können, die dann bestimmte Funktionalitäten der Hardware operationalisieren. Bestes Beispiel sind die Navigationsfunktionen vieler Mobilfunksysteme. Das Kartenmaterial, aktuelle Verkehrsdaten und die Routenlogik werden durch Daten aus dem Cloud-Umfeld dargestellt. Die Berechnungen der Routen erfolgt in der Cloud während deren Darstellung auf dem Gerät erfolgt.

Analog kann man den Secure-Plug-and-Work-Aspekt von Industriekomponenten organisieren. Die Hardware vor Ort wird durch webgestützte Systeme kontinuierlich aktualisiert. Neue Komponenten werden durch entsprechende Technologien schnell und sicher in Produktionsumgebungen eingeführt.

7.4.2.3.5 Secure Plug & Work

Betrifft: Unternehmen. Die Handlungsempfehlung betrifft KMU/Industrie als Anwender von I4.0, unterstützt durch die Wissenschaft (Forschung/Entwicklung von IT-Sicherheitstechnologie für I4.0).

Feststellung: Eine flexible Automatisierung erfordert die Fähigkeit zur autonomen Rekonfiguration und Optimierung der Produktionsumgebung, ohne dabei Safety oder Security zu gefährden.

Empfehlung: Entwicklung geeigneter Hardware- und Softwarekomponenten zur Umsetzung des Szenarios „Secure Plug & Work" für safety-kritische Systeme in der Industrie 4.0.

Zielzustand: Neu entwickelte Hard- und Softwarekomponenten bieten ein Höchstmaß an automatischer Konfigurations- und Rekonfigurations-Funktionalität im Sinne von Secure Plug & Work.

Zeitraum: Kurzfristig, da nur Änderungen an der Software erforderlich sind.

Schlüsselverwaltung für digitale Verschlüsselung

Wie in dem Abschnitt Industrial Rights Management bereits erwähnt wurde, kommt der Verschlüsselung von Industriedaten immer größere Bedeutung zu. Hierzu werden nicht nur entsprechend sichere Schlüssel auf integren Komponenten benötigt. Vielmehr muss insbesondere bei asymmetrischen Verschlüsselungsmethoden mit zwei unterschiedlichen Schlüsseln die dadurch erhöhte Komplexität der Schlüsselverteilung und –verwaltung entsprechend sicher dargestellt werden.

Dazu gibt es bereits Best-Practice-Ansätze aus dem PKI-Umfeld. Auch wenn diese Technologie nicht I4.0-spezifisch ist, sollte es möglich sein, eine Zertifikatsinfrastruktur zur Verschlüsselung analog dieser Methode zu etablieren.

Beispiel: Maschinen bekommen, wie im Abschnitt hardwarebasierte Sicherheitsanker bereits beschrieben wurde, zukünftig digitale Identitäten. Damit erfüllen sie alle Voraussetzungen, um mittels der verfügbaren Technologie PKI Identitäts- und Verschlüsselungszertifikate zu verarbeiten.

Die Verwaltung und Organisation dieser Schlüssel kann als Best-Practice-Ansatz aus der klassischen IT übernommen werden.

7.4.2.3.6 Aufbau von Public-Key-Infrastruktur oder Single-Sign-On

Betrifft: Unternehmen. Die Handlungsempfehlung betrifft Hersteller von Komponenten und Anlagen.

Feststellung: Der Aufbau einer zukunftsfähigen Infrastruktur, wie z. B. einer Public-Key-Infrastruktur (PKI) oder eines M2M-fähigen Single-Sign-On (SSO) Systems, dient der Ausstellung von Zertifikaten/Sicherheitstokens und Schlüsseln für Komponenten, Maschinen, Dienste und Personen. Eine solche Infrastruktur stellt grundsätzlich eine mögliche und sinnvolle Basis für den sicheren Betrieb und Austausch von Daten zwischen Komponenten, Systemen und Anlagen auch über Unternehmensgrenzen hinweg dar.

Empfehlung: Mit dem Aufbau einer PKI können je nach Größe und Zweck hohe Aufwände und Kosten verbunden sein. Außerdem müssen Parteien, die miteinander kommunizieren möchten, von derselben Zertifizierungsstelle erfasst sein oder die zertifizierenden Instanzen müssen über eine Zertifikatskette verbunden sein. Diese Voraussetzungen werden häufig als Hinderungsgrund für den Einsatz von Zertifikaten im industriellen Umfeld genannt. Ein möglicher Ansatz wäre die Bereitstellung entsprechender Infrastrukturen durch die Hersteller von Maschinen und Komponenten als Mehrwertdienst zu ihren Produkten.

Zielzustand: Hersteller von Maschinen und Komponenten liefern ihre Produkte bereits mit digitalen Identitäten aus und ermöglichen den Anwendern mittels geeigneter sicherer Verfahren Zugriff auf entsprechende Schlüssel und Zertifikate.

Zeitraum: Mittelfristig, da nicht ohne umfassende Änderungen an die bisherigen Prozesse möglich.

Production Line IT-Security Monitoring

Auch in einer Produktionsumgebung mit integren Komponenten, die verschlüsselte Daten halten und mittels eindeutiger Hardwareidentitäten sicher organsiert werden können, sind dennoch IT-Sicherheitsprobleme denkbar. Diese müssen zeitnah erkannt werden und auf ihre Ursachen zurückverfolgt werden können. Insbesondere an der Produktionslinie ist dabei ein Monitoring der gesamten Infrastruktur wünschenswert, die so organisiert ist, dass die Produktion nicht gestört oder verlangsamt wird.

Hier ist zu empfehlen, auf der Basis von Datenauswertung und Mustererkennung IT-Sicherheitsvorfälle so früh wie möglich zu erfassen und Abwehrmaßnahmen zu ergreifen.

Beispiel: Industrie 4.0 fokussiert sehr auf die Auswertung aller Daten, die im und um den Produktionsprozess erzeugt werden. Hier werden schon jetzt Auswerteverfahren herangezogen, um die Performance zu steigern und die Störanfälligkeit zu verringern. Diese Daten können ebenfalls dahin gehend ausgewertet werden, dass die Erkennung auf IT-Sicherheitsaspekte hin ausgeweitet wird.

7.4.2.3.7 Entwicklung von Anomalie-Erkennungssystemen

Betrifft: Unternehmen. Die Handlungsempfehlung betrifft Hersteller und Betreiber von Produktionsanlagen und Komponenten, Forschung und Entwicklung.

Feststellung: Um auch zukünftigen Sicherheitsrisiken nachhaltig zu entgegnen, sind neue, adaptive Verfahren notwendig, welche die IT-Systeme nicht isoliert betrachten, sondern zielgerichtet den Produktionsprozess selbst schützen. Es müssen neue Methoden gefunden werden, um die IT-Landschaft der Produktion im laufenden Betrieb einer Analyse und Absicherung zu unterziehen, ohne Ziele wie Echtzeitfähigkeit und Verfügbarkeit zu gefährden.

Empfehlung: Die Forschung und Entwicklung an intelligenten, kombinierten und adaptiven Anomalie-Erkennungssystemen (z. B. zur Erkennung von Eindringlingen (Intrusion Detection)) sollte intensiviert werden. Mit derartigen Systemen kann einer Vielzahl heutiger und häufiger Probleme der Industrie begegnet werden, u. a.:

- Analyse und Bewertung von IT-Sicherheit in Produktionsanlagen bereits in der Planungsphase
- Kontinuierliche Überwachung einer Anlage im Betrieb, ohne direkt auf die Systeme physikalisch zugreifen zu müssen
- Berücksichtigung von Kontextinformationen und semantischem Bezug auf den IST-Zustand
- Bereitstellung eines Tools, bspw. als Cloud-Dienst, ermöglicht die dezentrale und zeitgleiche Überwachung mehrerer Standorte
- Protokollierung aller Ereignisse für die Einhaltung der gesamten Compliance Auflagen

Zielzustand: Neue Komponenten sollen mindestens alle sicherheitsrelevanten Ereignisse protokollieren und zum Zwecke einer späteren Auswertung bereitstellen. Intelligente, kombinierte und adaptive Anomalie-Erkennungssysteme sollen in Produktionsanlagen integrierbar und einsetzbar sein.

Zeitraum: Mittelfristig, da Forschung und anschließende Produktentwicklung sowie Evaluierung der Ergebnisse notwendig ist.

7.4.3 Normungs-/Standardisierungsorganisationen

Ausgehend von den in Kapitel 6.1 vorgestellten technischen Konzepten und der Bewertung der Normen und Standards in Kapitel 6.4, werden nachfolgend entsprechende Handlungsvorschläge formuliert, die sich primär an Normungs- und Standardisierungsorganisationen richten und Industrieunternehmen als Anwender von I4.0 nur indirekt betreffen.

7.4.3.1 Erarbeitung integrierter Standards für Safety & Security

Betrifft: Standardisierungsorganisationen (Industrieunternehmen als Anwender von I4.0, aber auch als Mitglieder in Standardisierungsgremien, wie z. B. DIN, DKE oder internationale Pendants).

Feststellung: Für Safety gibt es eine Vielzahl branchenspezifischer Standards. In diese Standards sollen zukünftig die notwendigen Ergänzungen für IT-Security so eingebracht werden, dass Vernetzung über offene Netzwerke möglich wird. In Zukunft werden auch vermehrt Security-Zertifizierungen gefordert werden. Ziel ist es hier, eine integrierte Safety-Security-Zertifizierung vorzubereiten, die auch Systeme erfasst, welche sich zur Laufzeit autonom verändern.

Empfehlung: Erarbeitung eines integrierten Sicherheitskonzepts im Sinne von Security und Safety durch Standardisierungsorganisationen mit dem Ziel einer gemeinsamen Zertifizierung.

Zielzustand: Integrierte Methoden zur Gewährleistung von Safety und Security bei Planung, Inbetriebnahme und Betrieb produktionstechnischer Anlagen unter Berücksichtigung der wechselseitigen Implikationen sind durch die entsprechenden Gremien und Organisationen standardisiert.

Zeitraum: Mittelfristig, da Erarbeitung von Standards zeitaufwändiger ist.

7.4.3.2 Erarbeitung einer Struktur für IT-Sicherheitsstandards

Betrifft: Standardisierungsorganisationen (wie z. B. DIN, DKE oder internationale Pendants sowie Verbände wie BITKOM).

Feststellung: Es gibt keine allgemein akzeptierte Struktur von IT-Sicherheitsstandards, die für Industrie 4.0 unmittelbar einsetzbar wäre.

Empfehlung: Erarbeitung einer für Industrie 4.0 passenden Struktur und Klassifikation für IT-Sicherheitsstandards abgeleitet aus dem Referenzarchitekturmodell Industrie 4.0 (RAMI4.0) und den existierenden Referenzmodellen für ICS unter Einbindung wichtiger Unternehmen aus dem Bereich industrielle Produktion.

Zielzustand: Themenfeld IT-Sicherheit ist in einem Industrie-4.0-Referenzmodell klar strukturiert, mit einer Ableitung der dazu notwendigen Standards.

Zeitraum: Mittelfristig. Es ist unbedingt erforderlich, diese Standardisierungsaufgabe schnellstmöglich in Angriff zu nehmen, da beispielsweise das bereits existierende Referenzmodell IIRA[573] des IIC der IT-Sicherheit eine wesentliche Rolle zuschreibt.

7.4.3.3 Integration technischer Standards mit ISMS-Standards

Betrifft: Standardisierungsorganisationen (wie z. B. DIN, DKE oder internationale Pendants sowie Verbände wie BITKOM).

Feststellung: Standards im Bereich „Bewertung“ und „Richtlinien“ sind losgelöst von den technischen Standards.

Empfehlung: Aufruf an die Standardisierungsgremien zur Erarbeitung von Richtlinien zur Umsetzung der Bewertungsstandards und Richtlinien auf die technischen Standards der Internet-Welt (W3C, IETF, OASIS) und der Serie von OPC Unified Architecture (OPC UA) Standards (konzeptionell und technisch).

Dabei sollen die Spezifika von Industrie 4.0, insbesondere der nicht-funktionalen Anforderungen, in Form von Profilen/Ausprägungen der technischen Standards der Internet-Welt berücksichtigt werden, genauso wie die entstehenden Industrie-4.0-Referenzarchitekturen, abgeleitet aus dem RAMI 4.0 und den existierenden Referenzmodellen für ICS.

Zielzustand: Abgestimmte, integrierte Landschaft von IT-Sicherheitsstandards über die Ebenen Bewertung, Richtlinie und Technik.

Zeitraum: Mittelfristig. Standardisierungsgremien und Branchenverbände sollen diese Lücke schließen.

7.4.3.4 Engineering von sicheren IT-Systemen

Betrifft: Standardisierungsorganisationen (wie z. B. DIN, DKE oder internationale Pendants sowie Verbände wie BITKOM, VDI/VDE, VDMA und ZVEI unter differenzieller Berücksichtigung von Anforderungen verschiedener Branchen und Unternehmensgrößen).

Feststellung: IT-Sicherheitsstandards sollten einfließen in das Engineering von IT-Systemen („security and privacy by design“).

Empfehlung: Erarbeitung einer Richtlinie für eine IACS-bezogenen Analyse- und Design-Methode unter besonderer Berücksichtigung der IT-Sicherheitsmanagementanforderungen nach ISO/IEC 27001 in Verbindung mit ISO/IEC 27002, VDI/VDE 2182, BDSG und BSI-Grundschutz sowie der Fähigkeiten der zu der jeweiligen Wertschöpfungskette passenden technischen Referenzarchitektur und deren IT-Sicherheitsstandards.

Zielzustand: Richtlinie für eine IACS-bezogene Analyse- und Design-Methode unter Berücksichtigung von IT-Sicherheitsanforderungen existiert.

Zeitraum: Langfristig. Wegen der Fülle von Anforderungen erscheint dieses Ziel nur langfristig erreichbar.

573 Industrial Internet Reference Architecture des Industrial Internet Consortium (IIC), siehe http://www.iiconsortium.org/IIRA.htm

8. Anhang

8.1 Bedrohungen und Mapping auf Maßnahmen

8.1.1 Nummerierte Bedrohungen aus Kapitel 4

1. Für alle Prozesse im Rechenzentrum:

    1.1. Rechteausweitung: Ein Angreifer könnte Datenflüsse zwischen Prozessen verändern, um die Programmausführung zu beeinflussen, bspw. Ausführung von Schadcode im Prozesskontext.

    1.2. Rechteausweitung: Ein Anwender könnte aus der Ferne Schadcode im Kontext eines Anwendungsprozesses ausführen.

    1.3. Rechteausweitung: Ein Angreifer könnte sich durch Übernahme eines Anwendungsprozesses als Kunde ausgeben und in dessen Namen Käufe tätigen.

    1.4. Enthüllung: Ein Angreifer könnte durch Spoofing Zugriff auf vertrauliche Informationen erhalten.

    1.5. DoS: Crash, Stopp oder langsame Ausführung von Anwendungsprozessen.

    1.6. Leugnung: Anwendungsprozesse könnten abstreiten, z. B. Auftragsdaten von außerhalb der Vertrauensgrenze erhalten zu haben.

    1.7. Manipulation: Durch mangelnde Validierung von Eingabedaten durch Anwendungsprozesse. Datenflüsse über die Vertrauensgrenze zu Anwendungsprozessen können durch Angreifer manipuliert werden und zu Angriffen auf die Verfügbarkeit (DoS), Rechteausweitung oder Enthüllung vertraulicher Information durch Anwendungsprozesse führen.

    1.8. Verfügbarkeit: Ein Angreifer könnte mittels DoS-Angriff auf die zentrale Datenbank im Rechenzentrum die gesamte Logistik zum Erliegen bringen.

    1.9. Vertraulichkeit: Ein Angreifer könnte Zugriff auf vertrauliche Daten in der zentralen Datenbank erlangen.

    1.10. Integrität: Ein Angreifer könnte durch Manipulation an der zentralen Datenbank Einfluss auf sämtliche Logistikprozesse einschließlich nachgelagerter Systeme wie PLS und MES nehmen.

2. Kommunikation über das Internet:

    2.1. Unterbrechung von Datenflüssen über Unternehmensgrenzen und Internet. Beispielsweise Verhinderung der Übermittlung von Aufträgen.

    2.2. Datenübertragungen (z. B. Auftragsdaten) könnten abgehört oder manipuliert werden und dadurch zu Compliance-Verletzungen führen. (Sollte durch Annahme verschlüsselter Verbindungen abgesichert sein).

    2.3. Mittels Spoofing von Anwendungsprozessen, wie z. B. Verkauf, könnte ein Angreifer Zugriff auf vertrauliche Informationen erhalten.

    2.4. Mittels Spoofing externer Akteure, wie z. B. Kunden, könnte ein Angreifer beispielsweise unautorisierten Zugriff auf Anwendungsprozesse erlangen.

3. Produktion/Maschinenbetreiber:

    3.1. Verfügbarkeit: Angreifer könnten MES- oder PLS-Systeme mittels DoS-Angriffen zum Absturz oder zu verlangsamter Ausführung bringen.

    3.2. Datenübertragungen zu MES- & PLS-Systemen (z. B. Auftragsplanung) könnten abgehört oder manipuliert werden und dadurch zu Compliance-Verletzungen führen.

    3.3. Leugnung: MES des Auftragnehmers könnte behaupten, über Vertrauensgrenzen gesendeten Fertigungsauftrag nicht erhalten zu haben.

    3.4. Leugnung: PLS des Auftragnehmers könnte behaupten, einen über Vertrauensgrenzen gesendete Prozessdaten nicht erhalten zu haben.

    3.5. Angreifer könnte Zugriff auf Passwörter für Fernwartungsportal erlangen.

    3.6. Angreifer könnte Zugriff auf Fabrikationsdaten im Produktionssystem erlangen (Verlust von Know-how) oder diese Manipulieren (Sabotage der Produktion).

3.7. Auslesen und Ändern von Datenspeichern in Produktionsanlagen und Steuerungskomponenten: Verlust von Know-how, internem Wissen oder Sabotage der Produktion.

4. Dienstleister für Fernwartung:

4.1. Accounting: Passwörter könnten an unberechtigte Personen gelangen.

4.2. DoS gegen VPN-Concentrator möglich.

4.3. Zugriff auf oder Manipulation von Images für Wartungs-PC: von Firmwareupdates, Ausspähen von Anlagendetails über Konfiguration und Projektierungsdaten, Sabotage von Anlagen über das Fernwartungsportal.

4.4. Auslesen/Ändern von Fabrikationsdaten via Fernwartung: Verlust von Know-how oder Sabotage der Produktion.

5. Maschinenhersteller:

5.1. Passwörter für Fernwartungsportal könnten an unberechtigte Personen gelangen.

8.1.2 Kreuztabelle der Bedrohungen und Maßnahmen des ICS-Security-Kompendiums

Tabelle 8–1: Kreuztabelle der identifizierten Bedrohungen und Maßnahmen des BSI ICS-Security-Kompendiums

	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59-63	64	65	66-70	71-72	73
1.1		x	x		x			x							x				x	x			x	x	x				x		x	x	x	x	x						
1.2	x	x	x		x			x							x				x	x			x	x	x				x		x	x	x	x	x						
1.3		x	x		x			x							x				x	x			x	x	x				x		x	x	x	x	x						
1.4		x	x					x							x		x		x	x			x	x	x				x		x	x	x	x	x						
1.5	x		x						x						x			x	x						x											x					
1.6		x	x																	x			x	x							x		x								x
1.7			x		x			x							x				x	x															x						
1.8	x		x						x						x			x	x						x											x				x	
1.9			x		x			x									x		x	x															x	x			x		
1.10			x		x														x	x															x	x					
2.1			x		x																																				
2.2			x		x			x																							x				x	x					
2.3			x		x			x												x															x	x					
2.4		x	x		x			x												x															x	x					
3.1	x		x				x		x								x	x	x						x			x								x		x		x	
3.2			x		x		x	x	x									x		x								x							x	x		x	x		
3.3		x	x																	x			x	x							x		x								x
3.4		x	x																	x											x		x								x
3.5		x	x		x	x		x											x	x			x	x				x								x					
3.6			x		x		x	x							x				x	x								x			x				x	x			x		
3.7			x		x		x	x	x	x								x	x	x								x			x				x	x		x			
4.1		x	x		x	x		x															x	x							x					x					
4.2			x			x																																			
4.3			x		x	x		x											x																	x		x			
4.4			x			x		x									x														x				x	x		x			
5.1		x	x		x		x	x															x	x							x	x	x			x					

8.2 Glossar

Der vorliegenden Studie liegt der „Glossar Industrie 4.0 des Fachausschuss VDI/VDE-GMA 7.21 ‚Industrie 4.0'" [574] in Version 4 zugrunde.

- **Netzwerksegmentierung (VLAN)**
  VLANs (Virtual Local Area Networks) trennen Netzwerke auf logischer Ebene (OSI-Layer 2). Durch eine Segmentierung großer Layer-2-Netzwerke in viele kleinere ist zum einen eine erhebliche Steigerung der Netzwerkperformance und zum anderen auch eine zusätzliche Trennung nach Funktion, Geräte- oder Sicherheitsklassen möglich.

- **Sprungserver**
  Ein so genannter Sprungserver (englisch: Jump server) ist ein speziell gehärtetes und überwachtes System, das eine Brücke zwischen zwei unterschiedlichen Sicherheitszonen spannt und dadurch Zugriff zwischen beiden Zonen in stark kontrollierter Weise ermöglicht. Sprungserver werden typischerweise zwischen einer Sicherheitszone und einer DMZ eingesetzt, um eine transparente Verwaltung von Systemen in der DMZ zu ermöglichen. Dazu muss zuvor eine entsprechend gesicherte Sitzung durch einen Benutzer aufgebaut werden.

- **Defense-in-Depth**
  In der IT-Sicherheit bezeichnet Defense-in-Depth einen Ansatz zur Risikominimierung mittels gestaffelter Sicherheitsebenen. Der gleichzeitige Einsatz verschiedener Sicherheitstechnologien auf verschiedenen Ebenen minimiert das Risiko, wenn eine Sicherheitsmaßnahme ausfällt bzw. umgangen wird. Dies kann bspw. durch den redundanten Einsatz verschiedener Technologien oder Produkte verschiedener Hersteller auf verschiedenen System-Komponenten oder -Ebenen erfolgen.

- **Zero-Day-Exploit**
  Zero-Day-Exploit nennt man einen Exploit, der eingesetzt wird, bevor es einen Patch als Gegenmaßnahme gibt. Entwickler haben dadurch keine Zeit („null Tage" englisch: zero day), die Software so zu verbessern, dass der Exploit unwirksam wird, um so deren Nutzer zu schützen.

- **(Distributed) Denial of Service**
  In der IT-Sicherheit bezeichnet Denial of Service (DoS; englisch für „Dienstblockade") die Nichtverfügbarkeit eines Dienstes, der eigentlich verfügbar sein sollte. Obwohl es verschiedene Gründe für die Nichtverfügbarkeit geben kann, wie unbeabsichtigte Überlastungen, spricht man von DoS im Sinne der IT-Sicherheit dann, wenn diese die Folge einer Überlastung von Infrastruktursystemen in Folge eines mutwilligen Angriffs auf IT-Systeme bzw. Komponenten in einem Netzwerk ist. Wird diese Überlastung von einer größeren Anzahl anderer IT-Systeme verursacht, so wird von einer verteilten Dienstblockade oder englisch Distributed Denial of Service (DDoS) gesprochen.

- **Public-Key-Infrastruktur**
  In der IT-Sicherheit bezeichnet PKI ein System, das digitale Zertifikate ausstellen, verteilen und prüfen kann. Die innerhalb einer PKI ausgestellten Zertifikate werden beispielsweise zur Absicherung rechnergestützter Kommunikation verwendet.

- **Zonierung**
  Das Prinzip der Zonierung ist ein Ansatz, der im Standard IEC 62443 explizit eingeführt wird. Zonen werden durch physikalische und/oder logische Trennung auf Netzwerkebene implementiert. Netzwerkzonen stellen einen Defense-in-Depth-Ansatz auf Netzwerkebene dar, der zur Härtung des Gesamtsystems gegenüber Angriffen dient.

8.3 Begriffsdefinitionen

Alle verwendeten Begriffe sind im Text erläutert.

574 Siehe http://www.iosb.fraunhofer.de/servlet/is/48960/Begriffsdefinitionen_VDI_GMA_FA7-21_v4.pdf?command=downloadContent&filename=Begriffsdefinitionen_VDI_GMA_FA7-21_v4.pdf, zuletzt abgerufen am 07.12.2015.

www.bmwi.de