Vertrauliche Verarbeitung staatlich eingestufter Information - die Informationstechnologie im Geheimschutz

Wilfried Gericke[1], Dirk Thorleuchter[1], Gerhard Weck[2], Frank Reiländer[2], Dirk Loß[2]

[1] Fraunhofer Int, Appelsgarten 2, 53879 Euskirchen
[2] INFODAS Gesellschaft für Systementwicklung und Informationsverarbeitung mbH, Rhonestr. 2, 50765 Köln
{Wilfried.Gericke|Dirk.Thorleuchter}@int.fhg.de, {Gerhard.Weck|Frank.Reilaender|Dirk.Loss}@infodas.de

Bedingt durch die in den letzten Jahren aufkommende asymmetrische Bedrohung[1] ist von staatlichen Stellen eine vermehrte Aktivität zur Gefahrenabwehr im Bereich der öffentlichen Sicherheit notwendig. Diese ist von den staatlichen Einrichtungen nicht alleine zu erbringen. Ein wesentliches Element der Gefahrenabwehr ist die staatlich geförderte Sicherheitsforschung, die u.a. im nationalen Sicherheitsforschungsprogramm des BMBF und im 7. Forschungsrahmenprogramm der EU ab 2007 beheimatet ist. Diese Forschungsvorhaben werden häufig sicherheitssensible Informationen beinhalten und wahrscheinlich in Vielzahl nach dem Geheimschutzverfahren eingestuft. Eine wesentliche Voraussetzung für die Akquisition von Fördermitteln zur Durchführung solcher Forschungsvorhaben ist das Vorhandensein einer Geheimschutz-konformen informationstechnischen Infrastruktur. In diesem Bericht werden die allgemeinen Trends und Entwicklungen im Geheimschutz unter dem speziellen Aspekt der Informationstechnologie dargestellt und mögliche Probleme sowie deren Lösungsmöglichkeiten aufgezeigt.

In the last years, the rising asymmetrical threat is causing governments to pay more attention to security, especially in technical areas. New and ever more complex tasks in areas concerned with defence against these new types of threat require additional research and development of new techniques. For this reason, national and European governments are increasingly funding security research. So the German national research program now contains a lot of security topics, and the European framework research program (FP7) also contains security research as a central point. These security research projects will start in 2007/2008 and may often contain classified (e.g. restricted or secret) information. In order to acquire funding in this area, researchers have to demonstrate the existence of an IT infrastructure satisfying special requirements as are outlined in security standards like ISO 27001 or the German “Grundschutzhandbuch” (“Baseline Security Manual”). The following paper presents current trends and developments for the protection of restricted information and outlines possible problems as well as their solutions.

EINLEITUNG

Seit Bestehen der Bundesrepublik Deutschland ist der Geheimschutz in das Staatenwesen integriert. Seine Zielsetzung sind der Schutz und die Geheimhaltung von Verschlusssachen (VS). VS sind im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform [3]. Die Schutzbedürftigkeit gliedert sich in unterschiedliche Einstufungsgrade. Tatsachen, Gegenstände oder Erkenntnisse, die keine VS sind, werden als „offen“ bezeichnet. Nach §4 SÜG (Sicherheitsüberprüfungsgesetz) ist eine Verschlusssache

- VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD), wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann,
- VS-VERTRAULICH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder schädlich sein kann,
- GEHEIM, wenn die Kenntnisnahme durch Unbefugte die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen kann,

[1] [Mit] asymmetrische[r] Bedrohung [...] wird eine Konfliktform umschrieben, bei der sich Staaten oder Gesellschaften seitens staatlicher oder nichtstaatlicher Akteure, z.B. terroristische Netzwerke, Befreiungskämpfer, Computerhacker, einer Gefährdung durch zumeist nicht konventionelle Mittel ausgesetzt sehen. [8]

- STRENG GEHEIM, wenn die Kenntnisnahme durch Unbefugte den Bestand oder lebenswichtige Interessen der Bundesrepublik Deutschland oder eines ihrer Länder gefährden kann.

Die Einstufung erfolgt entsprechend der Schutzbedürftigkeit von einer amtlichen Stelle oder auf deren Veranlassung. Da die Definitionen der Einstufungsgrade gemäß §4 SÜG unscharf formuliert sind, erfolgt die Einstufung in der Regel subjektiv, d.h. die amtliche Stelle hat hierzu einen gewissen Ermessensspielraum.

Eine Statistik aus dem Jahr 2002 [10] zeigt die Verteilung der verschiedenen Einstufungen auf (Abbildung 1). Auch wenn die Daten nur eine Schätzung darstellen und aufgrund der aktuellen sicherheitspolitischen Lage bereits veraltet sind, so lässt sich daraus eine wesentliche Grundaussage ableiten: Nur wenige eingestuften Daten werden als Vertraulich oder Geheim eingestuft. Die mit Abstand am meisten eingestuften Daten unterliegen dem Einstufungsgrad VS-NfD. Oftmals sind hier praktische Gegebenheiten wie das einfachere Handling ausschlaggebend.

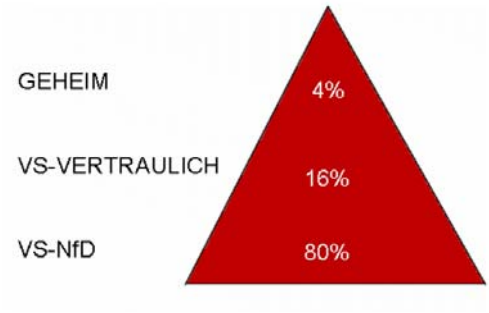

Abb. 1 Pyramide der Verschlusssachen

Mit der Einstufung ergeben sich konkrete Anforderungen an die Gewährleistung der Vertraulichkeit der betreffenden Informationen. Sofern diese Informationen nur in Papierform vorliegen, steht für ihre Handhabung schon lange ein detailliertes Regelwerk zur Verfügung, das genau vorschreibt, welche Aktionen im Umgang mit VS erlaubt sind und welche nicht. Ganz anders sieht es aus, wenn, wie heute allgemein üblich, VS als elektronische Dokumente erstellt, bearbeitet und ausgetauscht werden. Die geltenden Vorschriften versuchen, die Regularien für den Umgang mit Papier so auf die Handhabung elektronischer Dokumente zu übertragen, dass deren Vertraulichkeit gewahrt bleibt. Daraus ergeben sich eine Vielzahl von Einschränkungen für den Umgang mit VS-Daten, die alle letztlich das Ziel haben, Informationsflüsse so kontrollierbar zu machen, dass nur hinreichend ermächtigte Personen Zugriff auf VS erhalten.

Dieser Artikel stellt dar, welche Schwierigkeiten sich beim Umgang mit VS-Daten ergeben und welche Möglichkeiten die Informationstechnologie bietet, die notwendige Vertraulichkeit zu gewährleisten. Da die geltenden Regelungen den tatsächlichen Anforderungen jedoch nur zum Teil gerecht werden, ist eine historische Betrachtung des Geheimschutzes in der Bundesrepublik Deutschland sinnvoll, um die Entstehung dieser Vorgaben leichter nachvollziehen zu können.

HISTORISCHE BETRACHTUNG

Empirisch bzw. statistisch gewonnene Daten, welche die Anzahl von eingestuften Dokumenten chronologisch angeben und somit einen Eindruck über die Wichtigkeit des Geheimschutzes in verschiedenen Zeitperioden vermitteln, sind nicht verfügbar. Dies liegt daran, dass auch die Tatsache, dass ein Dokument eingestuft ist, ebenfalls in der Regel eine eingestufte Information darstellt. Dennoch lassen sich aufgrund eigener Erfahrungen drei unterschiedliche Zeitabschnitte charakterisieren.

Die Blütezeit des Geheimschutzes fand zu Zeiten des kalten Krieges (von den 50er bis Ende der 80er Jahre) statt. Im Vordergrund stand hier der Schutz von Informationen vor den feindlichen Kräften der Warschauer Pakt Staaten. Eine Vielzahl an Dokumenten wurde in dieser Zeit eingestuft, darunter auch viele mit höheren Einstufungen wie z.B. Geheim und Streng Geheim. Die Dokumente sind in der Regel nicht mit informationstechnischen Verfahren (Computer), sondern manuell mit Schreibmaschine, Stift und Papier erstellt bzw. bearbeitet worden. Auch später war – trotz der technischen Möglichkeiten – die Verwendung von PCs oft explizit verboten.

Mit dem Wegfall der Ost-West Konfrontation (Anfang der 90er Jahre) stellte sich eine neue Situation für den Geheimschutz dar. Man war allgemein überzeugt, dass Deutschland nun nur noch umgeben von „Freunden“ sei und kein Staat eine unmittelbare Gefahr für Deutschland darstellte. Die Sicherheit Deutschlands war also gewährleistet. Der mit der Einstufung eines Dokuments befasste amtliche Bearbeiter wählte in dieser Zeit nur selten hohe Einstufungen, da nach der Definition von Geheim und Streng Geheim die Sicherheit der BRD gefährdet sein musste. Der Trend ging eher dahin, meistens offen und wenn überhaupt, dann möglichst niedrig einzustufen.

Ein weiteres Indiz für die offene bzw. niedrige Einstufung war die in dieser Zeit zunehmend aufkommende Bearbeitung von Dokumenten mit informationstechnischen Verfahren. Die Einführung von Computern und Netzwerken in Behörden und Ämtern sowie bei den Auftragnehmern, die mit eingestuften Dokumenten arbeiteten, zwang die amtlichen Bearbeiter, eine möglichst niedrige Einstufung zu wählen. Denn für die informationstechnische Bearbeitung von eingestuften Dokumenten ist je nach Einstufung das Vorhandensein einer sehr teuren IT-Infrastruktur erforderlich. Selbst wenn diese beim Auftraggeber und Auftragnehmer vorhanden war, so konnte in dieser Zeit die IT-Bearbeitung von VS nur mit großen Einschränkungen hinsichtlich des Komforts erfolgen [13].

Der letzte Zeitabschnitt beginnt durch die in den letzten Jahren aufkommende asymmetrische Bedrohung (seit 2001) und mit dem sich daraus ableitenden neuen Sicherheitsverständnis. Dadurch bedingt ist von staatlichen Stellen eine vermehrte Aktivität zur Gefahrenabwehr im Bereich der öffentlichen Sicherheit zu beobachten, da man sich nicht mehr auf die Abwehr von Angriffen durch Fremdstaaten beschränken kann, sondern auch Bedrohungen durch Einzelpersonen wie etwa Bombenbauer in der Nachbarschaft berücksichtigen muss. Die Abwehr auch solcher Gefahren liegt im (sicherheitspolitischen) Interesse der Bundesrepublik Deutschland. Die unbefugte Kenntnisnahme von staatlichen Sicherheitsmaßnahmen stellt sich für die BRD zumindest als nachteilig dar. Somit liegen die Aktivitäten zur Gefahrenabwehr im Geltungsbereich der VS-Definitionen nach §4 SÜG und sind einzustufen.

Die staatlich geförderte Sicherheitsforschung unterstützt die Entwicklung neuer Methoden und Verfahren zur Gefahrenabwehr. Hinweise hierfür gibt das neue vom BMBF vorbereitete Programm zur zivilen „Sicherheitsforschung“. Es zielt auf einen bisher noch nicht ausreichend abgedeckten Bereich ab, nämlich Forschung für Sicherheit vor Terrorismus, Kriminalität oder Sabotage und vor den Folgen von Naturkatastrophen oder Unfällen besonderen Ausmaßes zu leisten [12]. Diese Forschungsvorhaben werden häufig sicherheitssensible Aktivitäten beinhalten und daher wahrscheinlich in Vielzahl eingestuft. Als wesentliches Bedrohungsszenario ist hier zu sehen, dass Informationen über sicherheitsrelevante Schwachstellen oder über Methoden und Verfahren zur Zerstörung von Infrastruktur, gesellschaftlichen Strukturen und Menschenleben in die Hände von Kriminellen oder Terroristen gelangen.

Auch im Rahmen der europäischen Union ist die Gefahrenabwehr ein Thema von steigendem Interesse. So liegt ein wesentlicher Schwerpunkt des kommenden 7. Forschungsrahmenprogramms im Bereich der Sicherheitsforschung [6]. Die EU hat hierzu im Sommer 2006 ihre Geheimschutzrichtlinien erneuert [5]. Es ist auch hier zu erwarten, dass eine Vielzahl an Forschungsvorhaben gemäß diesen Geheimschutzrichtlinien eingestuft wird.

Dies führt dazu, dass der rückläufige Trend bei der Einstufung von Verschlusssachen gestoppt wird. Es ist sogar aufgrund steigender Sicherheitsaktivitäten künftig mit einem wachsenden Vorkommen von Verschlusssachen zu rechnen. Daher werden auch Forschungseinrichtungen (Universitäten, Forschungsinstitute und gewerbliche Wirtschaft), die zukünftig Vorhaben in der Sicherheitsforschung akquirieren möchten, demnächst erstmalig bzw. verstärkt vom Geheimschutz betroffen sein.

Um VS-Aufträge akquirieren zu können, ist mit der Angebotseinreichung ein Nachweis über die VS-Berechtigung des Auftragnehmers erforderlich. Hierzu sind vorab für den jeweiligen Einstufungsgrad unterschiedliche organisatorische und informationstechnische Maßnahmen nach dem Geheimschutzhandbuch notwendig. Diese Maßnahmen sind für den niedrigsten Einstufungsgrad „VS – Nur für den Dienstgebrauch“ noch relativ preisgünstig umsetzbar. Der Aufbau einer VS-Infrastruktur für Vertraulich und Geheim ist aufwendig und kostenintensiv, da hier völlig in sich geschossene Systeme bzw. Netze mit aufwendigen Zugangs- und Zugriffskontrollen, umfangreiche Protokollierungs- und Überwachungsfunktionen sowie Schutz gegen kompromittierende Abstrahlung gefordert werden. Daher sollte man sich, wenn man bisher nur wenig Erfahrung mit dem Geheimschutz hat, zunächst auf den niedrigsten Einstufungsgrad VS-NfD beschränken. Aufgrund des prozentual hohen Anteils von VS-NfD erreicht man damit das beste Kosten-Nutzen Verhältnis [13].

In den folgenden Abschnitten werden die vom Geheimschutz geforderten Maßnahmen skizziert, wobei zu beachten ist, dass die geltenden Vorschriften, in Abhängigkeit von der Einstufung der Informationen, im Detail zu befolgen sind. Dies führt auf der Ebene der infrastrukturellen Maßnahmen oft zu erheblichen Kosten, während auf der technischen Ebene häufig gravierende Einschränkungen der Arbeitsmöglichkeiten zu verzeichnen sind,

insbesondere weil die heute im Client-/Server-Bereich eingesetzten IT-Systeme nur höchst eingeschränkt in der Lage sind, den geforderten Schutz der Vertraulichkeit von VS-Daten zuverlässig zu gewährleisten.

ORGANISATORISCHE UND INFRASTRUKTURELLE MAßNAHMEN

Organisatorische Maßnahmen sind bei der Verarbeitung von VS verpflichtend, die informationstechnischen Maßnahmen brauchen nur dann durchgeführt zu werden, wenn man den Auftrag mit Mitteln der Informationstechnologie bearbeitet. Da aber heute jeder Auftrag mit IT bearbeitet wird, und sei es nur, um den Abschlussbericht zu schreiben, sind die informationstechnischen Maßnahmen ebenfalls obligatorisch. [7]

Als organisatorische Maßnahme zur Einhaltung des Geheimhaltungsgrads VS-NfD gilt der Grundsatz „Kenntnis nur, wenn nötig“, d.h. VS dürfen nur Personen zugänglich gemacht werden, die im Zusammenhang mit der Auftragsdurchführung oder bei der Auftragsanbahnung Kenntnis erhalten müssen. Dabei ist über den Inhalt der VS generell Verschwiegenheit gegenüber Nichtbeteiligten zu wahren. Eingestufte Dokumente, Materialien und Datenträger sind deutlich sichtbar, z. B. mit „VS-Nur für den Dienstgebrauch“ am oberen Rand jeder beschriebenen Seite, zu kennzeichnen. Die VS sind in verschlossenen Räumen oder Behältern (Schränken, Schreibtische usw.) zu verwahren. Anfallendes VS-Zwischenmaterial (z. B. Vorentwürfe) ist wie VS zu behandeln. Nicht mehr benötigte VS sind so zu vernichten, dass der Inhalt nicht mehr erkennbar ist. Die Weitergabe von VS-NfD auf dem Postweg kann als gewöhnlicher Brief im einfach verschlossenen Umschlag erfolgen. Der Umschlag enthält dabei keine VS-Kennzeichnung. Weitere organisatorische Maßnahmen sind im Geheimschutzhandbuch des Bundesministeriums für Wirtschaft (BMWi) [3] dokumentiert.

Im Geheimschutzhandbuch werden auch konkrete Anforderungen an die Sicherheit der verwendeten physischen Infrastruktur gestellt, die – zumindest für „VS-Vertraulich“ oder höher eingestufte Informationen – zu erheblichen Einschränkungen und / oder Kosten führen. Dazu gehören relativ aufwendige Maßnahmen der Zutrittskontrolle, der Begleitung und Beaufsichtigung von Fremdpersonal, Vorgaben für Alarmanlagen bis hin zur Überwachung und zur Abwehr von Angriffen unter Anwendung von Waffengewalt. Räume, in denen als VS eingestufte Besprechungen durchgeführt werden sollen, sind gegen Abhören zu schützen, und eventuelle Abstrahlungen von IT-Geräten müssen durch aufwendige Filterung und Abschirmung auf das Innere von Räumen bzw. Gebäuden beschränkt werden, wenn kein ausreichender Abstand zu öffentlichen Bereichen gewährleistet werden kann („Zonenmodell“).

Auch die Beschaffung VS-geeigneter IT gestaltet sich schwierig, sobald höhere Einstufungen als VS-NfD bearbeitet werden sollen. So „ist insbesondere sicherzustellen, dass [...] Produkte mit IT-Sicherheitsfunktionen die erforderliche Zulassung aufweisen und sicherheitsgerecht implementiert werden“, und eine lückenlose Kontrolle jedes Zugriffs auf solche Produkte muss sichergestellt werden, um eventuelle Manipulationen durch Angreifer zu verhindern. Berücksichtigt man hierbei, dass sich der Prozess der Zulassung eines Produkts oft über Jahre erstreckt, so folgt daraus, dass aktuelle Produkte in der Regel nicht für eine VS-Bearbeitung eingesetzt werden dürfen, während es andererseits schwierig sein kann, zugelassene Produkte überhaupt noch zu beschaffen, weil sie inzwischen schon vom Markt verschwunden sind.

INFORMATIONSTECHNISCHE MAßNAHMEN

Ziel informationstechnischer Maßnahmen ist die zuverlässige Kontrolle aller Informationsflüsse, an denen VS-Daten beteiligt sind. Damit dies möglich ist, müssen die Maßnahmen auf verschiedenen Ebenen zuverlässig wirken. Aufbau, Konfiguration und Administration der verwendeten IT-Systeme müssen gewährleisten, dass Zugriffe auf VS-Daten nur den dafür ermächtigten Benutzern möglich sind. Dies reicht jedoch nicht aus, um den geforderten Schutz der Vertraulichkeit tatsächlich zu gewährleisten, da technische Fehler und Schwachstellen eventuell Hintertüren öffnen, die von einem versierten Angreifer ausgenutzt werden können, ggf. ohne dass der Betreiber des IT-Systems dies überhaupt merkt. Die geltenden Vorschriften tragen dieser Situation jedoch nur höchst unzureichend Rechnung, da sie noch weitgehend in einem traditionellen Bild der Informationstechnik verwurzelt sind, das heutigen technischen Strukturen nur noch teilweise entspricht, wie die folgenden Beispiele verdeutlichen.

Im Rahmen der vorgeschriebenen informationstechnischen Maßnahmen für VS-NfD sind Übersichten über Zugriffsberechtigungen zu VS zu erstellen. Nur vom Bundesamt für Sicherheit in der Informationstechnologie (BSI) zugelassene Funktastaturen und Funk-Netzwerke dürfen verwendet werden. Bei tragbaren IT-Systemen sind Speichermedien unter Verwendung BSI-zugelassener Verschlüsselungsprodukte zu verschlüsseln. Das Löschen von Datenträgern muss mit von BSI empfohlenen Produkten (mindestens 2fache Überschreibung) erfolgen. Private Informationstechnik (z. B. Laptops), Software oder Datenträger dürfen nicht für die dienstliche

VS-Bearbeitung eingesetzt werden. Eine Löschung der VS vor Wartungs- und Reparaturarbeiten ist durchzuführen, was bei heutigen Dateisystemen im allgemeinen nicht zuverlässig möglich ist, so dass die Möglichkeit von Wartungsarbeiten oft insgesamt in Frage gestellt ist, wenn kein ermächtigtes Wartungspersonal verfügbar ist.

Bei elektronischer Übermittlung außerhalb eines geschützten und örtlich zusammenhängenden LAN sind VS mit einem vom BSI zugelassenen und/oder von BMWi freigegebenen Kryptosystem zu kryptieren. Die Schlüssel sind nicht auf der Festplatte abzulegen. Hier besteht unter anderem das Problem, dass es sich bei dem für VS-NfD häufig eingesetzten Verfahren „Chiasmus“ [2] um eine symmetrische Verschlüsselung handelt, deren Schlüssel meist mehrfach, zur Verschlüsselung unterschiedlicher Dokumente, verwendet werden. Damit wird die Verschlüsselung notgedrungen angreifbar durch differentielle Kryptanalyse, ohne dass jedoch der Nachweis vorgelegt wurde, dass der verwendete Algorithmus gegen diese Art des Angriffs resistent ist. Umgekehrt ist jedoch die Nutzung gängiger hybrider Kryptoverfahren, die gegen solche Angriffe immun sind, oft ebenso wenig zugelassen wie die Verwendung allgemein genutzter Algorithmen wie AES, deren kryptographische Stärke in einem offenen Prozess nachgewiesen wurde. Damit ist es beispielsweise rein formal auch in einem abgeschlossenen Netz nicht möglich, VS-NfD geschützt über einen Web-Server zur Verfügung zu stellen, weil die zum Schutz einzusetzende SSL-Verschlüsselung nicht zugelassen ist.

Das Passwort muss mindestens 6 Stellen enthalten und aus alphanumerischen Groß- und Kleinbuchstaben bestehen – eine Regelung, die angesichts der Leistungsfähigkeit heutiger Crack-Programme eher antiquiert erscheint. Der Zugriff auf das BIOS muss mit einem Passwort geschützt sein. Das Booten des IT-Systems darf grundsätzlich nur von der Festplatte aus möglich sein. Für den Anschluss eines VS-NfD Rechners an das Internet müssen eine Firewall und ein Application Gateway vorhanden sein. VS-NfD Daten auf dem Server sind in eigener Partition bzw. einem speziell geschützter Datenbereich zu halten, ohne dass jedoch spezifiziert wird, auf welche Weise dadurch ein besserer Zugriffschutz zu erreichen ist. Je nach Umfang ist die Einrichtung eines eigenen VPN z.B. für eine Nutzergruppe oder ein Projekt erforderlich, was z.T. jedoch den kryptographischen Vorgaben widerspricht.

So detailliert diese Regelungen auch sind, verhindern sie doch nur einen Teil der möglichen Angriffe auf die Vertraulichkeit der zu schützenden Daten. Zur Abwehr von Angriffen, die sich auf technische Sicherheitslücken, beispielsweise die Möglichkeit der Ausnutzung eines Pufferüberlaufs, abstützen, ist der Einsatz vertrauenswürdiger Hard- und Software erforderlich. Dies setzt neben der Verwendung widerstandsfähiger Architekturen auch die sicherheitstechnische Überprüfung der Spezifikationen und ihrer Implementierung voraus, was jedoch meist an dem dafür erforderlichen Aufwand scheitert. Eine Evaluierung und Zertifizierung, beispielweise nach Common Criteria (ISO/IEC 15408) [4], wäre zwar für die verlässliche Verarbeitung von VS-Daten wünschenswert, wird jedoch von der Vorschrift nicht gefordert, sondern nur für bestimmte Funktionen als Alternative zu zugelassenen Produkten empfohlen.

VS-Vergehen ist Straftatbestand

So hinterlassen die für die VS-Verarbeitung geforderten informationstechnischen Maßnahmen einen eher zwiespältigen Eindruck. Einerseits werden durchaus sinnvolle Anforderungen gestellt, doch entsprechen diese in einzelnen Bereichen nicht mehr dem Stand der Technik und schaffen dadurch dort eher Unsicherheit oder schränken die Verarbeitungsmöglichkeiten unnötig ein. Der Verarbeiter ist jedoch, auch wider besseres Wissen, gezwungen, die Vorschriften im Detail zu befolgen, da sie nur an wenigen Stellen Alternativen zulassen.

Die organisatorischen und informationstechnischen Maßnahmen sind für die Bearbeitung von VS-NfD unbedingt zu beachten. Ansonsten verliert man die Berechtigung mit VS-NfD zu arbeiten. Dies bedeutet, dass man auch auf seine eigenen eingestuften Daten nicht mehr zugreifen darf. Weiterhin stellt ein solcher Verstoß gegen die o.g. organisatorischen und informationstechnischen Anforderungen einen Straftatbestand gemäß § 94 ff. StGB dar. Potentielle Angeklagte sind dabei nicht nur Personen auf der Sachbearbeiter-Ebene, sondern ggf. auch die Management-Ebene (Projektleiter, Verwaltungsleiter, IT-Verantwortliche, Sicherheitsbevollmächtigte, etc.) sowie die Leitungsebene (Geschäftsführung bzw. Vorstand) [7].

Höherstufung

In der Praxis kommt die grobe Fahrlässigkeit im Umgang mit den o.g. Maßnahmen eher selten vor. Stattdessen tritt ein anderes Szenario häufiger auf. Bei diesem besteht die Möglichkeit, dass man auch ohne eigenes Verschulden vom Zugriff auf seine eigenen Daten ausgeschlossen wird. Grundlage hierfür ist die Möglichkeit des amtlichen Bearbeiters, offene oder bereits eingestufte Daten jederzeit bei Bedarf höher einzustufen. Speziell bei

der Sicherheitsforschung ist dies häufig denkbar, da hierbei neue Erkenntnisse gewonnen werden, die unter Betrachtung der VS-Definitionen nach §4 SÜG eine geänderte Einstufung bedingen.

Eine weitere Grundlage für eine Höherstufung von VS ist mit dem § 50 Patentgesetz bzw. § 3 Gebrauchsmustergesetz gegeben. Schließt das Deutsche Patentamt bei einer Patentanmeldung die Bekanntmachung von Informationen aus, so sind diese Informationen als VS zu behandeln. Unter Umständen werden dabei auch sämtliche Rohdaten, Vorarbeiten, Entwürfe etc. des eingereichten Patents eingestuft.

In beiden Fällen erhält man einen Zugriff auf seine höher eingestuften Daten erst dann, wenn alle organisatorischen und informationstechnischen Maßnahmen des VS-Grades erfüllt worden sind. Bis zur Ausstellung der hierzu notwendigen Bescheinigung können unter Umständen mehrere Monate vergehen.

EINSTUFUNG VON NETZEN

Ein weiteres Problem besteht, wenn die höher eingestuften Daten nicht ausschließlich auf einem Stand-alone PC bearbeitet worden sind, sondern z. B. zeitweise auf einem Netzlaufwerk im Unternehmens-Netzwerk gespeichert worden sind. Dann wird auch das Netzwerk ebenfalls so eingestuft wie die am höchsten eingestuften Daten.

In diesem Zusammenhang werden üblicherweise die folgenden Begriffe verwendet:

- Man nennt den Teil des Netzes, in dem eingestufte Informationen im Klartext vorhanden sind oder waren, einen „roten“ Bereich,

- im Gegensatz zum „schwarzen“ Bereich mit kryptierten eingestuften oder unkryptierten offenen Informationen.

Alle weiteren Daten, die sich auf dem Netzlaufwerk befinden und vorher keiner Einstufung unterlagen, gehören nun ebenfalls zu diesem roten Bereich und werden wie eingestufte Daten behandelt. Das gleiche gilt auch für Storage-Systeme, Backup-Bänder, Mail- und Printserver etc., die bei einer Einstufung einzelner Daten auf ihrem System ebenfalls eingestuft und damit als Ganzes zum „roten“ Bereich gezählt werden. Somit könnte es sein, dass man auf eine Vielzahl seiner Unternehmensdaten nicht mehr zugreifen darf, obwohl nur wenige Daten nachträglich höher eingestuft worden sind.

Der Grund für diese Höherstufung auch unverfänglicher Informationen liegt darin, dass gängige Betriebssysteme, Datenbanksysteme, Anwendungs- oder Netzwerk-Software nicht in der Lage sind, Daten unterschiedlicher Einstufung sicher getrennt zu halten. Damit besteht prinzipiell die Gefahr, dass höher eingestufte Daten zusammen mit VS-NfD oder offenen Daten gedruckt oder in eine Datei kopiert werden, auch ohne dass der Bearbeiter dies will oder überhaupt bemerkt. Die Systeme werden dabei im sogenannten Betriebsmodus „System High“ gefahren, in dem die höchste Einstufung einer Information maßgebend ist für die Gesamteinstufung des Systems. Dies hat die unangenehme Konsequenz, dass auch niedrig eingestufte oder offene Daten als hoch eingestuft zu behandeln sind, sobald sie einmal in ein solches System aufgenommen wurden. Dass dies berechtigt ist, kann man sich verdeutlichen, indem man einmal ein gewöhnliches Dokument einer Textverarbeitung in Hexadezimaldarstellung betrachtet: Hier sind oft Daten enthalten, die früher in anderen Dokumenten enthalten waren, ohne dass der Bearbeiter dies in der normalen Darstellung sieht. Wer aber könnte garantieren, dass nicht eines dieser anderen Dokumente hoch eingestuft war oder noch ist?

SICHERHEITSTECHNISCHE TRENNUNG VON VS

Wenn man vermeiden will, dass auf diese Weise eine Vielzahl ursprünglich „schwarzer“ Daten auf einmal „rot“ eingefärbt wird, nur weil wenige Daten hoch eingestuft wurden, muss man für eine saubere Trennung unterschiedlich eingestufter Daten sorgen. Am einfachsten lässt sich dies dadurch erreichen, dass man ein separates System für die Bearbeitung hoch eingestufter Daten vorsieht, das keine Verbindung zu den Systemen mit normalen Daten besitzt. Selbst eine durch Firewall geschützte Netzverbindung ist nicht zulässig, da gängige Firewall-Systeme nicht in der Lage sind, Informationsflüsse nach ihrer Einstufung zu kontrollieren. [9]

Wenn sich dies als eine zu starke Einschränkung herausstellt, kann man versuchen, innerhalb der Systeme oder zwischen ihnen eine sicherheitstechnische Trennung unterschiedlicher Einstufungen durch technische Maßnahmen zu erzwingen. Eine Trennung innerhalb eines Systems lässt sich durch Übergang in den Betriebsmodus „Multi Level Security“ (MLS) erreichen, der allerdings die Verwendung von Betriebssystemen mit speziellen Eigenschaften voraussetzt. In den 80er Jahren wurden einige derartige Betriebssysteme wie Trusted Solaris,

CMW (Compartmented Mode Workstation) und SEVMS entwickelt. Diese Betriebssysteme waren durch Abstützung auf das Sicherheitsmodell von Bell und LaPadula [1] in der Lage, die Einstufung der Daten mit der Ermächtigung der Benutzer zu vergleichen und auf dieser Basis Zugriffsentscheidungen zu treffen und für eine sichere Trennung unterschiedlich eingestufter Daten zu sorgen. Die extrem komplexe Administration dieser Systeme führte jedoch letztlich dazu, dass sich dieses Konzept nicht durchgesetzt hat und dass MLS-Systeme, wenn überhaupt, heute nur noch in Nischen vorzufinden sind. Konzepte für MLS-Datenbanksysteme wurden jahrelang in diversen Forschungsarbeiten untersucht, sind jedoch an prinzipiellen Schwierigkeiten zumindest insoweit gescheitert, als sie nicht zu praktisch nutzbaren Produkten geführt haben.

Die Tendenz geht heute eher dahin, dass unterschiedlich eingestufte Daten in separaten Netzen bearbeitet werden und dass die notwendige Trennung durch Separation dieser Netze erreicht wird. Dies kann auf folgende Weise geschehen:

- Die strikteste Trennung, die für Daten der Einstufung Streng Geheim auch die einzige zulässige ist, besteht in der Verwendung von Einzelsystemen, die überhaupt nicht an ein Netz angeschlossen sind, zur Bearbeitung der hoch eingestuften Daten. Jeder Informationstransfer von und zu diesen Systemen muss manuell, etwa durch Abtippen eines ausgedruckten Dokuments oder Auslesen eines Bildschirminhalts, erfolgen. Man spricht hier von einer so genannten „Drehstuhl-Schnittstelle“.

- Eine gewisse Lockerung, die für Geheim oder Vertraulich eingestufte Dokumente üblich ist, besteht in der Vernetzung auch der hoch eingestuften Systeme in einem separaten Netz. Dies kann ein physikalisch getrenntes Netz sein, in welchem Fall jede Datenübertragung in andere Netze wieder über die Drehstuhl-Schnittstelle oder, unter Beachtung zusätzlicher Kontrollen, mit Hilfe von Datenträgern wie Disketten, CD-ROMs o.ä. erfolgt.

- Eine Alternative zur physischen Trennung kann auch die kryptographische Trennung mit Hilfe spezieller, vom BSI zugelassener Kryptogeräte sein, deren Aufbau und Funktionsweise sowohl kyptanalytische als auch technologische Angriffe erschwert. In diesem Fall werden die hoch eingestuften Daten verschlüsselt, während die niedrig eingestuften Daten im Klartext vorliegen. Da nur die für die VS-Bearbeitung vorgesehenen Systeme über Hardware zur Ver- und Entschlüsselung verfügen, kann bei vorschriftenkonformem Aufbau sichergestellt werden, dass ein unzulässiger Informationstransfer vermieden wird.

Durch diese strikte Trennung unterschiedlicher Einstufungsbereiche lässt sich zwar gewährleisten, dass hoch eingestufte Daten den für sie vorgesehenen Bereich nie verlassen, doch bleibt das Problem ungelöst, dass operationelle Erfordernisse auch Informationstransfers über Einstufungsgrenzen hinweg erzwingen können: Der General kann mit den hier beschriebenen Systemen zwar die Schlacht unter Wahrung der Geheimhaltung planen, aber er kann nie den Angriffsbefehl geben, weil er dazu Informationen an nicht ermächtigte Soldaten weitergeben müsste!

INFORMATIONSTRANSFER ÜBER VS-GRENZEN HINWEG

Dieses Problem lässt sich nur lösen, indem man kontrolliert offene bzw. VS-NfD eingestufte Daten aus dem roten Bereich in den schwarzen Bereich überführt. Dieser sichere Informationstransfer an Rot-Schwarz-Übergängen muss unter Zuhilfenahme eines Sicherheits-Gateways erfüllt werden, das an der Schnittstelle den Inhalt der übertragenen Daten kontrolliert: Es darf Informationen vom roten in den schwarzen Bereich nur dann weiterleiten, wenn es sich um niedrig eingestufte Informationen mit Geheimhaltungsgrad „offen“ oder „VS-NfD“ handelt [11]. Mit herkömmlichen Firewalls kann diese Aufgabe nicht gelöst werden, da hier die Daten lediglich anhand formaler und technischer Eigenschaften wie Absender, Empfänger sowie verwendetes Protokoll geprüft werden.

Durch eine exakte inhaltliche Kontrolle von Daten kann dabei die Prüfung sowohl manuell durch einen Benutzer als auch automatisiert erfolgen. Strukturierte Dokumente (z. B. XML-Dateien) können von einem Parser anhand eines speziellen Regelwerks (z. B. mittels XML-Schema) inhaltlich untersucht und direkt maschinell freigegeben und durch eine digitale Signatur gegen nachträglicher Verfälschung versiegelt werden. Bei dem manuellen Verfahren werden die erlaubten Dokumente nach einer Eingangsprüfung mittels eines spezifischen Anzeigeprogramms (Viewer) vollständig dargestellt und können vom Benutzer auf Vertraulichkeit untersucht werden. Wenn das Dokument keine vertraulichen Informationen enthält, wird es vom Benutzer zur Übertragung an das schwarze Netz freigegeben, in dem er dies mit einer qualifizierten digitalen Signatur bestätigt. Der Prüfarbeitsplatz kann dabei prinzipiell an einer beliebigen Stelle in das rote Netz integriert werden.

Vor der Netzgrenze müssen die signierten Dokumente einen Sicherheitsfilter passieren, der unmittelbar vor dem, die Netzgrenze schützenden, zweistufigen Sicherheits-Gateway steht und die Signatur validiert. Unter der Voraussetzung, dass alle Informationen, die aus dem „roten“ Bereich an einen Empfänger im „schwarzen“ Bereich zu übermitteln sind, durch eine digitale Signatur als freigegeben gekennzeichnet sind, kann eine zuverlässige Trennung zwischen den Bereichen erzwungen werden. Dazu überprüft der Sicherheitsfilter, ob eine gültige und zulässige digitale Signatur dieser Daten vorliegt. Wenn dies der Fall ist, wurden die Daten für den Transfer freigegeben und können somit an den „schwarzen“ Bereich übermittelt werden. Andernfalls liegt ein Sicherheitsverstoß (oder Fehler) vor, und entsprechende Maßnahmen, wie etwa das Senden einer Fehler- oder Alarmmeldung, können ergriffen werden. Die Software, die diese Überprüfung durchführt, muss vertrauenswürdig, d.h. sicherheitstechnisch evaluiert sein.

Die Sicherheit des roten Netzes vor Angriffen aus dem schwarzen Bereich sowie die exakte Kontrolle der Kommunikationsverbindungen am Rot-Schwarz-Übergang sind mit Firewall-Systemen zu realisieren, die nach CC EAL 4+ [4] zertifiziert und vom BSI zugelassen sein sollten.

Informationstransfers vom schwarzen in das rote Netz sind dagegen auf den ersten Blick unkritisch, da hier ja keine Gefahr besteht, dass hoch eingestufte Daten in ungesicherte Bereiche gelangen. Allerdings gibt es hier das Risiko unbemerkter Informationsflüsse durch den Quittungsverkehr der Netzprotokolle, der dem eigentlichen Datentransfer entgegengesetzt gerichtet ist, also aus dem roten in das schwarze Netz fließt und so zu Sicherheitsverstößen führen kann, indem er ungewollt oder beabsichtigt hoch eingestufte Daten mit sich führt. Dieser Rückkanal lässt sich nur vermeiden, indem man sich durch Einbau einer so genannten „Daten-Diode“ auf allen Ebenen der Netz-Architektur auf quittungslose Protokolle beschränkt, was bei den gängigen, TCP/IP-basierten Netzen nur schwer und mit erheblichen Leistungseinbußen möglich ist.

FAZIT

Das Gebiet des Geheimschutzes stellt aus Sicht der Informationstechnologie eine große Herausforderung dar, da die heute eingesetzten IT-Systeme und Netze nur sehr eingeschränkt in der Lage sind, die Vertraulichkeit der verarbeiteten Daten verlässlich zu schützen. Die einschlägigen Regelungen und Gesetze und die – besonders bei höheren Einstufungsgraden – sehr hohen IT-Sicherheitsanforderungen schränken derzeit die Möglichkeiten der Verarbeitung von VS-Daten nicht unerheblich ein. Eine dem Ziel des Vertraulichkeitsschutzes von VS angemessene Informationstechnik erfordert praktisch umsetzbare Vorgaben, besonders im Hinblick darauf, dass zukünftig eine Vielzahl von Unternehmen und Institutionen aus Forschung und Entwicklung erstmalig mit dem Geheimschutz in Berührung kommen wird. Hierfür ist es notwendig, dass Lösungsansätze für eine Vielzahl möglicher Problemstellungen existent und zeitnah einsetzbar sind. Bisher existieren Lösungen (als Beratungsdienstleistungen oder als IT-Produkte) oft nur für diskrete Fragestellungen. Für die Zukunft ist ihre Ausweitung auf weitere Problemstellungen notwendig sowie eine Zusammenführung aller Insellösungen wünschenswert.

LITERATUR

1. Bell D. E., LaPadula J.: Secure Computer Systems: A Mathematical Model. MITRE Corp. MTR-2547, Vol. II, Bedford MA (1973)
2. Bundesamt für Sicherheit in der Informationstechnik: Chiasmus® für Windows Version 1.7 http://www.bsi.bund.de/produkte/chiasmus/index.htm
3. Bundesministerium für Wirtschaft und Technologie: Handbuch für den Geheimschutz in der Wirtschaft (Geheimschutzhandbuch). p.8, Berlin (2004)
4. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 1, CCMB-2006-09 http://www.commoncriteriaportal.org/public/consumer
5. European Commission: COMMISSION DECISION of 2 August 2006 amending Decision 2001/844/EC, ECSC, Euratom. Official Journal of the European Union L 215/38, pp.38-43, Brüssel (2006)
6. European Council, European Parliament: DECISION No 1982/2006/EC of 18 December 2006 concerning the Seventh Framework Programme of the European Community for research, technological development and demonstration activities. Brüssel, p 5 (2006)
7. Gericke W., Thorleuchter D.: „Grundlagen des amtlichen Geheimschutzes“, Vortrag Rheinlandtreffen, sl.12, Birlinghoven (2006)
8. Bundesnachrichtendienst-Lexikon; http://cgi.bundesnachrichtendienst.de/faq/lexikon.htm
9. Loß, D.: Entwicklung/Evaluierung eines Hochsicherheits-Gateway zur Trennung verschieden eingestufter Netze. Vortrag DECUS IT-Symposium, Neuss (2006)
10. Neef, M.: Medienbruchfreie IP-basierte Bearbeitung und Übertragung von Verschlusssachen. Vortrag COMTEC 2004, sl.6, Dresden (2004)

11. Reiländer, F.: Sicherheits-Gateway für den Informationsaustausch an Rot-Schwarz-Schnittstellen. Vortrag Forum Informationstechnik der Deutschen Gesellschaft für Wehrtechnik e.V., DWT-Publikation, Bonn (2006)
12. Schavan, A: Sicherheitsforschung - Herausforderung und Notwendigkeit zum Schutz der Gesellschaft", Rede der Budesministerin für Bildung und Forschung anlässlich der Konferenz „Future Security“, p.2, Karlsruhe (2006)
13. Thorleuchter D.: „Geheimschutz in der Sicherheitsforschung“, DECUS-Bulletin, No.98, pp.24-25, München (2006)