Fraunhofer
ESK

FRAUNHOFER-INSTITUT FÜR EINGEBETTETE SYSTEME UND KOMMUNIKATIONSTECHNIK ESK

HOME GATEWAYS IN ZUKÜNFTIGEN NETZEN – DIE AUSWIRKUNG VON SDN UND NFV AUF DIE SICHERHEIT PRIVATER DATEN

Fraunhofer
ESK

FRAUNHOFER-INSTITUT FÜR EINGEBETTETE SYSTEME UND KOMMUNIKATIONSTECHNIK ESK

HOME GATEWAYS IN ZUKÜNFTIGEN NETZEN – DIE AUSWIRKUNG VON SDN UND NFV AUF DIE SICHERHEIT PRIVATER DATEN

Autoren: Mathias Leibiger, Ivan Furjanic, Thomas Messerer, Florian Krojer, Peter Handel

INHALTSVERZEICHNIS

Home Gateways in zukünftigen Netzen – die Auswirkung von SDN und NFV auf die Sicherheit privater Daten

ABBILDUNGSVERZEICHNIS

1 ZUSAMMENFASSUNG

Den zukünftigen Anforderungen an das Kommunikationsnetz hinsichtlich Einrichtung, Betrieb und der Bereitstellung von Diensten, muss u.a. mit neuen Technologien zum Netzmanagement begegnet werden. Software Defined Networks (SDN) und Network Function Virtualisation (NFV) sind aktuelle Technologien mit hohem Innovationspotential. Die Kombination beider Technologien wird das Netzmanagement vereinfachen und neue qualitativ hochwertige Dienste ermöglichen.

Die technologischen Änderungen der Infrastrukturen beim Einsatz von Software Defined Networks und Network Function Virtualisation machen vor keiner Netzkomponente halt. Daher sind nicht nur die Komponenten im Kernnetz betroffen, sondern auch die Netzübergänge zwischen den Anbietern und den Kunden, und insbesondere das **Home Gateway** (HGW).

Die neuen Möglichkeiten der Virtualisierung von Netzwerkfunktionen können dazu führen, dass zukünftig Funktionen, die aktuell lokal realisiert sind, **in die Provider-Cloud verschoben** werden. Gleichzeitig können Provider **neue Leistungsmerkmale und Dienste** schneller anbieten und das **Konfigurations- und Sicherheitsmanagement** wird vereinfacht.

Das Whitepaper zeigt die neuen Möglichkeiten SDN und NFV auf, vor allem hinsichtlich ihrer Auswirkungen auf Home Gateways. Zunächst wird dadurch eine bessere **Quality of Experience** ermöglicht. Je nach Anwendung bestimmen unterschiedliche Faktoren, ob der Endanwender den Service als hochqualitativ bewertet: Bei Online-Videospielen wird eine minimale Latenz benötigt, beim Home Office gesicherte, virtuelle Netzwerke. Mit softwaregesteuerten Kontrollmechanismen besteht für den Provider die Möglichkeit, die Verkehrsparameter des Internetanschlusses auch auf Kundenseite zu steuern, um flexibel auf die jeweils notwendigen Bedürfnisse der Anwendung zu reagieren. Da Software Defined Networks auch eine dynamische Wegewahl möglich machen, können **vertrauenswürdige Cloud Services** realisiert werden. Auch das **Smart Home Network** wird durch das neue Netzwerkmanagement sicher und komfortabel, da proprietäre Lösungen virtualisiert werden. Behält dabei der Nutzer die Kontrolle über Zugriffsrechte und Daten, steht dem Smart Home nichts mehr im Weg. Die Virtualisierung von Home Gateways bietet aber auch über den Heim-Bereich hinausgehende Chancen: Zum Beispiel können so die bisher stark abgeschotteten **industriellen Produktionsnetze** sicher geöffnet werden und die Vorteile von Industrie 4.0 werden greifbar.

Um diese Anwendungsfälle zu realisieren, ist eine internationale **Standardisierung** notwendig. Führend sind das European Telecommunications Standards Institute (ETSI) und die Open Networking Fundation (ONF). Das Broadband Forum ist in Teilbereichen aktiv. Die ETSI NFV Industry Specification Group definiert das komplette Ökosystem virtualisierter

Netzwerkfunktionen. Die Open Networking Foundation hat mit OpenFlow eine einsatzbereite Switch Spezifikation entwickelt und arbeitet an weiteren Projekten. Das Broadband Forum widmet sich unter anderem den Gateways. Im Zusammenhang mit dem erwarteten Einzug von SDN und NFV in die Telekommunikationsnetze kommt es zu einer Neudefinition von Geräten und deren Funktionen. Durch die technologische Neudefinition des Home Gatways werden Endanwender und Provider von neuen Funktionen profitieren können. Da aber noch längst nicht alle Konsequenzen der Einführung von Software Defined Networks und Network Function Virtualisation bekannt sind, widmen sich sowohl Universitäten als auch **Forschungsinstitute** diesen Themen. Forschungsbedarf besteht vor allem hinsichtlich Datenschutz und Datensicherheit, Verfügbarkeit von Funktionen und Diensten, Interoperabilität und Koexistenz sowie Hybrid-Zugangsszenarien und Multihoming mit unterschiedlichen Netzen und Anbietern.

2 FLEXIBLE NETZE BRAUCHEN NEUE HOME GATEWAYS

Der Bedarf an zukunftsweisenden Technologien und an neuartigen Kommunikationslösungen für neue Anwendungen führt derzeit zu grundlegenden Änderungen bestehender Paradigmen im Bereich der Kommunikations-Infrastruktur.

Der Executive Director des ONF, Dan Pitt, prognostiziert, dass Open-SDN (Software Defined Network) eine Voraussetzung in Ausschreibungen zwischen Netzbetreibern werden wird. Weiterhin setzen nach einer Brocade-Channel-Umfrage 18 Prozent der Befragten in EMEA bereits SDN- oder Network-Function-Virtualization-Technologien (NFV) um, während 62 Prozent SDN und NFV entweder bereits evaluieren oder dies im nächsten Jahr tun wollen.

Entsprechend einem Bericht von it-business.de sind Software Defined WAN und Netzwerkvirtualisierung zwei von zehn IT-Trends 2015: „Diese Entwicklung hat bereits in 2014 begonnen und wird sich in 2015 fortsetzen, und zwar unabhängig davon, in welchem Maßstab SDN in der Praxis eingesetzt wird. NFV ermöglicht es Service Providern, deutlich schneller und einfacher als bislang neue IT-Dienste aufzusetzen.".

Anwendungen von SDN und NFV erlauben im Vergleich zum Status Quo sowohl einen weitaus einfacheren und kostengünstigeren Betrieb der Kommunikationsinfrastrukturen als auch wesentlich vereinfachte und optimierte Verfahren zur Bereitstellung bestehender und neuer Leistungsmerkmale für die Kunden, zum Beispiel flexible kundengesteuerte VPNs.

Daher werden in den Standardisierungsgremien, speziell ETSI NFV-ISG, große Anstrengungen unternommen, den genauen Einfluss der SDN/NFV Technologie- und Paradigmen-Änderungen zu ermitteln und zu beschreiben beziehungsweise zu testen. Dadurch soll eine sanfte Migration ermöglicht werden, um die wirtschaftlichen Potenziale optimal auszuschöpfen.

2.1 Motivation: Flexibilität, Wirtschaftlichkeit und neue Anwendungen

Die Hauptaktivitäten der Gremien, der Open Source Community und großen Unternehmen konzentrieren sich auf Kernnetze und deren Optimierung durch Virtualisierung von Funktionen. In verschiedenen Use Cases und Veröffentlichungen wird eine Zukunft mit virtuellen Home Gateways „Virtual CPEs" aufgezeigt. Bei allen Vorteilen der neuen Technologien können einige, insbesondere sicherheitsrelevante Funktionen von Home Gateways nicht virtualisiert und in die öffentliche Cloud verlagert werden, sondern müssen in einer privaten Umgebung bleiben. Die Komplexität der Verteilung von Funktionen aktueller und zukünftiger Home-Gateway-Lösungen (HGW) in Verbindung mit SDN und NFV wurde noch nicht umfassend eruiert.

Im vorliegenden Dokument werden die Überlegungen festgehalten, welche die potenziellen Auswirkungen neuer SDN- und NFV-basierter Technologien auf die Netzelemente im Kundenbereich, speziell auf die Home Gateways (in bestimmten Anwendungsszenarien auch Residential Gateways [1], RGW genannt) haben können.

Die wesentlichen Beweggründe für derartige Analysen sind:

- Eine erwartete signifikante Reduktion der Betriebsaufwendungen der Netz- und Dienste-Anbieter.
- Die benötigte signifikante Steigerung der Flexibilität und der Effizienz bei der Bereitstellung der Kommunikations-leistungsmerkmale aus der Sicht der Anbieter und der Kunden.
- Auswirkungen der veränderten Aufteilung der HGW-Funktionalitäten bezüglich Kosten, Nutzen und Sicherheitsaspekten aus der Sicht der Kunden und der Anbieter.

Hierbei sind die Aspekte der Konnektivität, der Sicherheit, des Schutzes der Privatsphäre sowie der Wahlfreiheit der Anbieter und der Informationswege seitens der Kunden, aus technologischer Sicht entscheidend für eine erfolgreiche Einführung. Zusätzlich können nationale Regelungen zu Forschungs- und Anpassungsbedarf führen.

2.2 Problemstellung: Home Gateways in heutigen Netzen

Ein heutiges HGW ist meist repräsentiert durch DSL-, Mobilfunk- oder Kabelfernseh-Modems mit zusätzlichen internen Funktionen (wie Unterstützung von LAN/WLAN, VoIP/Telefoniedienst, Netz-Druckserver, Netz-Multimedia-Zentrale, etc.) und direktem Anschluss an das Zugangsnetz. Ein solches System integriert alle Funktionen beginnend mit der Terminierung einer Zugangsnetz-Leitung bis zur Unterstützung spezieller anwendungsbezogener Terminal-Funktionen– eine funktionale Trennung ist in der Regel nicht gegeben.

Die Rolle und Position eines HGWs ist oftmals durch eine starre Zuordnung zum Dienstanbieter gekennzeichnet, weil die Anbieter für bestimmte Angebote nur HGWs ihrer Wahl zulassen beziehungsweise vertreiben und unterstützen. Dies ist insofern bedeutsam, da Management-Eingriffe der Anbieter in die HGWs, aufgrund fehlender oder unzureichender Dienstgüte-Mechanismen (QoS, Quality of Service) nötig sind, um die Dienstleistungen, die sie vermarkten, auch garantieren zu können. Die Eingriffe bestehen meist aus anbieterspezifischer Steuerung der IP-Verkehre (IP Traffic Management, IPTM) zwischen den Verkehrsquellen und dem HGW-Anschluss der kundenspezifischen Endgeräte (PC/Tablet, Smart-TV, STB, etc.). Dies erfolgt durch Verkehrspriorisierung, Verkehrstrennung mittels VLAN etc.

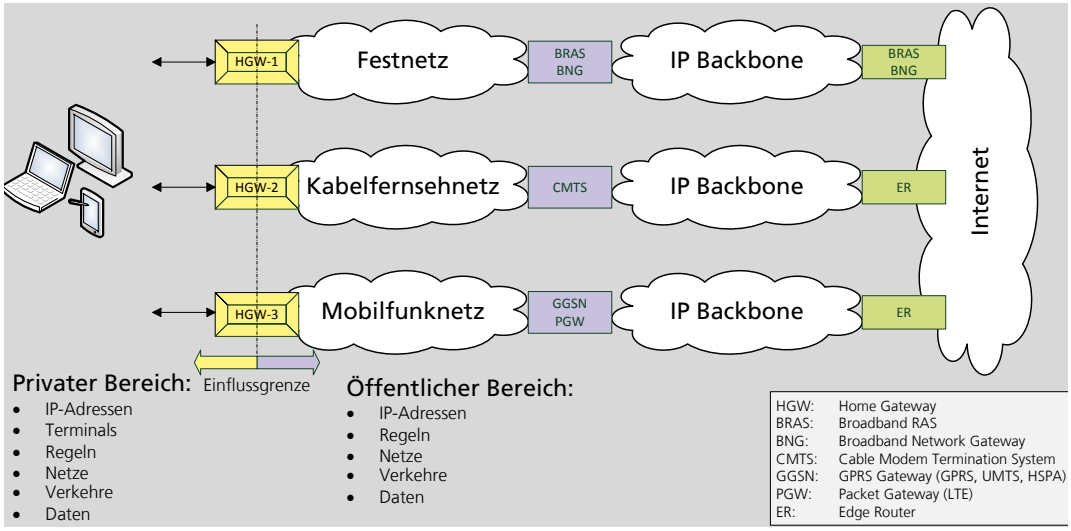

Abb.1: Home Gateways in heutigen Breitband-Kommunikationsnetzen

Die derzeitige Positionierung und Funktionsaufteilung von HGWs sind in der Abbildung 1 dargestellt. Die wesentlichen Herausforderungen bei der Neugestaltung von HGWs in den zukünftigen Netzen, ergeben sich für die möglichen Neukonstellationen und Verschiebungen der Funktionalitäten im privaten und öffentlichem Bereich (= Anbieter-Netz). Neue Anforderungen an das HGW können abgeleitet werden aus der dargestellten möglichen Verschiebung der Einflussgrenzen, an der Schnittstelle zwischen Kunde und Anbieter. Aus der sich ankündigenden Vereinheitlichung beziehungsweise vollständigen Öffnung dieser Schnittstelle ergeben sich weiterführende Szenarien, in welchen ein Home Gateway basierend auf SDN und NFV wesentliche Vorteile für alle Beteiligten im Vergleich zum jetzigen Stand aufweisen wird.

Bei der Anwendung von SDN/NFV-Technologien auf die HGWs sind resultierend unter anderem folgende Untersuchungsgegenstände von besonderer Bedeutung:

- Vor- und Nachteile der Verlagerung der privaten IP-Bereiche und Funktionen in die öffentlichen Netze
- Hybrid-Zugangsszenarien und Multihoming der Teilnehmer zu unterschiedlichen Netzen und Anbietern, sowie Umgebungen die derzeit im Rahmen von NGA-Forum (3) erarbeitet werden
- Definition von allgemein gültigen IPTM-Regeln insbesondere für HGWs
- Definition von neuen Sicherheitsstrategien im Kontext der Anbieter und der Kunden

Die vielen Funktionen heutiger HGWs erfordern eine komplexe Konfigurationsstrategie, die sowohl bei der ersten Inbetriebnahme, als auch bei Änderungen zu erheblichem Aufwand bei den Anbietern führt. Gerade im Bereich von Konfigurations- und auch Sicherheits-Management besteht die Möglichkeit, mit NFV Aufwände zu minimieren und Betriebs- und Wartungskosten zu senken. Mit SDN verbessern sich zusätzlich Flexibilität und Bereitstellungszeiten neuer Leistungsmerkmale für die Teilnehmer.

2.3 Technologie: SDN und NFV für zukünftige Home Gateways

Die Netzelemente im Teilnehmer-Zugangsbereich, insbesondere HGWs im Kunden – Heimbereich (Heimnetze, Home Network) bedürfen aufgrund vieler, noch nicht ausreichend adressierter Aspekte zusätzlicher grundlegender Untersuchungen. Die bisher veröffentlichten Konzepte und Standards hierzu besitzen bereits jetzt eine derart hohe Komplexität, dass im vorliegenden Dokument eine eigene, vereinfachte Abstraktion benutzt wird, um die Probleme mit SDN/NFV-basierten HGWs fokussierter ansprechen zu können.

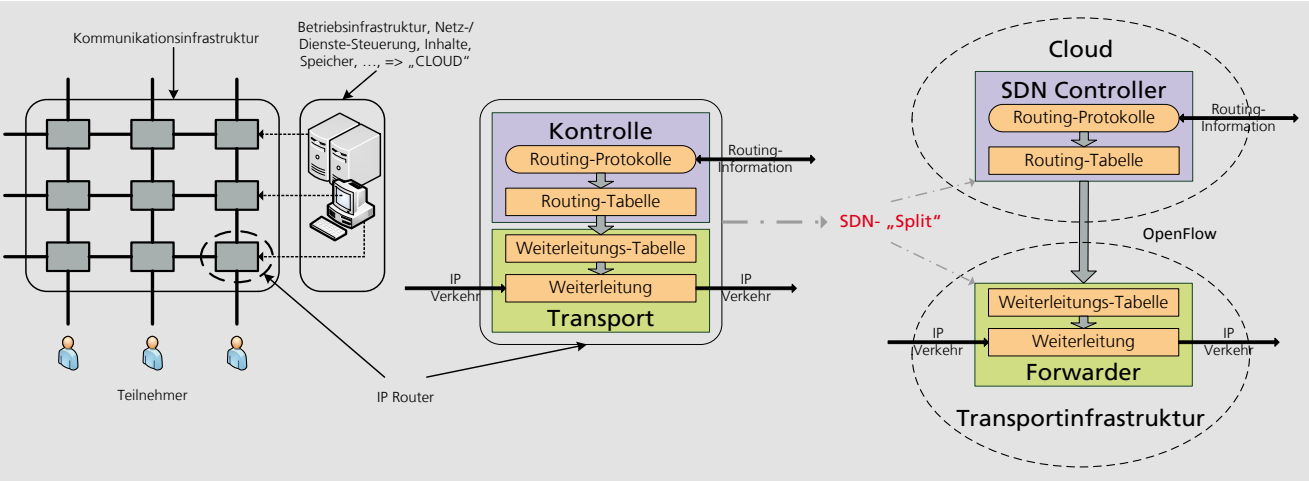

Abb.2: Anwendung von SDN

SDN (Software Defined Networks) beschreibt eine Technologie, bei der die Netz-Elemente für die IP-Verkehrs-Übermittlung beziehungsweise Behandlung (Router, Switch, Firewall, etc.) funktional und physikalisch in eine Verkehrs-Kontrollinstanz (SDN Controller, Kontrolle) und eine vom SDN Controller gesteuerte Weiterleitungs-Instanz (Forwarder, Transportinfrastruktur) aufgeteilt werden (SDN-„Split“, Beispiel siehe Abbildung 2).

Ein SDN-Controller ist hierbei als Server in einem Rechenzentrum („CLOUD“) positioniert, wogegen die Forwarder die in der Fläche verteilten steuerbaren Transportinfrastrukturelemente darstellen. Die Steuerung erfolgt durch das Protokoll OpenFlow. Die Grundfunktionalität des SDNs basiert auf der expliziten Steuerung der IP-Verkehre (IP Traffic Management, IPTM) mittels dynamisch konfigurierbarer Forwarder, wodurch sich die IP-Netze von statistischen (alleine durch Routing-Protokolle bestimmte Routen und Verhalten) in deterministische Netze transformieren.

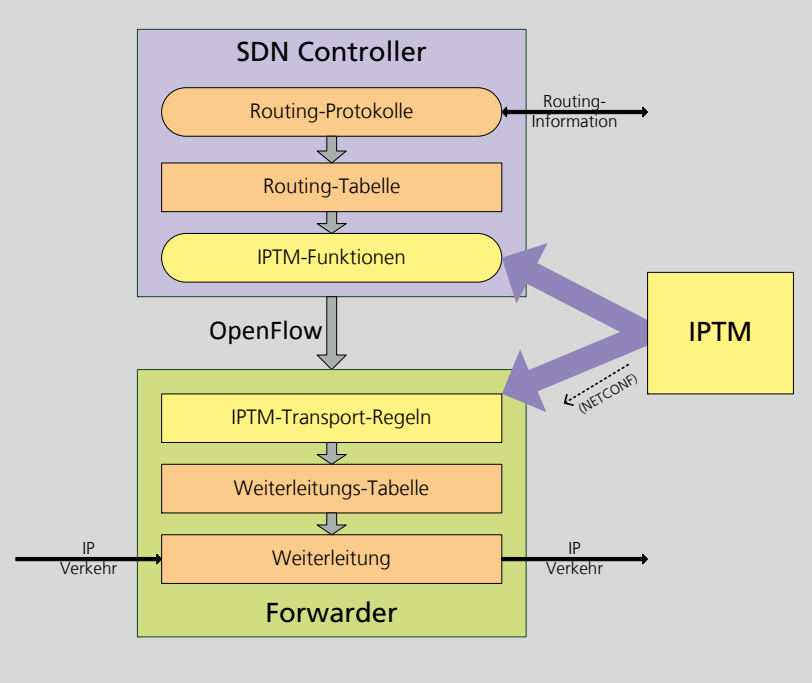

Abb.3: Rolle und Positionierung von IPTM in SDN-basierten Systemen

IPTM (IP Traffic Management) ist eine aus den Anwendungen abgeleitete funktionale Obermenge aller Maßnahmen, die IP-Verkehrs-Flüsse (IP-Flows) gezielt zu beeinflussen (Beispiel siehe Abbildung 3). Hierzu gehört die Modifizierung der Weiterleitung der IP-Flüsse entsprechend individuellen Regeln (Policy Based Routing), des Weiteren QoS/QoE-korrelierte Erweiterungen der Weiterleitungsregeln für IP-Verkehre, wie Bandbreitensteuerung, Priorisierung, Kennzeichnung und Statistiken. Ebenso gehören Filterregeln zur Nachbildung von Firewalls oder NATs zum Instrumentarium des IPTM. Mit Hilfe von IPTM können zusätzliche Weiterleitungsregeln für Inter-Operator-Schnittstellen, Multihoming-/Hybrid-Verkehrslenkung, etc. angewendet werden. Daher wird der Begriff „IPTM" in diesem Dokument breiter als üblicherweise genutzt, um den Ursachen und Auswirkungen vollständig gerecht zu werden.

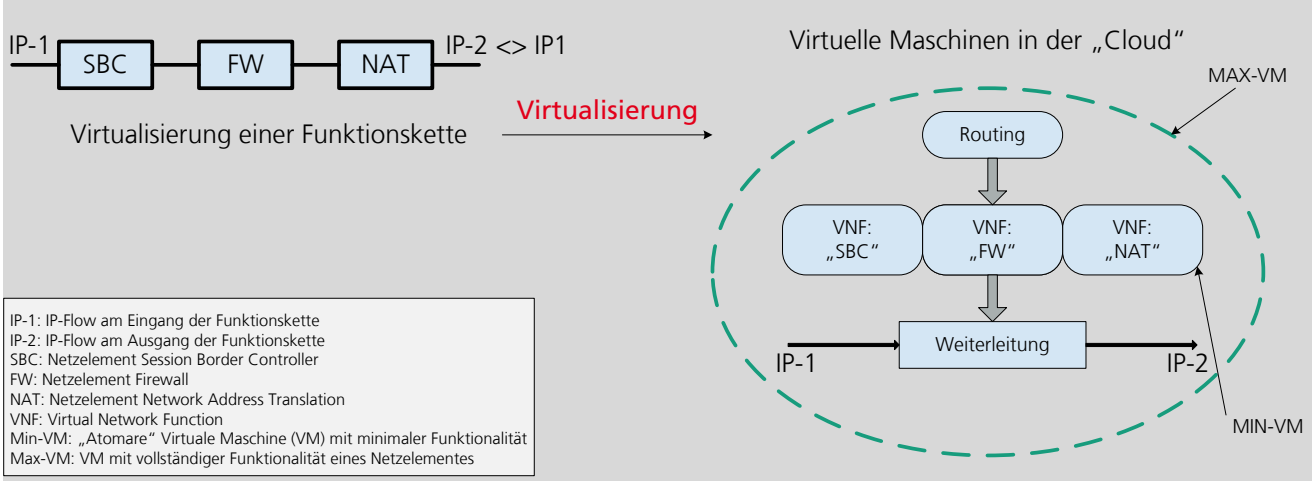

Abb.4: Beispiel eines Virtualisierungs-Prozesses anhand von „Network Service Chaining“ (Verkettung unterschiedlicher IP-Netz-Funktionen)

NFV (Network Function Virtualization) als die wichtigste technologische Neuerung in Kommunikationsinfrastrukturen, erlaubt die Eliminierung unterschiedlicher physikalischer Netzelemente und ihren Ersatz durch die Nachbildung ihrer Funktionen als ausschließlich in großen Rechenzentren („Cloud“) auf Standard-Server-Hardware ablaufenden Programmen (Beispiel siehe Abbildung 4). Die Technik der funktionalen Virtualisierung mittels Virtueller Maschinen (VM) ist ein bereits seit längerem genutztes Prinzip, die konsequente Anwendung auf die öffentliche Kommunikationsinfrastruktur ist der markante Fortschritt.

Die wesentlichen Komponenten der NFV-Technologie sind die standardisierten Schnittstellen und Verfahren zur Abbildung der Funktionen als interoperable VNF (Virtual Network Function). Die VNF können jeweils innerhalb einer VM pro IP-Flow individuell gestaltet werden. Hierbei sind entsprechend der Abbildung 4 „Max-VM“ und „Min-VM“ die lediglich in diesem Dokument gewählten Bezeichnungen für eine Vereinfachung der Lösungsdarstellung. Extrem-Beispiele dazu wären:

Max-VM (Maximal-funktionale VM) beinhaltet alle Funktionen der Layer 2 – 7 incl. Anwendungsfunktion (z.B. Routerfunktion + SBC + Firewall + NAT + Weiterleitung). Derartige VM bedingen die Durchleitung der vollständigen IP-Flows durch Höchstleitungs-Server ((2), mit z.B. 80 Gb/s Durchsatz pro Server-Blade) in der „Cloud“, wobei hier die Trennung der Kontroll- und Transportebene entsprechend SDN nicht stattfinden muss (soll).

Min-VM (Minimal-funktionale VM) beinhaltet die einfachsten/“atomaren“ VNF, wobei hier konsequent die Trennung von Kontroll- und Transportebene SDN-konform implementiert wird, da hier die Forwarder in der Fläche verteilt, aus der Cloud gesteuert werden.

Wichtig ist, dass die SDN- und NFV-Prinzipien und Implementierungen unabhängig voneinander eingeführt werden können. Jedoch werden sie aufgrund der gemeinsamen Ziele – Erhöhung der Kosten- und Betriebseffizienz der Kommunikationsnetze – und funktionalen Abhängigkeiten bei simultaner Anwendung im Netz, meist gemeinsam untersucht und definiert.

2.4 Strategie: Home Gateways in zukünftigen Netzen

Ein Anwendungsszenario der ETSI NFV-ISG ((1), Use Case #7: Virtualisation of the Home Environment), sieht vor, die Funktionalitäten des HGW in die NFV Cloud zu migrieren. Gegenstand der Virtualisierung sind die Bereiche Konnektivität, Security und Management.

Für die strukturierte Analyse findet im Folgenden die Methode der funktionalen Dekomposition Anwendung. Das HGW wird in seiner Gesamtheit als Endsystem mit abgrenzbaren Grundfunktionalitäten (Abbildung 5) betrachtet. Die Dekomposition des Endsystems erlaubt die Detailanalysen der SDN/NFV-Einflüsse und daraus resultierende Geräte- und Betriebskonzepte.

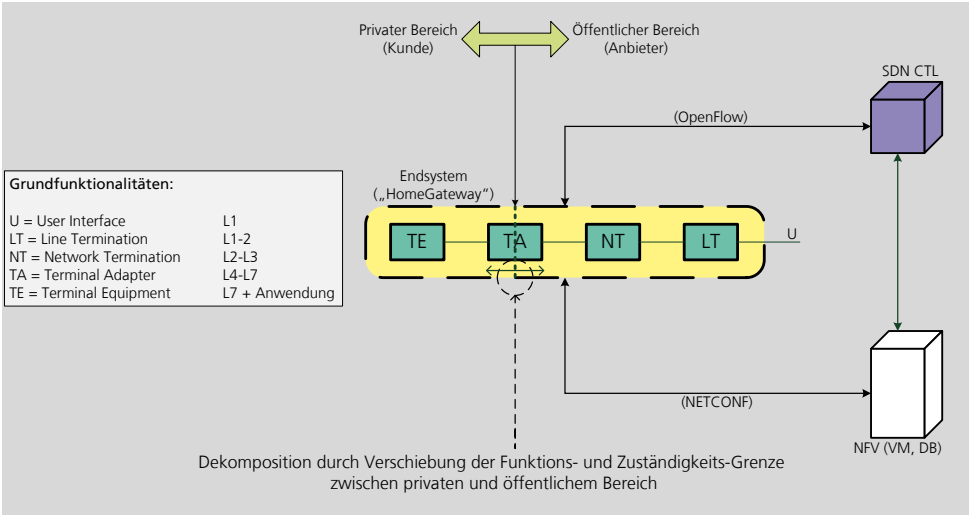

Abb.5: Modell eines HGW im Kontext von SDN und NFV

Die vielen Freiheitsgrade der funktionalen Zuordnung der SDN- und NFV-Prinzipien durch unterschiedliche logische Zerlegung des Endsystems und der Verschiebung der Grenzen zwischen privatem und öffentlichem Bereich werden deutlich sichtbar. Weiterhin beeinflussen unterschiedliche Ausprägungen und Leistungsparameter der Endgerätetypen die zu untersuchenden Konsequenzen. Die beiden folgenden Beispiele stellen die Auswirkungen anschaulich dar.

Dekomposition Beispiel 1:
Ein Mobilfunkgerät kann als Extrembeispiel eines hoch-integrierten Home Gateways verstanden werden, in dem alle L1-L7 Funktionen sowie die Anwendungen integriert sind. Hybride Zugangsfunktionalitäten, basierend auf unterschiedlichen Funktechnologien, wie LTE oder WiFi, bringen weitere Komplexität mit ein.

Dekomposition Beispiel 2:

Eine zum vorangegangenen Beispiel gegensätzliche Konfiguration stellt die Zusammenschaltung unterschiedlicher, jeweils einzeln adressierbarer Komponenten (im Sinne SDN/NFV) dar:

- LT = 1 GbE-Abschluss-Dose des Zugangsnetz-Anbieters mit integriertem L2 Switch
- NT = Netzabschluss aus der Sicht des Internet-Zugangs-Dienste-Anbieters (ISP)
- TA = STB des IPTV-Anbieters
- TE = Smart-TV/PC/Tablet/Smartphone

Nachfolgende Analyse-Schritte beinhalten Neugruppierung (= Komposition) der HGW-Funktionalitäten entsprechend dem Anwendungsfall, den Standards oder den technologischen, wirtschaftlichen und betrieblichen Gesichtspunkten. Die grundlegenden Prinzipien bei der Verlagerung der Einfluss-Grenzen zwischen privaten und öffentlichen Bereichen führen zu schwerwiegenden Konsequenzen, die einer detaillierten Untersuchung bedürfen und im Rahmen der Anwendungsbeispiele im folgenden Abschnitt eine wichtige Rolle spielen.

3 DAS HOME GATEWAY ALS SCHALTZENTRALE ZWISCHEN ANWENDERN UND NETZ – SZENARIEN

3.1 Neue Quality of Experience

Mit Hilfe neuer Technologien möchten die Anbieter ihre Betriebskosten senken und ihre Dienste schneller und flexibler anbieten. Dafür ist ein flexibles Netz- und Dienstemanagement von der Datenquelle bis zum Home Gateway notwendig.

Den Verkehr aktueller Internetzugänge übertragen die Netzbetreiber lediglich mit der Dienstgüte „Best-Effort". Dabei teilen sich die Anwendungen die Bandbreite statistisch auf, sie haben keinen Einfluss auf die Dienstgüte. Auch in den HGWs findet keine Priorisierung statt, die nutzerseitig gesteuert werden könnte. Derzeit werden zwar teilweise VoIP-Dienste vom Provider priorisiert, allerdings ohne Rücksichtnahme auf die weiteren aktiven Anwendungen der Nutzer. Vorgaben zur gleichberechtigten Übertragung der Verkehre müssen in den Lösungsarchitekturen entsprechend frühzeitig gemäß den regulatorischen Vorgaben berücksichtigt werden.

Auf Kundenseite bestehen je nach Anwendung folgende Anforderungen:

- Dynamische Bandbreiten-Steuerung auf der kundenseitigen Teilnehmerleitung, entsprechend dem momentanen Bedarf sowohl aus dem Netz zum Kunden als auch vom Kunden ins Netz
- Multimedia Streaming mit hoher Qualität
- Minimale Latenz für Online-Videospiele
- Gesicherte, virtuelle Netzwerke mit hohem Bandbreitenbedarf für Home-Office
- Weitreichende Einstellmöglichkeiten für fortgeschrittene Nutzer

Mit Kontrollmechanismen besteht für den Provider die Möglichkeit, die Verkehrsparameter des Internetanschlusses auch auf Kundenseite zu steuern, um flexibel auf die jeweils notwendigen Bedürfnisse der Anwendung zu reagieren. Für die Netzelemente ist diese Dynamik transparent, es sind keine Änderungen an den Geräten notwendig.

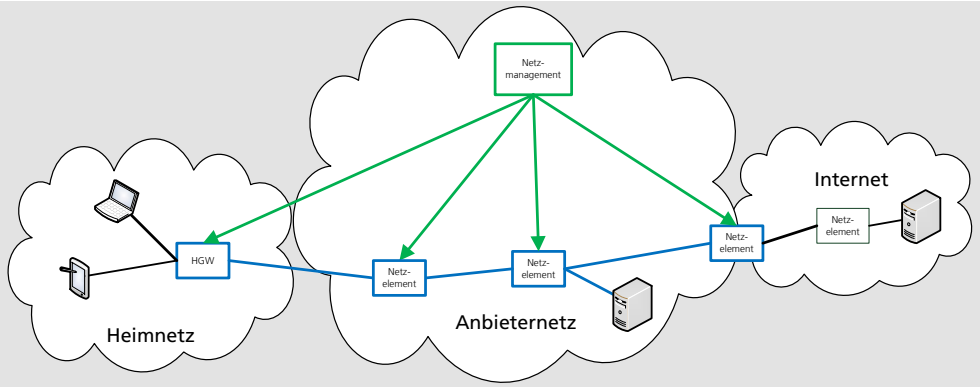

Abb.6:
Netzmanagement per SDN

Durch die in Abbildung 6 dargestellte Trennung der Transport- (blau) und der Kontrollebene (grün) können alle Netzelemente im Einflussbereich des Anbieters zentral und durchgängig administriert werden.

Mit SDN und NFV besteht für den Provider die Möglichkeit, die Verkehrsparameter des Internetanschlusses auch auf Kundenseite zu konfigurieren und zu steuern, um flexibel auf die jeweils notwendigen Bedürfnisse der Anwendung zu reagieren. Dem Provider wird die Administration auch einer großen Anzahl von Endgeräten wesentlich erleichtert.

Damit ist bei der Einführung von SDN und NFV für die HGWs von entscheidender Bedeutung, ein dynamisches IPTM zwischen den Anwendungen und den Servern zu implementieren – ohne dies kann eine Steigerung von QoE nicht konsequent erreicht werden.

Mit SDN entstehen adaptive Netze, die sich an die Anforderungen der Nutzer anpassen. Leistungsfähige User-Interfaces unterstützen sie bei der Einrichtung und beim Betrieb.

3.2 Vertrauenswürdige Cloud Services

Öffentlich verfügbare Cloud Services sind aus dem alltäglichen Leben kaum mehr wegzudenken; die Anwender können Daten mit verschiedenen Endgeräten von verschiedenen Orten aus nutzen, oder über das Internet Daten mit anderen Nutzern teilen. Bei vielen aktuellen Cloud Services muss der User jedoch die Kontrolle über seine Daten weitgehend aufgeben. Zudem ist das Angebot an Cloud Services schwer zu überblicken, und noch schwieriger hinsichtlich der Sicherheit zu bewerten.

Mit Hilfe privater Cloud Services in seinem lokalen Netz kann der Nutzer die Kontrolle über seine Daten selbst ausüben. Dabei ist er aber auch selbst für die Sicherheit und Verfügbarkeit der Plattform und der darauf gespeicherten Daten verantwortlich. Durch die Kombination von dynamischer Wegewahl per SDN und virtualisierten Cloud-Funktionen kann er die Kontrolle über seine Daten in zukünftigen HGWs zurückerlangen.

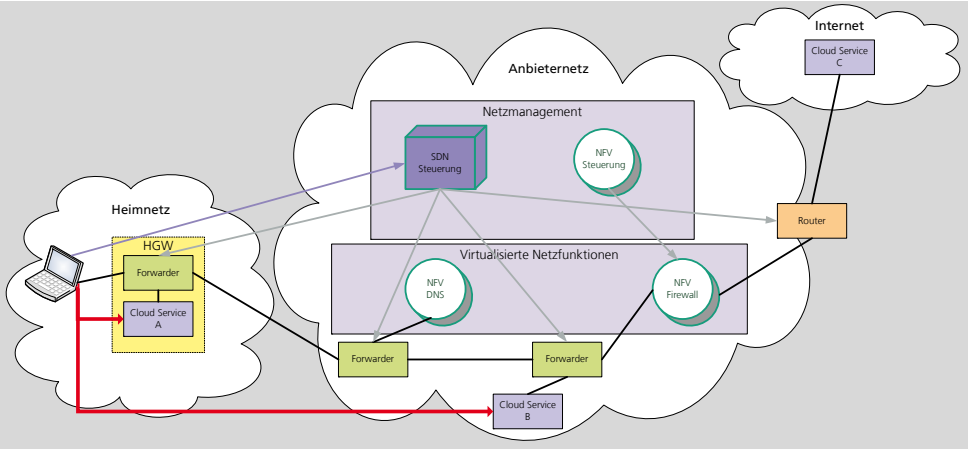

Abb.7: HGW als flexibles Portal zu Cloud Services

Über ein Benutzerinterface kann der Nutzer auswählen, ob er den Cloud Service eigenverantwortlich betreiben (Fall A), oder die Daten beim Provider lagern will (Fall B). Das Forwarding leitet die Benutzerzugriffe je nach Konfiguration auf den lokalen Cloud Service im HGW um, oder leitet die Anfragen transparent zum Provider weiter.

Im Falle des Cloud Services C kann über das Benutzerinterface des HGW und das Netzmanagement des Anbieters auch noch die in der Anbieter Cloud virtualisierte Firewall angesteuert werden. Dann können genau auf die Anforderungen abgestimmte Sicherheitsregeln konfiguriert, und über SDN ein durchgängiger Pfad bis zum Anwender hin geschaltet werden.

Mit Hilfe der neuen Technologien kann dies mit hohem Bedienkomfort realisiert werden. Neue Schnittstellen zu Cloud-Technologien im Home Gateway bieten etwa:

- Zentrales Portal auf dem Home Gateway für den Zugriff auf private (lokale) und öffentliche Cloud Services
- Zugangspunkt zu vertrauenswürdigen Diensten des eigenen Anbieters oder im Internet
- Eigene private Cloud als integraler Bestandteil der familiären und öffentlichen Vernetzung
- Sicherer Zugriff auf die eigenen Daten aus dem Internet
- Freigabe von Daten an Dritte, einheitliche Verwaltung von Zugangsrechten
- Globales Sinlge-Sign-On und Authentifizierung für Internetdienste

Die zukünftigen Entwicklungen adressieren neben der definierten, d.h. nutzergesteuerten Ablage der eigenen Daten vor allem auch die Vertraulichkeit und Integrität der privaten Datenbestände. Die private Cloud ermöglicht eine bedarfsgerechte Dezentralisierung in Abhängigkeit von den Erwartungen und Bedürfnissen der Nutzer.

3.3 Smart Home mit „Smart Network“

Zukünftige HGWs können verschiedene Heimautomatisierungs-Netze integrieren und mit diesem Ansatz komfortable Smart-Home-Lösungen anbieten. Bei Bedarf können ergänzend externe Anbieter eingebunden werden.

Im Bereich der Heimautomatisierung bestehen derzeit vielfältige, dezidierte Insellösungen, mit inhärenten Nachteilen für die Interoperabilität. Neben den meist auf Funklösungen basierenden Verfahren, finden vermehrt PLC-Installationen Eingang in die Steuerungszentralen der Hausanlagen. Derartige Lösungen müssen oftmals von Fachpersonal programmiert werden. Zukünftige HGWs können verschiedene Heimautomatisierungs-Netze anbinden und integrieren.

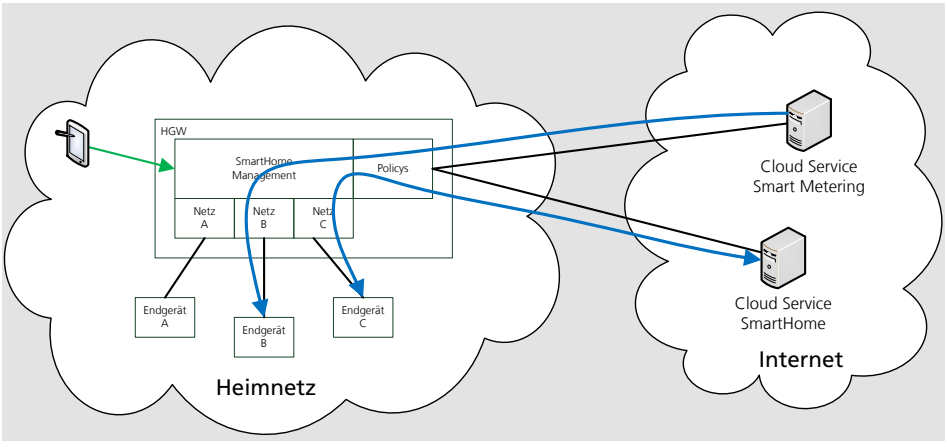

Abb.8:
HGW als Steuerungszentrale

Die neuen Home Gateways werden damit die Implementierung von Heimautomatisierungssystemen deutlich vereinfachen. Bei HGWs mit minimalem Funktionsumfang kann die Heimautomatisierung auch in ein externes Beistellgerät ausgelagert werden, über die SDN- und NFV-Mechansimen kann es nahtlos in das HGW eingebunden werden. Falls gewünscht, können Smart Home Funktionen auch im Internet virtualisiert werden, oder Funktionen aus dem Internet dynamisch in das lokale System eingebunden werden.

Virtualisierte Lösungen hätten folgende Vorteile:

- Nutzung von Smart Home Funktionen auf dem Home Gateway, mit transparenter Einbindung von Cloud Services durch SDN/NFV
- Freigabe von Ressourcen im Heimnetz über Policies
- Automatisierung von Steuerungsvorgängen im Haus, zum Beispiel nächtliches Lüften im Sommer, in Abhängigkeit von den Temperaturen und der Luftqualität, unter zusätzlicher Beachtung der Pollenvorhersage für Allergiker
- Steuerungszentrale für die Heimautomatisierung integriert verschiedene physikalische Netze, vor allem PLC und Funk
- „Out-of-the-Box" Sensoren / Aktoren zur einfachen Installation durch den Nutzer oder alternativ zur Installation und Konfiguration durch den Fachmann

Gerade im sensiblen Heimbereich werden nicht nur einfach zu bedienende, sondern vor allem sichere Lösungen benötigt. Dies bezieht sich sowohl auf die Betriebssicherheit, als auch auf den Zugriffsschutz. Zukünftig können Dienstleister im Internet auch Anwendungen für die Heimautomatisierung anbieten. Über Zugriffsregeln bestimmt der Anwender selbst, auf welche Bereiche welcher Dienstleister zugreifen und worauf nur lokal zugegriffen werden darf.

Vor allem bei PLC-Installationen ist davon auszugehen, dass die Basishardware wie alle Elektroinstallationsarbeiten und die erste Konfiguration auch zukünftig vom Fachmann durchgeführt werden. Die nachfolgenden Änderungen sollen zukünftig aber auch vom Anwender selbst durchgeführt werden können.

Die neuen Netzwerktechnologien können dafür die entscheidenden Impulse liefern, weg von proprietären Ansätzen, hin zu transparenter und vertrauenswürdiger Vernetzung.

3.4 Anwendungsfall industrielle Produktionsnetze

Die in diesem Papier konzipierten Ansätze für ein Aufbrechen der Funktionen (Dekomposition) eines HGW in virtualisierbare Module und die Anwendung von SDN und NFV Technologien für Konfiguration und Betrieb von solchen Gateways in künftigen Netzen lassen sich auch auf den Anwendungsfall der industriellen Produktionsnetze erweitern.

Bislang nach außen stark abgeschottete Netze von industriellen Automatisierungs- und Produktions-Kontrollsystemen (engl. Industrial Automation and Control Systems, IACS) werden im Zuge der zunehmenden Vernetzung ihrer Komponenten mit anderen Produktionsanlagen, mit den Maschinenherstellern, wiederum deren Zulieferern und weiteren Teilen der Wertschöpfungskette für die Kommunikation nach außen in Zukunft geöffnet werden müssen.

Diese Entwicklung ist unter den Begriffen Internet of Things (IoT), Cyber Physical Systems (CPS) oder in Deutschland „Industrie 4.0“ bekannt.

Dabei entstehen vor allem für die IT-Sicherheit mit klassischen Mitteln schwer beherrschbare Herausforderungen [4], da hier eine komplexe Landschaft von Protokollen und zum Teil gänzlich andere Prioritäten bei den Schutzzielen, als von der normalen Office-IT gewohnt, gehandhabt werden müssen.

Es ist zu erwarten, dass sich SDN- und NFV-basierte Technik für Konfiguration, Wartung oder auch Simulationstests der dafür erforderlichen Security-Appliances (etwa Gateway- , Firewall-, Datendioden- oder DPI-Funktionalität) als außerordentlich nützlich erweisen wird. Dabei steht im Mittelpunkt, die sogenannten „Conduits“ zu managen. Das sind die Übergänge sowohl zwischen den internen Zonen und Zellen eines Produktionsnetzes, dem Produktionsnetz und dem internen-Office Netz, als auch Anbindungen nach außen, zu anderen Standorten und Partnerfirmen im In- und Ausland.

Zu den zentralen Anforderungen eines solchen Netzes gehört es, dass es möglich sein muss, bestimmte Conduits sehr flexibel anzupassen, gleichzeitig muss dabei das Risiko einer Fehlkonfiguration, die letztlich zur Beeinträchtigung der Verfügbarkeit einer Produktionsanlage führen kann, auf ein absolutes Minimum reduziert werden. Diese Anforderung lässt sich komfortabel mittels SDN und NFV erfüllen.

HOME GATEWAY EVOLUTION

4.1 Standardisierung

An der Standardisierung von SDN und NFV wird in verschiedenen Gremien gearbeitet. Führend sind das European Telecommunications Standards Institute (ETSI) und die Open Networking Foundation (ONF). Das Broadband Forum ist in Teilbereichen aktiv. Im folgenden Kapitel wird ein Überblick über die Gremien und die jeweiligen Aktivitäten gegeben.

Die Open-Source-„Gemeinschaft" (auch vertreten durch führende Gerätehersteller) erzeugt stetig neue ergänzende Spezifikationen zu SDN und NFV. Die Leitlinien hierzu sind:

- Konsequente Transformation der bestehenden Kommunikationsinfrastruktur in reine IT-Technologie/ „Programme" basierend auf Open Source und offenen Standards.
- Nahtlose Migration der bestehenden Kommunikationsinfrastrukturen und Dienste.

Nachfolgend wird auf die Organisationen, Open-Source-„Gemeinschaften" und Industriegremien eingegangen, die im Bereich SDN und NFV aktiv sind. Diese sind in der Abbildung 9 dargestellt.

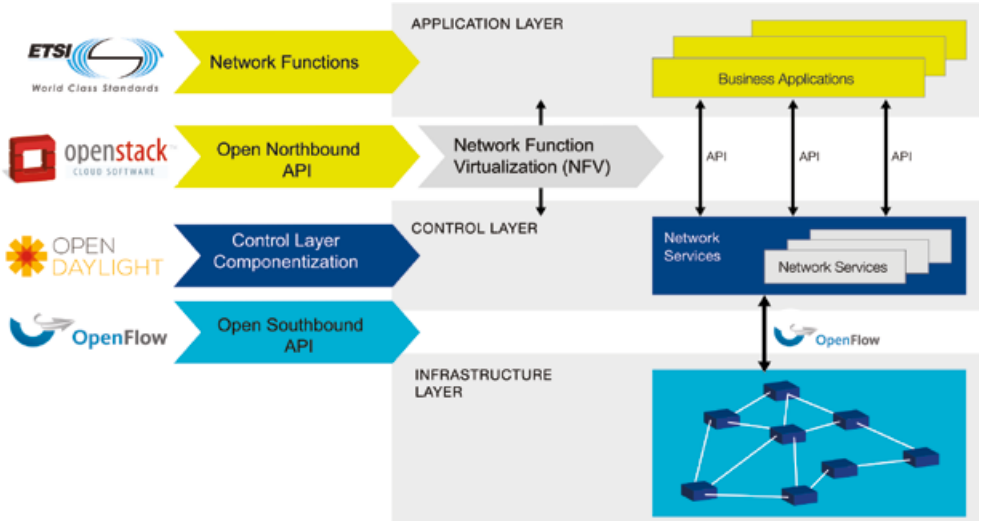

Abb.9: Einordnung wichtiger Organisationen im Kontext von SDN und NFV [5]

ETSI NFV-ISG (ETSI NFV Industry Specification Group) [6] arbeitet mit dem Hauptziel, das vollständige Ökosystem virtualisierter Netzwerkfunktionen zu definieren (White Paper, [3]). Die gesamte Arbeit entspricht einem vollständigen Design eines neuen Kommunikationsnetzes, bei dem alle Aspekte, funktionale wie betriebliche, im Detail beschrieben werden.

Hierzu werden mehrere Dokumente erzeugt [6], davon die wichtigsten:

- Anwendungsszenarien für NFV (NFV Use Cases document [1]), in welchen die Initial-Anwendungen analysiert werden. Hier sind die jeweils charakteristischen technologischen Herausforderungen maßgeblich, um die Rolle von NFV zu adressieren.
- Anforderungen (NFV Requirements document [7]) an ein NFV Rahmenmodel (NFV Framework) aus geschäftlicher und technischer Sicht.
- NFV Architektur-Rahmenmodell (NFV Architectural Framework document [8]) das die funktionale Architektur, Design-Philosophie virtualisierter Netzfunktionen (VNF) zusammen mit der Virtualisierungs-Infrastruktur beschreibt.
- NFV-Terminologie (NFV Terminology document [9]) als die Sammlung aller Begriffe, die im NFV benutzt werden.
- Funktionsnachweis des NFV-Konzeptes (NFV Proof of Concept Framework document [10]) mit dem Anspruch, auf globaler Basis (da alles ein Open Source Werk ist) die NFV-Annahmen und Implementierungen zu validieren.

Die **Open Networking Foundation (ONF)** ist ein Industriegremium und gilt als die derzeit führende Gruppierung zur Definition von SDN (ONF, White Paper [11]). Der Schwerpunkt der Aktivitäten liegt auf dem Kontrollprotokoll **OpenFlow**. Die OpenFlow Switch Spezifikation, die aktuell in der Version 1.4.0 (Stand Oktober 2013) vorliegt, hat bereits einen hohen Reifegrad erreicht, sodass es aktuell mehrere Hersteller mit OpenFlow-kompatiblen Switchen am Markt und im Einsatz gibt.

Open Daylight [12] ist als ein Open-Source-Projekt eine modulare und flexibel erweiterbare Kontroll-Plattform implementiert als reine Softwarelösung, basierend auf der Programmiersprache Java. Das Softwarepaket bietet eine Schnittstelle (Northbound API) zum OSGI Framework und zu NFV Funktionen im OpenStack. Weitere Schnittstellen (Southbound API) ermöglichen die Einbindung verschiedener Protokolle wie OpenFlow 1.0, OpenFlow 1.3 oder BGP-LS. Das erste Open Daylight Release trug den Namen Hydrogen (veröffentlicht im Februar 2014), aktuell ist das Release Helium (Stand November 2014).

OpenStack [13] als ein Open-Source-Projekt ist ein Cloud-Operating-System (COS) basierend auf globaler Zusammenarbeit von Entwicklern und Technologen. Das entwickelte Betriebssystem ermöglicht über die „Dashboard"-Oberfläche die Kontrolle verschiedener Speicher-, Rechenleistungs- und Netzwerkressourcen. Diese drei Ressourcen werden als einzelne Teilprojekte geführt. Dabei beschäftigt sich „OpenStack Compute" mit Einrichtung und Management von Netzwerken virtueller Maschinen, „OpenStack Storage" mit der Speicherung von Objekten, Datenblöcken für Applikationen und Servern und letztlich „OpenStack Networking" mit einem skalierbaren API-orientierten Netzwerk und IP Management.

Das **Broadband Forum** [14] arbeitet auch an verschiedenen Projekten im Bereich SDN und NFV. Hinsichtlich NFV arbeitet das Forum eng mit der NFV-ISG der ETSI zusammen. Konkrete Arbeitsthemen des Broadband Forum (deren Ergebnisse als Technischer oder Marketing Report veröffentlicht werden) sind die nachfolgend beispielhaft aufgelisteten Standardisierungsprojekte:

- WT-317 Network Enhanced Residential Gateway architecture (partial virtualizing of RG functions)
- WT-328 Virtual Business Gateway
- WT-345 Migrating to NFV in the context of TR-178 (the current Multi-Service Broadband Network – MSBN)
- SD-313 SDN in Broadband Networks (high level requirements and a framework for)
- SD-340 Introducing NFV into the MSBN (Multi-Service Broadband Network)

Wie aus den dargestellten Standardisierungsaktivitäten erkennbar ist, wird SDN und NFV neben Gremien wie der ETSI auch intensiv von Open-Source-Aktivitäten vorangetrieben. Die Open-Source-„Gemeinschaft" (in der sich auch führende Gerätehersteller engagieren) erzeugt stetig neue ergänzende Spezifikationen und Softwarepakete.

Der aktuelle Stand der Spezifikationen, zusammen mit bereits verfügbaren Lösungen, erlaubt einen Einsatz von SDN und NFV in Testnetzen. Weitergehende Betrachtungen hinsichtlich der Home und Business Gateways sind aktuell nur aus dem Broadband Forum bekannt und somit ein noch offenes Arbeitsfeld.

4.2 Forschungsaktivitäten

Forschung zum Thema SDN und NFV findet an zahlreichen Universitäten und außeruniversitären Einrichtungen statt. Nahezu jeder Lehrstuhl für Kommunikationsnetze weltweit beschäftigt sich heute mit diesen Technologien. Aus dem außeruniversitären Bereich ist in Deutschland vor allem das Fraunhofer FOKUS (mit OpenSDNCore) zu nennen. Forschungsprojekte zu den Themen SDN und NFV gibt es dementsprechend weltweit in allen industrialisierten Ländern.

Auf EU-Ebene nimmt die IKT-Forschung sowohl im abgelaufenen Rahmenprogramm FP7 als auch im jetzt anlaufenden Rahmenprogramm „Horizon 2020" einen breiten Raum ein. Im Jahr 2008 wurde die Future Internet Assembly (FIA) [15] gegründet, um die Zusammenarbeit von Forschungsprojekten insbesondere aus den EU-Forschungs-Rahmenprogrammen (derzeit ca. 150) mit dem Ziel zu koordinieren, die europäischen Aktivitäten zur Stärkung der Wettbewerbsfähigkeit Europas bei der Entwicklung des zukünftigen Internets zu stärken.

Auf der Jahreskonferenz 2014 in Athen [16] bildeten SDN und NFV den zentralen Schwerpunkt.

Auch auf nationaler Ebene werden sowohl vom Bundesministerium für Bildung und Forschung (BMBF, Programm „IKT 2020 - Forschung für Innovation") als auch vom Bundesministerium für Wirtschaft und Energie (BMWi, „Internet der Zukunft"), entsprechende Forschungsvorhaben gefördert.

Nahezu alle diese Forschungseinrichtungen und Verbundprojekte beschäftigen sich jedoch vornehmlich mit den grundlegenden Prinzipien von SDN und NFV, mit der Realisierung in den Core-Netzen der Telekommunikationsnetz-Betreiber und mit dem Aspekt der „Cloud Connectivity".

Der Erforschung der Auswirkungen und des Nutzens dieser Technologien an der Schnittstelle zum Endnutzer und auf dessen Seite wurde im Rahmen dieser Forschungsaktivitäten bisher nur begrenzte Aufmerksamkeit gewidmet. Selbst in der „NFV Research Agenda" („ISG NFV proposed topics for Research Agenda 2014") der ETSI NFV-Gruppe [17] wird der Access- und Endnutzer-Bereich nicht explizit thematisiert. So gibt es derzeit nur vereinzelte wissenschaftliche Projekte, beispielsweise über „Virtual CPE" [18], [19], in denen in diesem Bereich geforscht wurde.

4.3 Forschungsthemen

Bei der durch die Einführung von SDN- und NFV-Technologien im Bereich der Home Gateways nun möglichen neuen Aufteilung der Funktionen zwischen privater und öffentlicher Vertrauensdomäne müssen vor allem deren Auswirkungen auf die folgenden Fragenkomplexe näher untersucht werden

- Datenschutz und Datensicherheit
- Interoperabilität und Koexistenz
- Hybrid-Zugangsszenarien und Multihoming mit unterschiedlichen Netzen und Anbietern

Datenschutz und Datensicherheit

Dies betrifft vor allem den Schutz der Privatsphäre und von personenbezogenen Daten bei einer Verlagerung von Funktionen aus der privaten Vertrauensdomäne in diejenige von Netzbetreibern.

Es ist zu klären, auf welche Parameter einer virtualisierten Funktion dem Teilnehmer Einfluss zugestanden wird. Darf der Netzbetreiber seinerseits vom Teilnehmer vorgenommene

Sicherheitseinstellungen verändern und wie kann die Einhaltung entsprechender Regelungen technisch sichergestellt werden?

Wem gehören die Daten auf einem NFV-Server? Wer trägt welche Verantwortung für die Einhaltung von Datenschutzbestimmungen und wie kann diese von Betroffenen überprüft werden? Wie kann die Sicherheit der Daten unterschiedlicher privater Nutzer auf einem Virtualisierungs-Server gewährleistet werden? Welche regulatorischen Vorgaben sind einzuhalten und neu zu treffen?

Interoperabilität und Koexistenz

SDN/NFV-basierte HGW-Lösungen und herkömmliche Technik müssen für eine Übergangsphase parallel betrieben werden und zusammenwirken können. Mit NFV können Netzfunktionalitäten vom HGW ins Providernetz verlagert werden, sodass sich neben den HGW unter Umständen auch die Endgeräte vereinfachen. Gleichzeitig müssen jedoch vorhandene Endgeräte weiter betrieben werden können. Es sind daher Mechanismen zu erarbeiten, mit denen die Interoperabilität zwischen alten und neuen Endgeräten und HGWs hergestellt werden kann. Nicht zuletzt bedarf es auch eines Konzeptes für eine Migrationsstrategie zur Einführung dieser Technologien. Hier muss untersucht werden, wie die hergebrachte Technik und eine neue SDN/NFV-basierte Technik im Anschlussbereich zeitweilig koexistieren können, ohne dass die Vorteile der neuen Technik für die Betreiber verlorengehen.

Hybrid-Zugangsszenarien und Multihoming mit unterschiedlichen Netzen und Anbietern

Die bedarfsgerechte Steuerung von Verkehrsparametern wird Heimnetze und Internetzugänge hervorbringen, die sich an den Bedürfnissen der Nutzer orientieren. Die Provider können ihren Kunden optimale Dienste anbieten. In Dual-Access Szenarien kann die Auswahl des zu nutzenden Internetzugangs abhängig von den Anforderungen der Anwendung oder abhängig von eventuellen Volumenbegrenzungen der einzelnen Zugangswege erfolgen. Provider könnten die Wegewahl auch ausgehend von den Auslastungen ihrer Netze steuern, um so bestimmte Netze oder Netzbereiche gezielt zu entlasten.

Hier müssen auch Regelungen und technische Methoden gefunden werden, um den unterschiedlichen Betreibern einen Zugriff auf die Konfiguration der sie betreffenden Daten im virtualisierten HGW zu erlauben, ohne mit den jeweils anderen zu interferieren. Dazu gehört neben der Definition auch die Verifikation von IPTM-Regeln, die in genau solchen Szenarien auftreten.

REFERENZEN

[1] ETSI GS NFV 001. Network Functions Virtualisation (NFV); Use Cases. [Online] V1.1.1, Oktober 2013. http://docbox.etsi.org/ISG/NFV/Open/Published/.

[2] ETSI. Network Functions Virtualisation - Whitepaper #3. [Hrsg.] SDN & OpenFlow World Congress. Düsseldorf : ETSI, 14.-17. Oktober 2014.

[3] Bundesnetzagentur - Aktuelle Dokumente. [Online] http://www.bundesnetzagentur.de/cln_1411/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Breitband/NGA_NGN/NGA-Forum/Aktuelle%20Dokumente/aktuelledokumente-node.html.

[4] Junker, Holger. Lernen aus Industrie 3.0 und Weiterdenken in Industrie 4.0. [Hrsg.] Jürgen Jasperneite und Ulrich Jumar. Jahreskolloquium Kommunikation in der Automation (KommA 2014). Nov. 2014.

[5] ETSI - NFV. [Online] http://www.etsi.org/technologies-clusters/technologies/nfv.

[6] ETSI. docbox.etsi.org. [Online] http://docbox.etsi.org/ISG/NFV/Open/.

[7] ETSI GS NFV 004. Network Functions Virtualisation (NFV); Virtualization Requirements. [Online] V1.1.1, Oktober 2013. http://docbox.etsi.org/ISG/NFV/Open/Published/.

[8] ETSI GS NFV 002. Network Functions Virtualisation (NFV); Architectural Framework. [Online] V1.1.1, Oktober 2013. http://docbox.etsi.org/ISG/NFV/Open/Published/.

[9] ETSI GS NFV 003. Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV. [Online] V1.1.1, Oktober 2013. http://docbox.etsi.org/ISG/NFV/Open/Published/.

[10] ETSI GS NFV-PER 002. Network Functions Virtualisation (NFV); Proof of Concepts; Framework. [Online] V1.1.1, Oktober 2013. http://docbox.etsi.org/ISG/NFV/Open/Published/.

[11] Open Networking Foundation. Software-Defined Networking: The New Norm for Networks. [Online] 13. April 2012. https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf.

[12] OpenDaylight - A Linux Foundation Collaborative Project. [Online] http://www.opendaylight.org/.

[13] OpenStack - Open Source Cloud Computing Software. [Online] http://www.openstack.org/.

[14] Broadband Forum. [Online] https://www.broadband-forum.org/.

[15] Future Internet Assembly (FIA). Future Internet Assembly (FIA) Homepage. [Online] [Zitat vom: 08. 12 2014.] http://www.future-internet.eu/home/future-internet-assembly.html.

[16] Future Internet Assembly (FIA). FIA Conference Athens 18-20/03/2014. [Online] [Zitat vom: 08. 12 2014.] http://www.future-internet.eu/home/future-internet-assembly/athens-mar-2014.html.

[17] ETSI NFV ISG. ISG NFV proposed topics for Research Agenda 2014. [Online] [Zitat vom: 09. 12 2014.] https://portal.etsi.org/Portals/0/TBpages/NFV/Docs/NFV_Research_Agenda_2014.pdf.

[18] Hansen, Ole Frendved, et al., et al. OpenNaaS and Virtual CPE: a new way to connect to the Internet. [Online] http://www.opennaas.org/wp-content/uploads/2013/08/vCPE-Paper.pdf.

[19] Minoves, Pau, et al., et al. Virtual CPE: Enhancing CPE's deployment and operations through Virtualization. [Hrsg.] IEEE. IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom), 2012. 3-6. Dec. 2012, S. 687 - 692 .

[20] LMU München; Forschungsverbund Intelligente Infratrukturen und Netze. 29. 08 2014. Informations- und Kommunikationstechnologien als Treiber für die Konvergenz Intelligenter Infrastrukturen und Netze – Analyse des FuE-Bedarfs, Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie, Schlussbericht.

GLOSSAR

API	Application Programming Interface
CPE	Customer Premises Equipment
CPS	Cyber Physical Systems
DPI	Deep Packet Inspection
DSL	Digital Subscriber Line
EMEA	Wirtschaftsraum Europa (Europe), Naher Osten (Middle East) und Afrika (Africa)
ETSI	European Telecommunications Standards Institute
ETSI NFV-ISG	ETSI NFV Industry Specification Group
FIA	Future Internet Assembly
HGW	Home Gateway
IACS	Industrial Automation and Control Systems
IoT	Internet of Things
IP	Internet Protocol
IPTM	IP Traffic Management
ISP	Internet Service Provider
JVM	Java Virtual Machine
IKT	Informations- und Kommunikationstechnik
IT	Informationstechnik
LAN	Local Area Network
LT	Line Termination
LTE	Long Term Evolution
MSBN	Multi-Service Broadband Network
NAT	Network Address Translation
NFV	Network Function Virtualisation
NGA	Next Generation Access
NT	Network Termination
ONF	Open Networking Foundation
PLC	Powerline Communication
RGW	Residential Gateway
SBC	Session Border Controller
SDN	Software Defined Networks
STB	Set-Top-Box
TA	Terminal Adapter
TE	Terminal Equipment
QoE	Quality of Experience
QoS	Quality of Service
VM	Virtuelle Maschine
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network

Impressum und Kontakt

Home Gateways in zukünftigen Netzen –
die Auswirkung von SDN und NFV auf die Sicherheit privater Daten

Herausgeber und Kontakt

Fraunhofer-Institut für Eingebettete Systeme und Kommunikationstechnik ESK
Hansastr. 32
80686 München

Telefon: 089 547088-0
Fax: 089 547088-220
info@esk.fraunhofer.de
www.esk.fraunhofer.de

Autoren:
Mathias Leibiger
Ivan Furjanic
Thomas Messerer
Florian Krojer
Peter Handel

Redaktion:
Susanne Baumer
Telefon: 089 547088-353
susanne.baumer@esk.fraunhofer.de

Heidi Dorn
Telefon: 089 547088-361
heidi.dorn@esk.fraunhofer.de

Bitte rufen Sie uns an, wenn Sie Fragen haben, weitere Informationen oder ein konkretes Angebot wünschen.