Netzarchitekturen und IKT-Dienste in der nächsten Generation

Daniel Kellenberger • Christian Kuhr • Ralf Steinbach

Die derzeitige Netzevolution von der leitungsvermittelnden zur paketvermittelnden Kommunikation erzeugt bei Netzbetreibern und Systemlieferanten Kopfzerbrechen über die Neuorientierung von Dienstleistungen und Netzplattformen. Zur Debatte stehen vor allem die Inhalte der neuen Dienste, die Netzsicherheit und der Zeitpunkt einer Abschaltung der alten Plattformen, da diese Faktoren für Lieferanten und Betreiber ein hohes Umsatzrisiko darstellen. Die raschen Technikschübe sowie schrumpfende Umsatzerlöse je Nutzer lassen für Migrationen jedoch nicht viel Zeit. Umso wichtiger ist es daher, die zentralen Chancen und Anforderungen kommender IKT-Dienste im Blick zu haben.

Mit dem Einzug von IP Multimedia Subsystems (IMS), die künftig alle Sprach- und Multimediadienste über eine einheitliche IP-gestützte Technikplattform abwickeln sollen, entstehen neue Umsatzquellen für Netzbetreiber, da sich der Kundschaft schneller mehr Dienste erbringen lassen. Mit einer sauber geplanten FMC-Strategie (Fixed-Mobile Conversion) rückt zudem auch das klassische Funknetz näher an das Festnetz, so ähnlich wie die Telekommunikationstechniken immer mehr mit den IT-Techniken verschmelzen. Neue Dienstleistungen und Mehrwerte müssen aber heute, anders als noch vor vielen Jahren, bei der Bereitstellung genau auf die Kundenerwartungen zugeschnitten und innerhalb weniger Monate oder gar Wochen verfügbar sein. Wenn ein Rollout länger dauert, blüht Anbietern ein ähnliches Szenario wie während der xDSL-Einführung, als der massiven Nachfrage nur schwerlich nachzukommen war und die Netze zu langsam mit zahlenden Daten befüllt wurden.

Neue Umsatzquellen mit IP Multimedia Subsystems

Dienste wie Mobile Gaming (z. B. weltweites und unbeschränktes Schachspielen über das Handy als Massengeschäft), Carrier-Class-Ethernet für Wiederverkäufer und Endkunden, Push-to-Talk oder Video-Sharing können die Einnahmen erweitern. Allerdings müssen die Mehrwerte unbedingt rechtzeitig marktfähig sein. In einem IMS-erweiterten Netz ändern sich jedoch viele Planungs-, Routing-, Optimierungs- und Schaltabläufe.

Zwar verstehen genügend Spezialisten für das Signalisierungssystem Nr. 7 (SS7) die Gewährleistung von Sicherheit (Security Assurance) in einem leitungsvermittelnden Netz. Für paketvermittelnde IMS-Netze fehlen solche Spezialisten vielfach. Dieser Sicherheitsproblematik sind sich viele Netzanbieter jedoch nicht bewusst. Eine weitere oft von Systemlieferanten unterschätzte Herausforderung besteht in der Überwachung von „Multi Vendor Platforms“ in einer IMS-Umgebung.

Mit neuen Architekturen und abgeschalteten Legacy-Plattformen wird kein Weg daran vorbeiführen, ein „Network Operation Center“ in ein „Revenue Operation Center“ zu überführen. Kommt der Ersatz von Plattformen nicht in Frage, werden die logischen Schnittstellen zumindest die SOA-/TMForum-Empfehlungen erfüllen müssen. Da die neuen NGN-Architekturen IMS als Subsystem sowie die bewährte SIP-Architektur unterstützen, wird die Kapazitätsplanung dabei künftig nicht mehr im gleichen Ausmaß abhängig davon sein, ob das Transportnetz über Kupfer, LWL oder Luft getragen wird. Folglich werden teure, hauptsächlich aus Hardwarekomponenten bestehende Vermittlungszentralen kaum noch benötigt. Vielmehr werden Netzanbieter mehrheitlich Soft-Switching-Systeme ausrollen, betreiben und vermarkten, um damit Umsatz und Margen auszuweiten und vermehrt Ressourcen für neue Investitionen zu gewinnen.

Auf einen Blick

Es wird auch künftig trotz sinkender Preise ein breites Spektrum an Umsatzquellen mit innovativen IKT-Diensten geben wird. Die Herausforderung wird darin bestehen, einen zuverlässigen, sicheren und dennoch wirtschaftlichen Betrieb der erforderlichen Infrastrukturen rechtzeitig sicherzustellen.

Warum Fixed Mobile Convergence?

Da die Preise für klassischen Mobilfunk (Sprache und SMS) im gesamten Geschäftsmodell künftig weiter fallen, sind Anbieter gezwungen, umzudenken. Diesen Prozess haben Festnetzbetreiber bereits oder zumindest teilweise hinter sich. Als etwa die Preise für Standleitungen Anfang dieses Jahrzehnts schrumpften, waren rasch neue Geschäftsmodelle wie Carrier-Class-Ethernet (MEF) zu entwickeln. Diese Fokussierung hat sich gelohnt, weil die Nachfrage an Bandbreite immer noch groß ist. Und sie wird mittelfristig nicht abnehmen, da durch neue Kundenservices wie Web 3.0 der Nutzen konsistent hoch bleibt. Das hiermit verbundene und viel versprechende Datengeschäft wird höchstwahrscheinlich viele Mobilfunkanbieter fördern oder gar retten. Insbesondere virtuelle Mobilfunknetzbetreiber (MVNO)

befinden sich hier im Vorteil, weil sie weniger investieren müssen und abhängig von den Konditionen ihrer Verträge mit Netzbetreibern rasch an neue Kundenverträge gelangen.

Für den kommerziell „mühsamen“ Sprachverkehr werden sowohl Fest- als auch Mobilfunkbetreiber ihre Geschäftsmodelle kurzfristig anpassen müssen. Durch gegenseitige Konkurrenz im Rahmen der Konvergenz (FMC) kann sich auf längere Zeit kein Netzbetreiber mehr leisten, alle Kundenstämme einem einheitlichen Segment zuzuordnen. Wesentlich besser beraten wären Netzbetreiber, wenn sie die Kundenstämme strukturiert und unterschiedlich bepreisten Geschäftsmodellen zuordnen würden. Ein Beispiel wären unterschiedlich teure Platin-, Gold- und Silberklassen, die entweder eine hundertprozentige Dienstgüte (QoS, Quality of Service), eine begrenzte Dienstgüte oder lediglich „Best-Effort“-Leitungsqualität anbieten. Eine solche Kundenaufteilung ist mit der Aufwand-Ertrags-Relation in früheren Frame-Relay-Netzen vergleichbar. Die garantierte und teurer bezahlte Bandbreite wäre für den entsprechenden Kundenstamm immer oder je nach MTBF mit 99,xx % verfügbar.

Erweiterte Verfügbarkeit mit WiMAX

Neue Chancen entstehen weiterhin durch die stetigen Technikschübe. Bedenkt man, welche Massenbandbreiten mit DWDM/CWDM- und PON-Techniken verfügbar wurden, geht WiMAX noch einen Schritt weiter. Dieser IEEE-802.16-Standard ermöglicht künftig im Rahmen des 4G-Mobilfunks ein Metropolitan Area Network (MAN), das dem Kunden nicht nur ein Hot Spot (WiFi), sondern auf eine Distanz von ungefähr 50 km eine Hot Zone, also ein relativ großes Gebiet mit bis zu etwa 70 Mbit/s verfügbar macht, ohne in Bauarbeiten investieren zu müssen.

Die neu gegründete Organisation OPA (Open Patent Alliance) soll der WiMAX-Technik darüber hinaus zum Zugang zum Massengeschäft verhelfen. Netzknoten wie auch Endgeräte werden zudem durch das WiMAX-Forum beispielsweise als WiMAX-kompatibel zertifiziert. Somit soll die seit vielen Jahren bekannte und beinahe vergessene Technik den Ruf einer Schwellenland-Technik verlieren und auch in Europa genutzt werden. Leider gibt es in Europa überwiegend erst Test- bzw. Labornetze. Worldmax in Holland hat jedoch kürzlich ein erstes kommerzielles Netz angekündigt. Dies stärkt die Hoffnung, dass weitere Anbieter ausrollen, sofern die Regulierungsbehörden effizient Lizenzen vergeben.

Vorteile von Femto-Zellen, Mobile-IP und NFC

Weiterhin versprechen Femto-Zellen in heute noch eingeschränkten oder gar nicht abgedeckten Standorten ein nicht zu unterschätzendes Umsatzpotenzial. Mit einer Mini-Basisstation wird der Kunde mit dem Kernnetz unkonventionell verbunden: Muss sich heute der Benutzer mühsam das Netzsignal suchen, damit er telefonieren kann (z. B. aus dem Zug steigen oder ein nicht versorgtes Büro verlassen), bringt mit der Femto-Technik der Netzbetreiber über z. B. im abgeschotteten Büro platzierte Basisstationen das Kernnetz hin zum Handy-Kunden. Dies wird den Endkunden dazu motivieren, nicht mehr so oft auf das Festnetz auszuweichen.

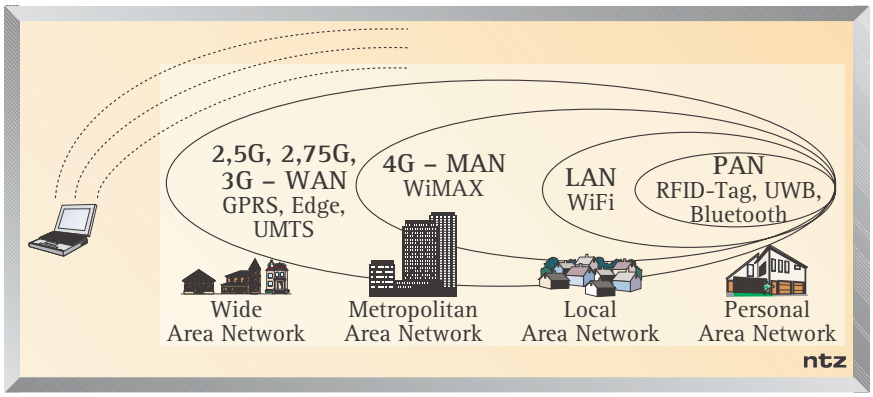

***Bild 1**. Verschiedene Mobilfunktechniken und ihre Reichweiten im Vergleich*

Abkürzungsverzeichnis

3G	3rd Generation
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization, Accouting
ATM	Asynchronous Transfer Mode
BSS	Business Support System
CWDM	Coarse Wavelength Division Multiplex
DSL	Digital Subscriber Line
DWDM	Dense Wavelength Division Multiplex
Edge	Enhanced Data Service for GSM Evolution
EAP	Extensible Authentication Protocol
ETSI	European Telecommunications Standards Institute
FMC	Fixed Mobile Convergence
GPRS	General Packet Radio Service
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKT	Informations- und Kommunikationstechnik
IMS	IP Multimedia Subsystem
LAN	Local Area Network
LWL	Lichtwellenleiter
MAC	Media Access Control Layer
MAN	Metropolitan Area Network
MEF	Metro Ethernet Forum
MPLS	Multi-Protocol Label Switching
MTBF	Mean Time Between Failures
MVNO	Mobile Virtual Network Operator
NFC	Near Field Communication
NGN	Next Generation Network
NGOSS	New Generation Operations Systems and Software
OPA	Open Patent Alliance
OSS	Operations Support System
PAN	Personal Area Network
PHY	Physical Layer
PON	Passive Optical Network
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RFID	Radio Frequency Identification
SDH	Synchronous Digital Hierarchy
SIP	Session Inititiation Protocol
SMS	Short Message Service
SOA	Service Oriented Architecture
SS7	Signalling System #7
Tispan	Telecoms and Internet converged Services and Protocols for Advanced Networking
TMForum	Telemanagement Forum
UMTS	Universal Mobile Telecommunications System
UWB	Ultra Wide Band
VoIP	Voice over IP
WiFi	Zertifikat für die Interoperabilität von WLAN-Geräten
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network

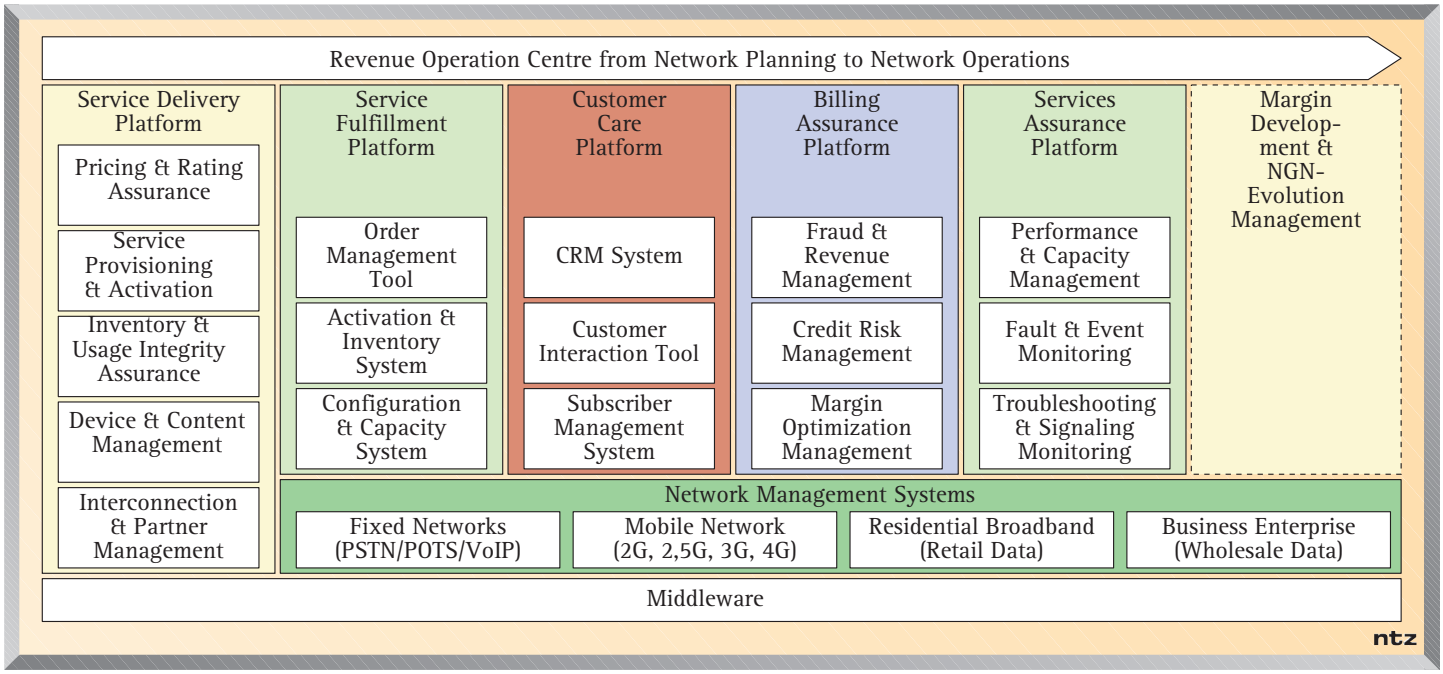

***Bild 2**. Funktionale Architektur der wichtigsten Komponenten einer „NGN Management Plane" im Zusammenhang von IMS und Service Delivery Platform*

Mobile-IP bietet als IETF-Standard eine identische und statische IP-Adresse für sich im Netz bewegende Endgeräte. Da das Internet-Protokoll naturgemäß auf einheitliche Identifikation jedes sich im Internet anmeldenden Host besteht, ruft dies in Mobilfunknetzen ein deutliches Problem hervor: Bei jeder physikalischen Standortänderung muss eine neue IP-Adresse zugeteilt werden. Dies ist bei Festnetzanwendungen selbstverständlich kaum der Fall. Weil höher liegende Protokolle wie TCP auf eine statische IP-Adresse für z. B. identifizierende Verbindungen bestehen, füllt der IETF-Standard genau diese Lücke mit einer bleibenden IP-Adresse – egal, wo sich das Endgerät befindet. Die Verbindung bleibt bestehen und die Mobilität transparent für höhere Protokolle.

Mit NFC (Near Field Communication) lassen sich Daten drahtlos und im 13,56-MHz-Bereich mit bis zu 424 Kbit/s übertragen. Zudem ermöglichen NFC-kompatible Endgeräte einen kontaktlosen, sowohl lesenden als auch schreibenden Datentransfer innerhalb von 4 cm. Zusätzlich werden Signale zu etablierten Funktechniken wie WiFi und Bluetooth unterstützt. Durch die sehr kurze Distanz laufen die Transaktionen sicher ab und sind nicht zu knacken. Somit können Nutzer einfache Zahlungen über das Handy abwickeln oder Daten bzw. Grafiken an Laptops oder Kameras übermitteln. Für den Massenmarkt stellt dies ein interessantes Geschäftsmodell dar, um das Überlastungsrisiko des Sprach-, Terminierungs- und SMS-Verkehrs zu lindern.

Infrastruktur auch gemeinsam nutzbar

Ergänzend zu diesen Möglichkeiten, Margen und Umsätze zu sichern bzw. zu erhöhen, ist auf drei wesentliche strategische Punkte hinzuweisen:

- Ein Outsourcen der Netzplanung und -optimierung ist gründlich abzuwägen.
- Eine gemeinsam mit der Konkurrenz genutzte Infrastruktur schadet nicht, bringt Kostenvorteile durch reduzierte Investitions- und Betriebskosten und lässt sich an die konkurrierenden Partner weiter verrechnen.
- Bereitstellung (Provisioning), Betrieb (Operations) und Qualitätssicherung (Quality Assurance) sind frühzeitig NGN-tauglich umstrukturieren, damit eine „Multi Vendor Platform" verwendbar wird.

Ein langfristig planender Netzbetreiber kann sich nicht mehr nur auf Mobilfunk, Festnetz, Daten, Sprache oder Transport fokussieren. Pauschalen (Flat Rates) ermöglichen es dabei, möglichst viele Dienstleistungen als Massengeschäfte anbieten, und sichern langfristig Umsatz und Gewinn.

Bild 2 zeigt beispielhaft eine in diversen Projekten gewachsene funktionale Architektur der wichtigsten Komponenten einer „NGN Management Plane" im Kontext von IMS und SDP. Die oben erwähnte notwendige Umstrukturierung von Bereitstellung, Betrieb und Qualitätssicherung wurde hier umgesetzt, einerseits aufbauend auf (Industrie-) Standards wie TMForum NGOSS, andererseits auch die am Markt verfügbaren Produkte berücksichtigend.

Sicherheitsaspekte in Next Generation Networks

Bei der Migration zu einem NGN und der damit verbundenen Einführung neuer Kunden- und Mehrwertdienste begegnen Netzbetreiber vielschichtigen Herausforderungen im Bereich der Sicherheit. An dieser Stelle seien beispielhaft wesentliche Fragestellungen aufgezeigt.

So ergeben sich wichtige Sicherheitsanforderungen im Bereich der erstma-

Dr. Daniel Kellenberger ist seit 1988 in der IKT-Industrie für mehrere Netzbetreiber und Hersteller in Engineering und Operations tätig gewesen. Für Detecon Consulting arbeitet er seit 2007 als Experte im Bereich Network Architecture.
E-Mail: Daniel.Kellenberger @detecon.com

Christian Kuhr arbeitet als Consultant bei Detecon International in Bonn. Sein Arbeitsgebiet sind Migrationen von Next Generation Networks mit dem Fokus Netzmanagement und Operations.
E-Mail: Christian.Kuhr@detecon.com

Dipl.- Inform. Ralf Steinbach arbeitet als Berater bei Detecon International in Bonn mit dem Schwerpunkt Architektur im Bereich NGOSS.
E-Mail: Ralf.Steinbach@detecon.com

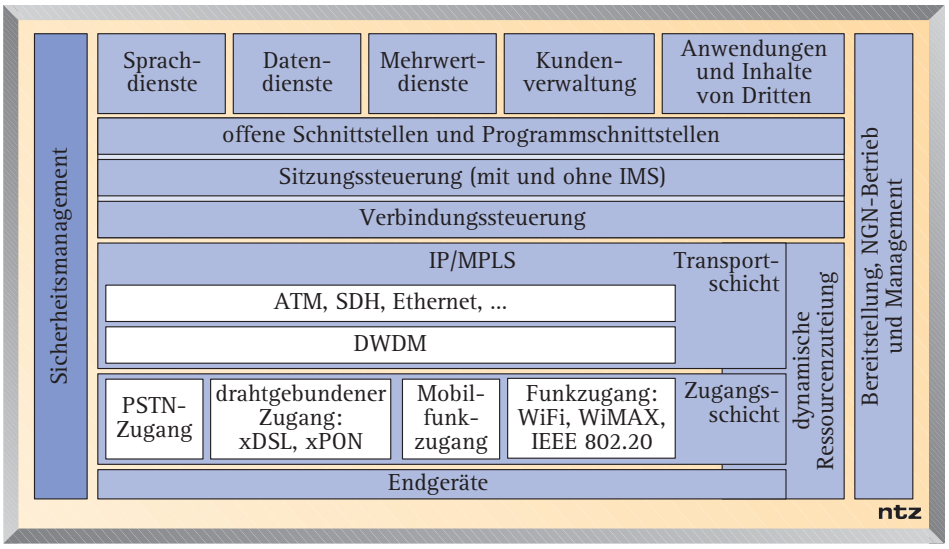

***Bild 3**. Sicherheitsaspekte im NGN-Schichtenmodell*

ligen Bereitstellung und dauerhaften Speicherung von Kundendiensten (User Data Provisioning) sowie bei Anmelde- und Authorisierungsprozeduren (User Registration/Authentication). Auch sind die Dienste im NGN exakt abzurechnen (Charging). Die Sicherheit der Schnittstellen zu verschiedensten OSS/BSS, wie z. B. den Abrechnungssystemen, spielt hier eine entscheidende Rolle.

Aus neuen Kunden- und Mehrwertdiensten entstehen zusätzliche dienstspezifische Sicherheitsanforderungen (Application Level Protection), die vom Netzbetreiber effizient verwaltet werden müssen. Der Schutz des Kunden innerhalb einer spezifischen Anwendung (z. B. VoIP) bezogen auf die Steuerungs- und Dienstesicherheit als auch auf die Transportsicherheit (Transport Layer Security) – mittels Funktionen für das SIP-Protokoll – sind hier beispielhaft zu nennen.

Die genannten Aspekte verdeutlichen, dass sich das Sicherheitsmanagement über alle Schichten eines Next Generation Network erstreckt. **Bild 3** versucht die Tragweite von NGN-Sicherheit im NGN-Schichtenmodell noch einmal zu veranschaulichen.

Jede Schicht eines NGN stellt dabei unterschiedliche Anforderungen an das Sicherheitsmanagement. Grob betrachtet lassen sich folgende Bereiche unterscheiden:

- Dienstesicherheit,
- Steuerungssicherheit,
- Transportsicherheit,
- Zugangsnetzsicherheit und
- Kundendatensicherheit.

Mit der Lösung dieser komplexen Anforderungen beschäftigen sich u. a. zahlreiche internationale Standardisierungsgremien. Die derzeit verfügbaren Standards in diesem Bereich betrachten das Sicherheitsmanagement aus unterschiedlichen Blickwinkeln:

- ETSI Tispan: Tispan-Arbeitsgruppe 7 ist verantwortlich für das Management und die Entwicklungskoordination von Sicherheitsspezifikationen in NGN- und Multimedia-Diensten. Sie führen Sicherheitsanalysen durch und geben Empfehlungen für Netzprotokolle und -elemente im NGN [1].
- 3GPP TSG SA WG 3 (Security): Die Arbeitsgruppe 3 ist verantwortlich für Sicherheit im 3GPP Standard. Sie analysiert potenzielle Sicherheitsbedrohungen für das System und Netz. Im Besonderen fokussiert sie sich auf die Sicherheitsanforderungen zur Einführung neuer IP-gestützter Dienste in Mobilfunknetzen [2].
- IETF: Verschiedene Arbeitsgruppen beschäftigen sich mit Sicherheitsthemen, wie z. B. mit AAA-Netzelementen und Authentifizierungsprotokollen (z. B. EAP).
- WiMAX-Forum: Standardisierung von Sicherheitsmechanismen auf der Grundlage von IEEE 802.16 e (MobileWirelessMAN). Die Fokussierung liegt auf Sicherheitsmechanismen in der Luftschnittstelle (PHY- und MAC-Schicht durch die Verwendung von Security Sub Layer) [3].
- IEEE: Herleitung von neuen Anforderungen an das Sicherheitsmanagement auf der Basis von vorhandenen Standards, wie z. B. Wireless LAN Security (802.11i), WiMAX Air Interface Security (802.16e) oder Port based Network Access Control for Network Access (802.1x).

Aufbauend auf den genannten Standards und Themenbereichen entwickeln Festnetz- und Mobilfunknetzbetreiber unternehmensindividuelle Sicherheitskonzepte für die Migration in Richtung NGN.

Betrachtet man die derzeitigen „Best Practices“ im Umgang mit Sicherheitsmanagement näher, wird in allen Implementierungen ein Trend deutlich: Sicherheit wird zunehmend als ganzheitliche und netzweite Funktion betrachtet. Ein deutliches Indiz ist die Integration von dedizierten Elementen in bestehende oder neu entwickelte OSS/BSS-Architekturen, welche hauptverantwortlich das Sicherheitsmanagement übernehmen. Zwei wichtige Elemente heutiger Sicherheitslösungen seien stellvertretend erwähnt:

Das erste Element wird als Sicherheitsmanagement bezeichnet und ist für die Überwachung und Umsetzung von Sicherheitsregeln (Policies) in NGN verantwortlich. Die wesentlichen Aufgaben dabei sind:

- Vorbeugung und Erfassung von netzfremden Eindringlingen sowie die kontinuierliche Überwachung und Pflege der Dienst- und Netzsicherheit. Dabei werden Sicherheitslücken überwacht und Wiederherstellungsprozeduren initiiert.
- Korrelierung von sicherheitsrelevanten Dienst- und Netzinformationen mit vordefinierten Metriken zur Abschätzung von bestehenden und sich entwickelnden Bedrohungen innerhalb des NGN und seinen Diensten. Beim Überschreiten von definierten Schwellenwerten werden Gegenmaßnahmen frühzeitig ausgelöst.

Das zweite Element besteht aus dem Regelmanagement (Policy Management) im NGN. Es erstellt, aktualisiert und entfernt Sicherheitsregeln und stellt Policy-Informationen für andere OSS/BSS zur Verfügung.

Die Kombination beider Elemente ermöglicht die zentralisierte Verwaltung der festgelegten Sicherheitsbestimmungen und die gezielte Ansteuerung von NGN-Netzelemente bzw. OSS/BSS-Komponenten. Anwendungsbeispiele dafür sind beispielsweise die Zugangsregelungen zu NGN-Komponenten, Kundendiensten oder Informationen. Beide Elemente sind wichtige Bestandteile der Architektur eines Netzbetreibers, um definierte Sicherheitsregeln effektiv umzusetzen.

Literatur und Quellen

[1] http://portal.etsi.org/tispan/WG7_Tor.asp
[2] http://www.3gpp.org/TB/sa/SA3/SA3.htm
[3] http://epress.lib.uts.edu.au/dspace/bitstream/2100/172/1/157_Pang.pdf