Eine Themenbeilage der Heise Medien GmbH & Co. KG

KOMMUNIKATION UND NETZE

ITK – PRODUKTE UND LÖSUNGEN

I 2016

Störerhaftung:

Was Public WLAN zu freiem WLAN macht

Seite 8

Wo WLAN-Schiedsrichter auf Abseits entscheiden

Wer in Frankreich eine Prepaid-SIM-Karte kauft, muss dort schon länger seine Identität nachweisen. Im Laden an der Ecke wird das zwar oft ziemlich „mediterran“ gehandhabt, aber das Beispiel zeigt, wie unterschiedlich die politischen Prioritäten sind. Hierzulande hat die Bundesregierung einen entsprechenden Gesetzesvorstoß als vorbeugende Antiterrormaßnahme erst in diesem Juni unternommen. In Deutschland sind es sonst eher die Urheberrechte, deren Schutz mit der technologischen Entwicklung schwer zu synchronisieren ist. Das gilt für die GEMA auf YouTube ebenso wie für Public WLAN.

Hotspots, Störerhaftung und Access Points sind darum der erste Schwerpunkt dieser Ausgabe: Dr. Harald Karcher zeichnet nach, was sich bei Telemediengesetz und offenen Funknetzen getan hat (Seite 8). Außerdem war er 2015 und 2016 mit der Bayerischen Seenschifffahrt unterwegs, um das kostenlose @BayernWLAN zu testen (Seite 11). Die Funkverteiler auf den Fähren beziehen ihr Netz offenbar von den LTE-Mobilfunkmasten und reichen es an die Fahrgäste weiter. „Wenn der professionelle WLAN-Hotspot der Seenschifffahrt das @BayernWLAN aus LTE speist, müssten wir das doch auch können“, dachte sich der Autor und nahm die kleine Fritz!Box 6820 LTE mit auf die nächste Tour, um versuchshalber ein eigenes Netz aufzuspannen (Seite 13). Wie dieser LTE-to-WLAN-Router mit den diversen Mobilfunknetzen klarkommt, hat Karcher außerdem für einen separaten Beitrag getestet, den Sie auf Seite 24 finden.

Das Thema hat auch noch einen IoT-Aspekt: Immer mehr Machine-to-Machine-Kommunikation wird künftig per Mobilfunk vonstattengehen. Meist sind es nur minimale Datenmengen, die aber in regelmäßigen Intervallen durch die Luft gehen. Das wirft zum einen die Kostenfrage auf und birgt zum anderen ganz eigene Risiken. Wie man sie in den Griff bekommt, erklärt Lawrence Miller (Seite 22). Überhaupt ist jeder Netzwerkverantwortliche gut beraten, wenn er den internen Datenverkehr vom öffentlichen Netz trennt. Eine elegante und flexible Möglichkeit sind Virtuelle LANs. Eine praktische Einführung in die VLAN-Konfiguration gibt Thomas Molkenbur gleich zu Beginn (Seite 4), von der einfachen Switch-Auftrennung bis zu komplexen Netzen aus mehreren Geräten und Access Points. Das funktioniert bei virtuellen Servern mutatis mutandis übrigens genauso.

Damit wären wir bereits beim zweiten Schwerpunkt dieser Ausgabe: der Umstellung auf All-IP. Bekanntlich stellt die Telekom bis 2018 alle TK-Anschlüsse auf Internet Protocol um (Seite 16). Was das für ISDN-Sonderdienste, bestehende Telefonanlagen, Analog- und DECT-Geräte bedeutet, hat Doris Piepenbrink untersucht (Seite 17). Sie rät Unternehmen und Organisationen dazu, die Optionen der Migration rechtzeitig zu prüfen. Schließlich sind auf IP-Basis auch Cloud-basierte TK-Anlagen möglich, und die gründliche Einbindung von Groupware, Videokonferenz-Software oder ausgebauten Unified Communications wäre eine Überlegung wert. An diesem Punkt setzt dann der Beitrag von David Williams an (Seite 20); er beschreibt genau, wie man UC-Systeme so an die Datenbanken von ERP und CRM anbindet, dass sie bei Anruf die jeweils passenden Informationen beziehen.

Die All-IP-Umstellung wiederum wird maßgeblich durch die Deutsche Telekom vorangetrieben – und damit kommen noch einmal Recht und Politik ins Spiel. Die Politik nämlich hat uns bis 2018 mindestens 50 MBit/s im Download versprochen. Die Telekom will dieses Versprechen erfüllen – mittels VDSL2-Vectoring. Dazu ist allerdings ein exklusiver Zugriff auf die jeweiligen Hauptverteiler und Kabelverzweiger notwendig, was Mitbewerbern und unabhängigen Dienstebetreibern gar nicht schmeckt; sie befürchten eine neue Monopolstellung der Post-Infrastrukturerbin. Hinzu kommt: Vectoring wird die Glasfaser-Förderkulissen kräftig verändern – und damit den FTTB-Netzausbau mindestens verzögern. Wer hier mitreden will, liest am besten den Hintergrundbeitrag von Doris Piepenbrink auf Seite 15.

Thomas Jannot

Mehr Sicherheit mit logischen Subnetzen

Fünf Konfigurationsszenarien zeigen die Möglichkeiten von Virtual LANs

Derzeit halten VLANs auch Einzug in kleineren und mittelgroßen Firmennetzen – etwa um den Publikumstraffic vom internen Datenverkehr zu trennen. Die Vorteile gegenüber physikalisch getrennten LANs liegen vor allem in der größeren Flexibilität und überwiegen den Aufwand der Einarbeitung nach kürzester Zeit.

VLAN ist das Kürzel für Virtual Local Area Network. VLANs verwendet man, um physikalische Layer-2-Netze aus Netzwerkkabeln, Switches und Wireless Access Points in logische Netze aufzutrennen. Das führt zu Einsparungen bei der Hardware und zu mehr Flexibilität und Übersicht bei der Konfiguration – auch wenn mancher Administrator von der besseren Übersicht nur schwer zu überzeugen ist. Das liegt dann meistens daran, dass er mit dem Thema nicht hinreichend vertraut ist.

Ein Switch mit mehreren VLANs

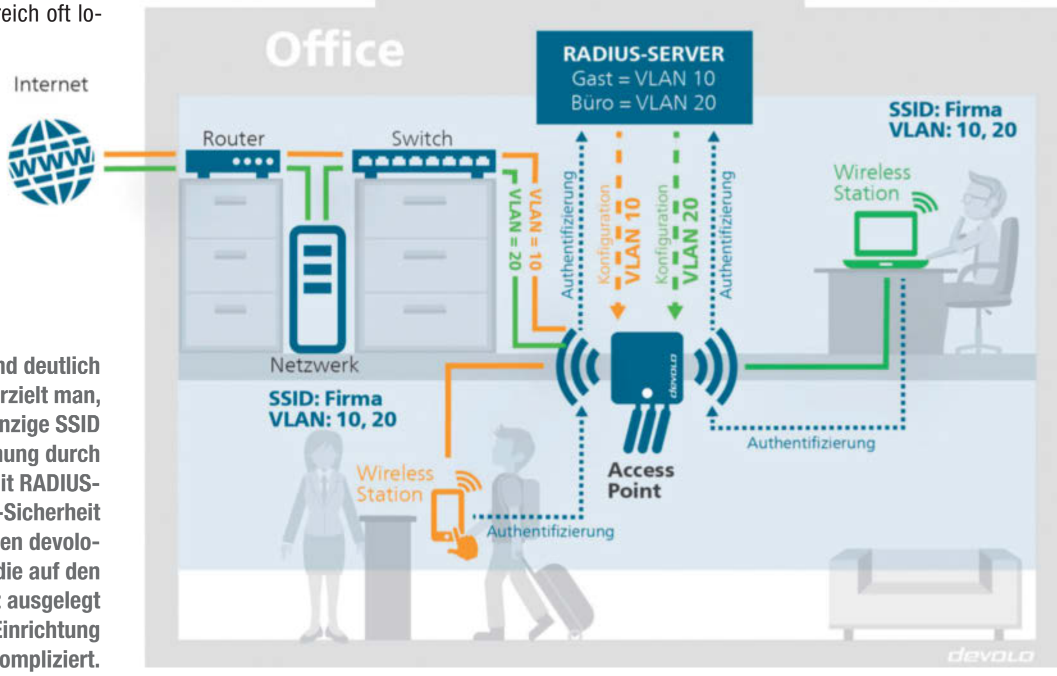
Beginnen wir mit einem einfachen Beispiel. VLANs sind eine Basiseigenschaft, die von jedem managebaren und auch von den günstigeren smart-managebaren Switches unterstützt wird. Wir möchten nun einen physikalischen Switch in mehrere logische Switches aufteilen.

Angenommen der Switch hat 48 Ports und wir benötigen eigentlich 6 Switches mit jeweils acht Ports, dann konfigurieren wir im Switch sechs VLANs mit unterschiedlichen VLAN-IDs. VLAN-IDs haben einen Wertebereich von 1 bis 4095. In der Praxis wird dieser Bereich oft logisch segmentiert, damit man eine bessere Übersicht bekommt und weil davon auszugehen ist, dass die anfänglich gewählten IDs im Laufe der Zeit um weitere ergänzt werden. In unserem Beispiel bekommt der Switch 1 die ID 10, Switch 2 die ID 20 usw. Meistens bieten Switches die Möglichkeit, dem VLAN auch gleich noch eine Bezeichnung zu geben.

Der Switch 1 soll die Ports 1 bis 8 umfassen, welche in der Konfiguration nun der VLAN-ID 10 zugeordnet und als „untagged“ konfiguriert werden. Genauso verfährt man mit den übrigen Switches 2 bis 6. – Was heißt jetzt „untagged“?

VLAN-Tags und VLAN-IDs

Ein VLAN-Tag ist eine Erweiterung des Ethernet-Headers um vier Oktette, die zwischen den MAC-Adressen und der Länge des Frames eingefügt werden. Die Bedeutung dieses Tags ist im VLAN-Standard IEEE 802.1q definiert. Er besteht im Wesentlichen aus einer zwei Oktette langen, fixen ID zur Erkennung, ob ein VLAN-Tag vorhanden ist oder nicht, der VLAN-Priorität und der bereits erwähnten VLAN-ID.



Quelle: devolo Business Solutions

Optimale Kontrolle und deutlich weniger Airtime-Last erzielt man, indem man nur eine einzige SSID verwendet und die Trennung durch dynamische VLANs mit RADIUS-basierter Enterprise-Sicherheit vornimmt. Bei APs, wie den devolo-WiFi-pro-Modellen, die auf den geschäftlichen Einsatz ausgelegt sind, ist die VLAN-Einrichtung relativ unkompliziert.

be.IP

Zeit für das neue Netz

- Telefonanlage für bis zu 40 Benutzer **mit SIP-Trunk Unterstützung**
- Unterstützung für analoge, ISDN und IP / IP-DECT-Endgeräte
- 4 analoge Schnittstellen zusätzlich
- Optionale Erweiterung für Benutzer, Voice-Mail, VPN und WLAN-Management
- Unterstützung von LANCAPI
- Drehbare ISDN-Schnittstellen durch optionalen Adapter
- Sanfte Migration – Betrieb als Media-Gateway

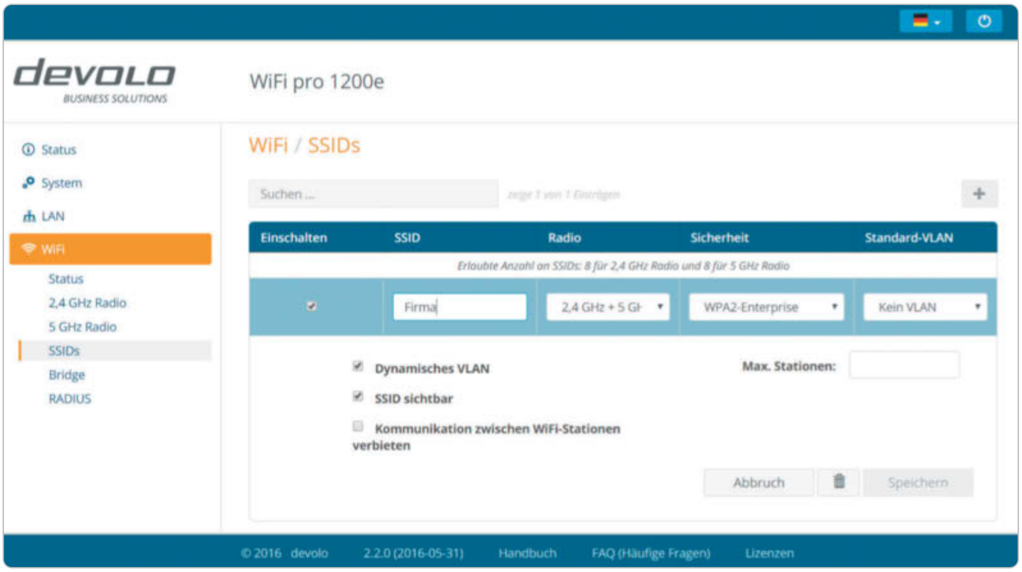
Die be.IP *plus* ist eine **vollwertige Kommunikationszentrale** für Sprache, Daten und Sicherheit. Sie ist die ideale ALL-IP-Lösung **für Geschäftskunden** und anspruchsvolle Anwender.

2 Systeme in einem Gerät mit dem *Plus* an Leistung. Ob als **TK-Anlage oder Media Gateway** zur sanften Migration vorhandener ISDN-TK-Systeme - mit der be.IP *plus* gelingt der **Umstieg auf ALL-IP** spielend einfach.

Mehr erfahren zu bintec elmeg ALL-IP-Lösungen unter:
all-ip.bintec-elmeg.com
oder QR-Code scannen:

bintec elmeg
Teldat Group Company

bintec elmeg GmbH
Südwestpark 94
D-90449 Nürnberg
Telefon: +49-911-96 73-0
www.bintec-elmeg.com



Quelle: devolo Business Solutions

Im Web-Interface des WiFi pro 1200e lassen sich VLAN und SSIDs übersichtlich konfigurieren.

Ein Switch-Port, an dem ein nicht VLAN-fähiges Endgerät angeschlossen ist, muss ungetaggt konfiguriert werden, damit keine Frames mit VLAN-Tag an das Endgerät gesendet werden. Der Switch entfernt dann vor dem Senden das Tag und versieht im Gegenzug Frames, die vom Endgerät eingehen, beim Empfang mit dem entsprechenden Tag. Der Grund für diese Konfiguration ist, dass die allermeisten Endgeräte kein VLAN unterstützen. Ausnahmen sind häufig VoIP-Telefone und Server. Vor allem in Verbindung mit virtuellen Servern sind VLANs aber enorm attraktiv. Doch dazu später mehr.

Wichtig ist: Innerhalb des Switches können Frames mit einer bestimmten VLAN-ID nur an Ports weitergeleitet werden, die ebenfalls Mitglied in genau diesem VLAN mit dieser ID sind.

Außerhalb des Switches sind in diesem Beispiel also niemals getaggte Frames unterwegs. Man bezeichnet solche VLANs als Port-based VLANs und die Ports, an denen nicht VLAN-fähige Endgeräte angeschlossen sind, als Edge-Ports.

VLAN über mehrere Switches hinweg

Interessanter und praxisnäher ist das nächste Beispiel: Jetzt sollen die virtuellen Switches aus dem ersten Beispiel auf einen weiteren managebaren Switch ausgeweitet werden, d.h. die Switches 1 bis 6 sollen Ports dazubekommen, die an einem anderen Switch sind. Dazu verbindet man beide Switches mit einem Ethernetkabel.

Im Unterschied zum ersten Beispiel ist nun am ersten Switch ein weiteres VLAN-fähiges Gerät angeschlossen. In diesem zweiten Switch konfigurieren wir nun dieselben VLAN-IDs wie im ersten. Dann fügen wir die Trunk-Ports zu jedem der VLANs 10 bis 60 als tagged hinzu. Hier gibt es nun einen wichtigen Unterschied: Ein Port kann in maximal einem VLAN untagged sein, aber in beliebig vielen VLANs tagged. Auch beides gleichzeitig ist möglich.

Dieses Beispiel können wir beliebig ausbauen. Ein Switch kann zum Beispiel der Core-Switch sein, an dem Server, Access-Switches, eine Telefonanlage, die Firewall oder der Internet-Zugang angeschlossen sind, und der andere ein Access-Switch oder Etagenverteiler, an dem Desktop-Rechner, Kameras oder Telefone angeschlossen sind.

Es gilt an dieser Stelle, sich vor Augen zu halten, wozu wir überhaupt verschiedene logische Switches benötigen und warum wir unser physikalisches LAN segmentieren. Es gibt mehrere Gründe dafür: Erstens schafft ein VLAN Sicherheit. Es verhindert den Zugriff auf sensible Daten der Buchhaltung durch Überlauf der MAC-Adresstabelle durch MAC-Spoofing und kann zum Beispiel das Produktiv- sauber vom Gästenetz trennen. Ein zweites Argument betrifft die Performance: Logische Netze verkleinern die Broadcast-Domäne, um die Anzahl der Broadcast-Pakete zu minimieren, und verhindern eine Überlastung von leistungsschwachen Endgeräten wie zum Beispiel VoIP-Telefonen. Ein dritter Vorteil liegt in den Möglichkeiten der Priorisierung: Mit VLANs können wir zum Beispiel leicht den Voice-Traffic trennen und ihm gegenüber dem Bulk-Traffic den Vorzug einräumen.

Internet-Zugriff für mehrere VLANs

Im dritten Beispiel kommt IP-Routing mit ins Spiel. Wenn wir LAN-Segmente mit VLANs trennen, dann können und sollen die Geräte aus verschiedenen LANs nicht miteinander kommunizieren. Dennoch sollen aber mehrere VLANs denselben Internetzugang nutzen.

Wenn wir eine Firewall-Appliance besitzen, dann kann diese typischerweise ebenfalls mit getaggten VLANs umgehen. In diesem Fall gibt es einfach einen Trunk zur Appliance – und alle VLANs sind mit verschiedenen logischen Interfaces der Firewall verbunden. Über die Konfiguration der Firewall können wir dann gezielt bestimmten Datenverkehr zwischen den VLANs erlauben. Die Firewall fungiert hier als Router.

Falls wir keine dedizierte VLAN-fähige Firewall haben, dann ist es sinnvoll, einen Layer-3-Switch als Core-Switch zu verwenden. Dadurch sind wir in der Lage, durch Setzen von Routing-Einträgen den Datenverkehr zwischen einem oder mehreren virtuellen Switches zum VLAN für den Internetzugang und zurück zu leiten.

VoIP-Telefonie im VLAN

Das vierte Beispiel macht sich zunutze, dass man an einem Port gleichzeitig getaggte sowie ein ungetaggtes VLAN konfigurieren kann. Diese Konfiguration verwendet man zum Beispiel für Switch-Ports, die per PoE (Power over Ethernet) Telefone, Kameras und WLAN-Access-Points mit Strom versorgen können. Das ungetaggte VLAN ist für den Anschluss von Arbeitsplatzrechnern konfiguriert und das getaggte VLAN für die Verwendung von VoIP-Telefonen.

VoIP-Telefone booten und verbinden sich untagged mit dem Netzwerk. Sie beziehen eine temporäre IP-Adresse von dem DHCP-Server, der für die Arbeitsplatzrechner zuständig ist. Zusätzlich bekommt das Telefon die Information mit, auf welchem VLAN sich der Voice-Dienst befindet. Mit dieser Information startet das Telefon neu und verbindet sich nun getaggt mit dem Voice-VLAN.

WiFi Access Points sicher einbinden

Das letzte Beispiel zeigt die Verwendung von VLANs in Verbindung mit Wireless Access Points. Der typische Anwendungsfall ist wohl der, dass man die Daten von Mitarbeitern und Gästen trennen will.

Ein physikalischer Business-AP kann mehrere SSIDs ausstrahlen, die den drahtlosen Zugang zu verschiedenen Netzen erlauben. Dabei wird jeder SSID ein VLAN zugewiesen, das vom AP getaggt zum Switch gesendet wird.

Wenn aber, wie das im Enterprise-Umfeld normal ist, die Mitarbeiter in viele unterschiedliche VLAN-Netze aufgeteilt sind, dann steigt schnell die Anzahl der benötigten SSIDs. Und jede konfigurierte SSID führt dazu, dass der Access Point Beacons mit einem Intervall von 100 ms aussendet. Das kann die Effizienz des WLAN-Kanals schnell verschlechtern. Man kann gegensteuern, indem man die minimale Basisrate, mit der die Beacons gesendet werden, hochsetzt. Diese ist bei 2,4 GHz typischerweise auf nur 1 MBit/s konfiguriert. Ein Anheben auf mindestens 6 MBit/s ist eine gute Idee und senkt den Overhead um den Faktor 6. Eine andere Möglichkeit besteht darin, das Beacon-Intervall selbst zu konfigurieren, was bei vielen APs möglich ist. Dabei sind aber Interoperabilitätsprobleme nicht ganz auszuschließen.

Wenn für die Authentifizierung der WiFi-Clients ohnehin Enterprise Security nach 802.1x (RADIUS-Server) genutzt wird, dann bietet es sich an, überhaupt nur eine einzige SSID zu verwenden und stattdessen dynamisches VLAN im AP einzuschalten, was mit tauglichen Access Points für gewerbliche Ansprüche relativ einfach möglich ist. Dabei kommt die Information, in welchem VLAN sich ein Client befinden muss, vom RADIUS-Server. Um ein VLAN beim RADIUS-Server zu konfigurieren, werden folgende Parameter aus dem RFC 2868 genutzt: Tunnel-Type, Tunnel-Medium-Type und Tunnel-Private-Group-ID. Eine umfangreiche VLAN-Konfiguration im Wireless Access Point ist dann nicht mehr nötig.

VLAN in virtuellen Umgebungen

Zu guter Letzt sei noch erwähnt, dass es gute Praxis ist, für das Management aller Netzwerkgeräte (Switches, Router, Wireless Access Points) ein dediziertes VLAN zu verwenden. Dieses sollte man überall nur getaggt verwenden, damit ein Mitarbeiter mit einem Standardrechner sich nicht einfach per Ethernet mit einem Switch verbinden kann.

Zuvor wurde die besondere Rolle von virtuellen Servern in Verbindung mit VLANs erwähnt. Alle Virtualisierungslösungen bieten die Möglichkeit, den Host selbst wie einen virtuellen VLAN-fähigen Switch zu verwenden. Dabei werden die Ethernet-Interfaces der virtuellen Maschinen durch den Host den VLANs zugeordnet. So können auf einem physikalischen Host virtuelle Maschinen für verschiedene Abteilungen laufen, ohne dass eine Abteilung auf die Maschinen der anderen Abteilungen zugreifen kann.

Thomas Molkenbur,
Leiter Entwicklung, devolo Business Solutions

Wireless-Netze mit offenen Risiken

Der Mai 2016 hat den Weg für Gästefunknetze freigemacht – aber nicht ganz

Hotels und Gastronomie, Geschäfte und engagierte Freifunker haben lange auf diesen Moment gewartet: das Ende der Störerhaftung. Die praktische Rechtsprechung zur Gesetzesänderung bleibt abzuwarten. Viele kleine Betreiber werden sich nun mit Fragen der WLAN-Sicherheit auseinandersetzen müssen.

WLAN-Hotspots der Gattung IEEE 802.11b gibt es in deutschen Hotels seit 2001. Für 24 Stunden WLAN zahlten Geschäftsgäste anno 2001 im Kempinski Vier Jahreszeiten München zunächst 150 DM. Dieser Hotspot war von Anfang an technisch sehr professionell durchgestylt, aber in einigen anderen Hotels passierten Fehler, die man nicht wiederholen sollte: Ein großes Hotel in Stuttgart etwa ließ kurz nach der Jahrtausendwende die ersten WLAN-11b-Access-Points von einem WLAN-Gerätehersteller direkt an das Ethernet (und somit auch Internet) des Hotels anschließen. Schnell hatten technisch versierte Hotelgäste per WLAN-Laptop aus der Lobby den vollen Zugriff auf die hotelinternen Daten und Dokumente, auf die Zimmerbelegung und die Gästelisten.

Fahrlässige Hotspots in Hotels

Diese Security-Schlamperei kam auch anderen Hoteliers zu Ohren. Irgendwann mussten die WLAN-Provider dann immer erst einen gesonderten DSL-, SDSL- oder VDSL-Anschluss und ein gesondertes Ethernet-Kabelnetz im Hotel verlegen, an dem sie dann die WLAN-Sender für die Gäste installieren durften. Komplette physikalische Trennung von Hotelnetz und Gäste-WLAN hieß dann die Parole – obwohl man die Netze auch schon damals rein virtuell hätte trennen können.

Ein großes Hotel in München (nicht das oben genannte Kempinski) hatte einige Dutzend WLAN-Access-Points eines weltbekannten Technikherstellers in den Doppeldecken verbaut. Kurz nach der Fertigstellung merkte der Autor dieser Story bei einem Test, dass er mit seinem WLAN-Laptop aus der Lobby den anderen Hotelgästen in den Konferenzräumen auf die Festplatte schauen konnte. Der Grund: Die verbauten Access Points waren nicht in der Lage, den Querverkehr zwischen den im WLAN angemeldeten Laptops zu unterbinden. Dutzende WLAN-Geräte wurden daraufhin wieder abmontiert und durch eine andere Marke ersetzt, bei der man den internen Querverkehr zwischen den Geräten direkt im Access Point abschalten kann.

Quelle: Harald Karcher

Am bequemsten ist der WLAN-Gastzugang ganz ohne jede Anmeldung. Eine andere Möglichkeit ist die Anmeldung per Passwort, NFC oder QR-Code. Dieser Screenshot der QR-Codes für Funkzellen auf 2,4 und 5 GHz stammt aus einer AVM Fritz!Box 7390, Hardware-Baujahr 2009, Software-Stand Mai 2016.

Zeitbombe im TMG

WLAN-Sicherheit und die saubere Trennung von internem Netz und Gästezugang wird aller Voraussicht nach ein Massenthema werden. Denn bislang hat die deutsche Gesetzgebung mit der Störerhaftung viele Unternehmen, Gewerbetreibende und Amateure davon abgehalten, ein offenes Funknetz zur Verfügung zu stellen. Tatsächlich hätten wir in Deutschland de facto eine nahezu flächendeckende WLAN-Versorgung. Es gibt ja schon mehrere Millionen private Funknetze. Würde jeder private WLAN-Betreiber sein Netz auch für Gäste öffnen, dann hätten wir auf einen Schlag fast flächendeckend kostenloses Internet (zumindest in den dichter besiedelten Regionen). Just diese Öffnung hat in Deutschland bislang aber nicht stattgefunden, eben weil wir seit 2010 einen Innovationsverhinderer namens WLAN-Störerhaftung hatten.

Die Störerhaftung stört

Die deutsche Hotellerie hat unter der WLAN-Störerhaftung wohl mehr gelitten als jede andere Branche; sie erklärte am 11. Mai in Windeseile: „Der Deutsche Hotel- und Gaststättenverband (DEHOGA Bundesverband) und der Hotelverband Deutschland (IHA) begrüßen diese überfällige Entscheidung der Großen Koalition ausdrücklich. Um die Chancen der Digitalisierung im Interesse der Gäste vollumfänglich nutzen zu können, gehörte die unsägliche WLAN-Störerhaftung auch in Deutschland endlich beseitigt. Für die Hotels, Restaurants und Cafés bedeutet die nun verabredete umfassende Haftungsbefreiung der

WLAN-Betreiber den lange erwarteten Befreiungsschlag."

Was geschehen war? Am 11. Mai 2016 hatten die Regierungsparteien CDU, CSU und SPD beschlossen, die Störerhaftung für öffentliche WLAN-Hotspots wieder abzuschaffen. Dieser Schritt war von vielen Seiten seit Langem gefordert worden.

„Es ist absurd, dass wir uns seit über sechs Jahren diese Störerhaftung in Deutschland leisten. […] Das ist ein Sonderfall, den kein anderes Land in der Welt hat. Das ist auch der Grund, warum wir kaum offene WLANs in Deutschland haben", wettert Markus Beckedahl, Gründer der Digitalkonferenz re:publica und Chefredakteur von netzpolitik.org in einem Interview mit dem WDR.

Die EU macht Druck

Am 16. März 2016 brachte eine Verlautbarung des Gerichtshofes der Europäischen Union mehr Handlungsdruck in den deutschen Parteienstreit: „Nach Ansicht von Generalanwalt Szpunar ist der Betreiber eines Geschäfts, einer Bar oder eines Hotels, der der Öffentlichkeit ein WLAN-Netz kostenlos zur Verfügung stellt, für Urheberrechtsverletzungen eines Nutzers nicht verantwortlich. Zwar könne der Betreiber durch eine gerichtliche Anordnung verpflichtet werden, diese Rechtsverletzung zu beenden oder zu verhindern, doch könne weder die Stilllegung des Internetanschlusses noch seine Sicherung durch ein Passwort oder die allgemeine Überwachung der Kommunikation verlangt werden".

Der Auslegung des EU-Generalanwaltes Maciej Szpunar zufolge greift diese Haftungsbeschränkung, wenn „drei kumulative Voraussetzungen erfüllt sind: 1. Der Anbieter von Diensten hat die Übermittlung nicht veranlasst. 2. Er hat den Adressaten der Übertragung nicht ausgewählt. 3. Er hat die übermittelten Informationen nicht ausgewählt oder verändert."

Nun die entscheidende Passage: Der EU-Generalanwalt ist der Auffassung, dass „diese Haftungsbeschränkung auch für eine Person wie Herrn McFadden gilt, der als Nebentätigkeit zu seiner wirtschaftlichen Haupttätigkeit ein WLAN-Netz betreibt, das der Öffentlichkeit unentgeltlich zur Verfügung steht. Nach Ansicht des Generalanwalts ist es nicht erforderlich, dass diese Person gegenüber der Öffentlichkeit als Anbieter von Diensten auftritt oder für ihre Tätigkeit bei potenziellen Kunden ausdrücklich Werbung macht."

Diese Haftungsbeschränkung stehe „nicht nur einer Verurteilung des Vermittlers zur Leistung von Schadensersatz entgegen, sondern auch seiner Verurteilung zur Tragung der Abmahnkosten und der gerichtlichen Kosten im Zusammenhang mit der von einem Dritten begangenen Verletzung des Urheberrechts."

Erste Reaktionen

Bei den Zitaten handelt es sich zwar noch nicht um finale Gesetze oder Urteile, aber um richtungsweisende „Schlussanträge des Generalanwalts in der Rechtssache C-484/14" des Tobias McFadden, der ein Geschäft für Licht- und Tontechnik unweit von München betreibt, in dem er ein öffentlich zugängliches WLAN-Netz bereitstellt. Ein Streit mit der Sony Music Entertainment Germany GmbH über einen rechtswidrigen Download eines Dritten über McFaddens kostenlosen WLAN-Hotspot war vor dem Landgericht München I gelandet. Dieses hat sich Rat beim Gerichtshof der EU eingeholt. Die Antworten des Generalanwalts Szpunar vom 16. März 2016 auf den Einzelfall McFadden haben der deutschen Politik nun eine WLAN-freundliche Richtung vorgegeben.

Die frohe Kunde vom Ende der Störerhaftung löste in weiten Kreisen Deutschlands Freude aus. Bitkom-Hauptgeschäftsführer Dr. Bernhard Rohleder kommentierte noch am selben Tag: „Die Neuregelung macht den Weg frei für den Ausbau von WLAN-Hotspots in Cafés, Restaurants, Geschäften oder anderen öffentlich zugänglichen Einrichtungen." Zudem erleichtere sie Kommunen das Angebot öffentlicher WLAN-Bereiche.

Die Grünen jubelten auf ihrem GrünDigital-Blog darüber, „dass die Union ihre jahrelange Blockade in Sachen Störerhaftung nun offenbar endlich beendet hat. Es war mehr als überfällig, ein Konstrukt zu beseitigen, das in der Vergangenheit zu einer erheblichen Rechtsunsicherheit für die Anbieter und Nutzer von Funknetzen geführt hat."

Laut SPD-Blog hat sich die Regierungskoalition „darauf verständigt, mit einer Änderung des Telemediengesetzes klarzustellen, dass WLAN-Anbieter als Access Provider anzusehen sind und dass diese die Haftungsprivilegierung für Access Provider beanspruchen können und keinen weiteren Prüfpflichten unterliegen. […] Da das deutsche Recht keine Unterscheidung zwischen gewerblichen oder privaten Anbietern kennt, gilt diese Klarstellung für alle Betreiber, die ein freies WLAN anbieten."

Die sogenannte Haftungsprivilegierung für Access Provider galt bisher nämlich nur für größere WLAN-Betreiber: etwa für die

Deutsche Telekom, Telefonica oder Vodafone (vormals Kabel Deutschland). Deren WLAN-Hotspots sind aber meist kostenpflichtig und außerdem nicht wirklich flächendeckend.

Das Gastgewerbe steht in den Startlöchern

Viele Top-Hotels haben schon seit Jahren langfristige WLAN-Verträge mit bekannten Access Providern abgeschlossen, weil sie die technischen und rechtlichen Probleme eines Hotel-Funkhotspots mit ständig wechselnden Surfgästen nicht selber tragen wollen.

Im Gegenzug zahlen einige Spitzenhotels noch immer bis zu 30 Euro pro Nacht und belegtem Zimmer an ihren WLAN-Provider, obwohl sie Ihren Gästen heutzutage kaum noch WLAN gesondert auf die Rechnung schreiben können, schon gar nicht auf der Executive-Etage, wo sogar der Schampus rund um die Uhr im Zimmerpreis enthalten ist. Solche Altverträge schmerzen auch Manager teurer Hotels, die bei sich zu Hause für 30 Euro doch einen ganzen Monat lang schnelles Internet samt WLAN-Router-Miete bekommen.

Laut DEHOGA wollen die Koalitionsparteien den Ausschluss der Störerhaftung für offenen WLAN-Zugriff sogar „ohne technische Hürden wie eine Zugangsverschlüsselung oder eine Vorschaltseite […] ermöglichen.“ Der WLAN-Router muss also technisch nicht viel können.

Alte Verträge und neue Gästenetze

Also könnte der Hotelier nach Wegfall der Störerhaftung sogar den billigsten und technisch einfachsten WLAN-Router für seine Gäste installieren – sofern er aus seinem langfristigen WLAN-Provider-Vertrag herauskommt. In solchen Verträgen haben etliche Hotels nämlich schon vor Jahren unterschrieben, dass weder das Hotel selber, noch dessen Gäste ein anderes als das vom Provider betriebene WLAN innerhalb der Hotelmauern nutzen dürfen. Theoretisch darf der Gast in solchen Hotels nicht einmal den kleinen WLAN-Hotspot seines LTE-Smartphones einschalten. Im wirklichen Leben bringen aber viele Veranstalter und Aussteller ihre eigenen Router in die Hotels mit, um etwa in Konferenzen und Foyer-Ausstellungen eigenes WLAN zu betreiben. Die Hotels müssten das eigentlich kontrollieren und verbieten, schauen aber meist nicht so genau hin, in der Hoffnung, dass der offizielle Provider des Hotels die „fremden“ WLAN-Funker nicht bemerkt oder zumindest stillschweigend duldet.

UPDATE MIT UNTERLASSUNG

Es bleibt zum Redaktionsschluss Ende Mai nur zu hoffen, dass die Politik das Konzept nicht in letzter Sekunde wieder verwässern wird. Die ursprüngliche Freude ist bereits deutlich gedämpft. Der Antrag der Koalition vom 31. Mai 2016 nämlich, mit dem der § 8 TMG (Telemediengesetz) entsprechend geändert werden soll, beschränkt sich auf die Ausdehnung des Providerprivilegs: Cafés, Frisörsalons, Hotels, Arztpraxen und alle anderen, „die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen“ (Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes), sind damit als Diensteanbieter für Rechtsverstöße Dritter in ihrem WLAN prinzipiell nicht verantwortlich. Damit zeichnet sich aber auch ab, dass sie nicht vor Unterlassungsansprüchen sicher wären – und genau diese sind die Grundlage der grassierenden WLAN-Abmahnungen, wie netzpolitik.org und heise online sofort erkannt haben.

Während rein private WLANs in der Regel durch die WPA2-Verschlüsselung recht zuverlässig gegen unerwünschte Eindringlinge abgeschottet sind, ist ein offenes WLAN – ohne Verschlüsselung und ohne Vorschaltseite – natürlich im Gegenteil genau dazu gedacht, dass jeder Surfgast ruckzuck ohne technische Probleme ins Netz kommen kann.

Dem frischgebackenen WLAN-Betreiber ist daher zu raten, durch eine strikte Trennung der beiden Netze den Surfgast klar von seinen eigenen Rechnern, Smartphones und Tablets fernzuhalten. Manche WLAN-Router, etwa viele Fritz!Boxen von AVM, bieten zu diesem Zwecke schon ab Werk einen weitgehend vorkonfigurierten „Gastzugang“ an, der das Gäste-WLAN vom internen Netz virtuell trennt.

Laute Freude bei den WLAN-Herstellern

Mit dem Wegfall der Störerhaftung dürften sich bald viele Privatleute, Vereine, Praxen, Gemeinden, Handwerker und Ladengeschäfte trauen, in Eigenregie einen kostenlosen WLAN-Hotspot für Gäste, Freunde oder Kunden anzubieten. Dürfen sich die Hersteller deshalb auf mehr Umsatz mit WLAN-Routern (oder mit Security-Lösungen) freuen?

Jan Koch, Technical Presales Consultant, TP-LINK Deutschland, kommentierte am 12. Mai 2016 durch Versand einer Presseinfo: „Als Hersteller von WLAN-Geräten freuen wir uns, dass es in Deutschland künftig mehr offene WLAN-Hotspots geben wird. Jedoch gerade als Netzwerkexperten warnen wir auch vor den Risiken, die entstehen, wenn das WLAN-Netz für Gäste nicht ausreichend vom eigenen Heimnetz getrennt ist. Stichworte sind hier etwa unbefugter Zugriff ins private Netzwerk oder Virenbefall. Besitzer von Cafés oder Ladengeschäften sollten also auf Nummer sicher gehen, zum Beispiel mit Lösungen unserer Partner wie Socialwave, Hotsplots oder Freefii.“

Andreas Zießnitz, Product Manager WLAN beim deutschen WLAN-Marktführer AVM aus Berlin, kommentierte gegenüber teltarif.de: „WLAN wird mit dem Wegfall der Störerhaftung im Herbst noch stärker zum kabellosen Standard – auch unterwegs. Aus anderen Ländern kennt man die Vorzüge der einfachen Hotspot-Nutzung. Abgesehen davon können Cafés oder Arztpraxen ihren Besuchern mit einer Fritz!Box bereits jetzt ganz einfach einen WLAN-Gastzugang anbieten, der unabhängig und sicher isoliert vom eigenen Netzwerk ist. Fritz!Box bietet Betreibern von WLAN-Hotspots dabei viele Optionen: Wahlweise nutzen Gäste den Zugang ohne weitere Anmeldung. Alternativ ist eine Anmeldung per Passwort, QR-Code oder sogar NFC-Chip möglich. Auch eine Vorschaltseite mit Logo des Betreibers ist setzbar. Über die Fritz!Box-Oberfläche kann er nachvollziehen, wann und womit der Gastzugang benutzt wurde.“

Das Schweigen der Enterprise-Anbieter

Die Hersteller von teuren Enterprise-WLAN-Access-Points, etwa Aruba, Cisco, HP, Lancom Systems oder Zebra Technologies, haben offenbar keine spontanen Kommentare zur Abschaffung der Störerhaftung an die Presse verschickt. Die professionellen WLAN-Hotspot-Provider ebenfalls nicht. Vielleicht werden diese Profianbieter mit komplexen Produkten ja nicht so viel profitieren, wenn die juristischen und damit auch die technischen Hürden eines offenen WLAN-Hotspots bald vereinfacht werden.

Aus Sicht der gesamten Wirtschaft jedoch „ist das eine überaus gute Nachricht, denn jahrelang war Deutschland im Vergleich zu anderen Ländern eine echte Hot-Spot-Wüste“, lobt etwa Oliver Süme, Vorstand Politik & Recht beim eco-Verband der Internetwirtschaft e.V., die Abschaffung der WLAN-Störerhaftung.

Dr. Harald Karcher,
freier Mobile-Communications-Tester

WLAN-Surfen auf dem Wasser

Die Bayerische Seenschifffahrt funkt mit LTE-to-WLAN-Routern

Auf dem Ammersee, Tegernsee, Königssee und Starnberger See gibt es seit 2015 kostenlose WLAN-Hotspots. 2015 probierten wir den staatlichen Internet-Service zunächst als End User mit Smartphone und Laptop aus. 2016 blickten wir mit einem Wifi Analyzer etwas tiefer in das technische Design der WLAN-Installation.

Der bayerische Finanzminister Dr. Markus Söder kündigte bei der Freischaltung des ersten WLAN-Netzes auf einem staatseigenen Schiff am 7. April 2015 in Starnberg an, es könne fortan „kostenlos auf den Schiffen der Bayerischen Seenschifffahrt im Internet gesurft werden. […] Ein innovatives und modernes Zusatzangebot für alle Schiffspassagiere." So können die Fahrgäste Informationen zu den Sehenswürdigkeiten am Ufer direkt abrufen, Erinnerungsfotos sofort an Freunde und Verwandte versenden oder Anschlussverbindungen prüfen. Alle sechs Schiffe der weißblauen Flotte auf dem Starnberger See würden in der Saison 2015 freies WLAN anbieten, sagte der Minister damals. Nun wird dieser kostenlose Service auch 2016 fortgeführt.

LG G4 grüßt @BayernWLAN

Am 9. August 2015 waren wir erstmals mit dem Android-Smartphone LG G4 auf der MS Seeshaupt, Baujahr 2012, und absolvierten die große Rundfahrt Starnberg–Seeshaupt–Starnberg: ein wirklich schönes Vergnügen mit Erholungswert, besonders wenn das Wetter passt. Das Schiff war auch viel nobler als erwartet, mit Klimaanlage, Sonnendeck, Liegestühlen, Restaurant, Café, Bar und Platz für 800 Personen. Wer nur nostalgische Dampfer in Erinnerung hat, sollte sich mal diese MS Seeshaupt zu Gemüte führen. Sie ist das modernste Schiff auf dem Starnberger See.

Am Schiffseingang klebte anno 2015 noch eine Folie mit der Aufschrift „BAYERN WLAN kostenloser Hotspot" in leicht verblasstem Weißblau. Daneben ein Rauchverbot in knalligem Weißrot. 2016 war diese Folie weg, dafür gibt es jetzt im Inneren des Schiffes ein viel professionelleres Plakat mit derselben Aufschrift, direkt neben der Garderobe im EG, am Abgang in das UG Richtung Toiletten.

Auf dem LG G4 mit eingebautem WiFi-11a/b/g/n/ac kamen auf Anhieb gleich beim Start der Rundfahrt am 9. August 2015 zwischen Starnberg und Berg drei WLAN-SSIDs namens „@BayernWLAN", „Fritz!Box WLAN 3030 (YCP)" und „Yachtclub" auf das Handy-Display. Wir tippten auf das @BayernWLAN-Funknetz, und damit hat sich das LG G4 ruckzuck verbunden. So viel zu den WLAN-Einstellungen.

Landung auf der Landingpage

Zum Surfen im Internet tippten wir dann auf den Handy-Browser. Da kam aber nicht die übliche Startseite, auch nicht die zuletzt besuchte Webseite, sondern die Startseite der Bayerischen Seenschifffahrt. Das ist normal in einem professionellen WLAN-Hotspot, das ist ein sogenannter Forced Redirect, eine vom WLAN-Netzwerk automatisch er-

Quelle: Harald Karcher

Rechts über der weißen Mütze des Kapitäns erkennt man eine mannshohe LTE-UMTS-Antenne auf dem Dach des Seehotels Leoni. Aus solchen stationären Mobilfunkantennen wird der schwimmende WLAN-Hotspot mit dem schnellen Internet vom Lande her versorgt.

zwungene Umleitung des Browsers auf die Landingpage des WLAN-Betreibers.

Im Handy-Browser entzifferten wir 2015 beim Redirect den Anfang einer URL namens https://portal.m3c… Das klingt nach einem staatsexternen Access Provider namens www.m3connect.de. Das ist ein deutscher Anbieter von Internet-Technologie für den Hospitality-Markt aus Aachen.

Zurück zum Handy. Wir akzeptierten die Allgemeinen Geschäftsbedingungen und klickten auf „Kostenfreier Zugang“. Prompt kam die Handy-optimierte Webseite der Seenschifffahrt. Danach wurden alle bayerischen Seen zur Auswahl angeboten, auf denen die Bayerische Seenschifffahrt agiert, nämlich: Königssee, Tegernsee, Starnberger See und Ammersee. Wir nahmen den Starnberger See und fanden dort unter anderem den aktuellen Fahrplan und eine Seeskizze.

Messfahrten 2015: Saison der Ausfälle

Nach der Hotspot-Landingpage wechselten wir zum Ookla Speedtest. Damit bekamen wir im August 2015 Downloads von circa 1 MBit/s, Uploads von 1,44 bis 1,69 MBit/s und Ping-Zeiten von 61 bis 71 ms. Das reicht auf alle Fälle zum Mailen, Surfen und für Social Media Postings.

Beim zweiten Test am 22. August 2015 hatten wir per Zufall wieder das modernste Schiff erwischt, die MS Seeshaupt. Aber das @BayernWLAN war nicht mehr zu finden. Kann ja mal vorkommen, dass ein WLAN-Hotspot spinnt.

Beim dritten Test am 30. August 2015 wollten wir erneut den Surf-Speed auf dem schwimmenden @BayernWLAN testen. Diesmal erwischten wir den Vorzeigekatamaran MS Starnberg, Baujahr 2004. Das schöne Schiff auf zwei Außenrümpfen wirkt nicht ganz so brandneu wie die MS Seeshaupt. Trotzdem vermittelt auch dieses 1000-PS-Gefährt einen Hauch von Kreuzfahrtfeeling. Nur leider war auch dort das kostenlose @BayernWLAN nirgends zu finden.

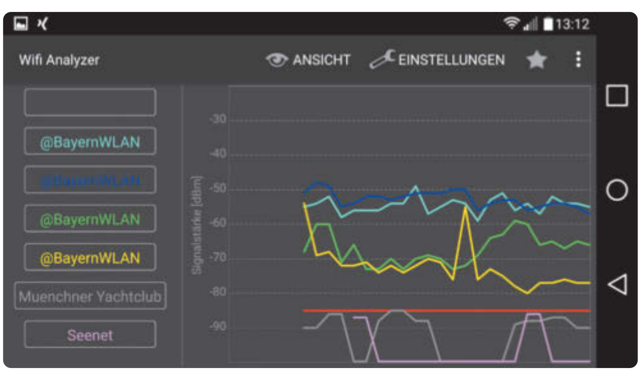
Laut Auskunft der Besatzung war der WLAN-Hotspot wegen technischer Probleme und Störungen der Schiffselektronik vorübergehend abgeschaltet. Der eine meinte, Schiffskabel und WLAN-Kabel störten sich gegenseitig. Ein anderer meinte sinngemäß: „Wir haben noch keine Order bekommen, dass wir das WLAN wieder einschalten dürfen. Probieren Sie es doch mal auf der MS Bayern, das ist unser ältestes Schiff, Baujahr 1939 bis 1948, kriegsbedingt, dort funktioniert das WLAN noch.“ Nun ja, eine vierte Messfahrt auf dem wunderbaren Lago di Starnberg schafften wir anno 2015 dann doch nicht mehr.

Messfahrt 2016: WLAN aus LTE

Neues Jahr, neues Glück: Beim nächsten Test am 31. März 2016 funktionierte das kostenlose @BayernWLAN auf der modernen MS Seeshaupt wieder auf der kompletten Rundreise über drei Stunden hinweg mit minimalen Aussetzern gut. Ganz mit Absicht verwendeten wir zum Test wieder das gleiche LG-G4-Smartphone wie 2015. Damit kamen 2016 bis zu 2,03 MBit/s im Download und bis zu 2,38 MBit/s im Upload bei flotten 47 ms Reaktionszeit.

Zudem hatten wir im März 2016 einen 4K-Laptop Toshiba Satellite P50t-C-104 mit Windows 10 dabei. Die Durchsatzwerte waren damit marginal geringer als mit dem LG G4. Die Darstellung der Hotspot-Landingpage und weiterer Webseiten war auf dem großen Windows-10-Laptop mit dem neuen Microsoft-Edge-Browser aber komfortabler und kompletter als auf dem weitaus kleineren Smartphone-Display mit Android 6.0.

Egal ob Smartphones, Tablets oder Laptops im @BayernWLAN surfen: Die Fernanbindung des schwimmenden WLAN-Hotspots klingt – bei Speed-Werten um die 2 MBit/s und Ping-Zeiten um die 50 ms – auf alle Fälle sehr nach LTE. Lediglich in der Nähe wenig besiedelter



Quelle: Harald Karcher

WLAN-Signalstärkeverlauf auf der MS Seeshaupt am 18. Mai 2016: Die vier obersten Funkzellen mit den identischen Namen @BayernWLAN zeichneten wir im ersten OG auf dem Zwischendeck auf. Sie stammen direkt aus dem Linienschiff. Die beiden Funkzellen unten strahlten von außen herein.

Quelle: Harald Karcher

Mit diesem Signalstärke-Meter des Wifi Analyzers kann man eine Funkzelle aus dem @BayernWLAN herauspicken und den AP suchen, aus dem heraus diese WLAN-Wolke funkt. Genauer gesagt: die Antenne. Je stärker die Nadel nach rechts ausschlägt, desto näher ist man der gesuchten Antenne.

EIGENER FRITZ!BOX-HOTSPOT AUF @BAYERNWLAN-SCHIFF

Wenn der professionelle WLAN-Hotspot der Seenschifffahrt das @BayernWLAN aus LTE speist, müssten wir das doch auch können. Konkret gefragt: Könnte die kleine Fritz!Box 6820 LTE für 199 Euro (die wir für dieses Heft eingehend getestet haben – siehe Seite 24) mit eingesteckter SIM-Karte von Vodafone zur Not auch eine große MS Seeshaupt mit Internet versorgen?

Am 21. Mai 2016 nahmen wir gegen 16:40 Uhr die Zwei-Stunden-Rundfahrt Starnberg–Tutzing und zurück. Im verglasten Gästebereich des OG fanden wir eine freie Steckdose. Daran ließen wir die Fritz!Box hochfahren, allerdings nicht unverschlüsselt offen für alle Gäste, sondern stark verschlüsselt mit WPA2. Die Gründe: Erstens die unsägliche WLAN-Störerhaftung, zweitens wollten wir die surfwilligen Schiffsgäste nicht mit einem zweiten Hotspot verwirren, drittens wollten wir bei den Speed-Messungen nur einen einzigen User im WLAN haben, um die Höchstwerte bei Speed und Pingzeiten zu bekommen.

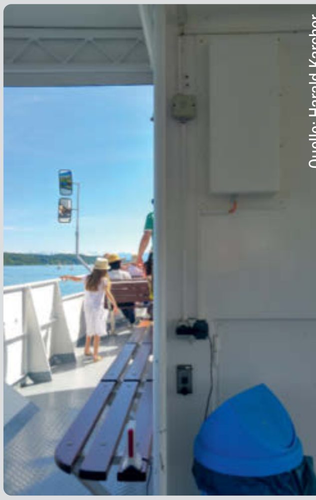
Noch unvollständig, aber deutlich schneller

Ergebnis: Die kleine Fritz!Box 6820 LTE mit nur einer einzigen 802.11-b/g/n-Funkzelle versorgte mehr als die Hälfte der Schiffsflächen im EG, OG und DG immerhin so gut, dass flottes WLAN-Surfen mit einem LG-G4-Smartphone möglich war. Bei Werten bis 20 MBit/s im Download und 10 MBit/s im Upload war das Surfen im EG sogar bis zu knapp zehnmal schneller als über den offiziellen Schiffshotspot, obwohl die Fritz!Box beim Test im OG des Schiffes stand. Allerdings war im Test halt nur ein einziger User, nämlich der Tester, in der Funkzelle der AVM-Box eingebucht.

Lediglich in den hinteren Bereichen des Schiffes unweit der Dieselmotoren sowie mittig auf dem Sonnendeck funkte die kleine AVM-Box erheblich schwächer als die offizielle WLAN-Installation. In diesen Bereichen bremsten massive Stahlflächen die AVM-Box wohl stärker aus als das offizielle WLAN aus den Access Points des Enterprise-WLAN-Herstellers Lancom Systems. Würde man jedoch weitere LTE-to-WLAN-Router der Gattung Fritz!Box 6820 LTE gezielt an den schwächsten WLAN-Stellen (mittig auf dem Sonnendeck sowie ganz hinten auf dem Schiff) positionieren, dann hätte man mit einigen wenigen AVM-Böxchen ebenfalls die Chance auf eine WLAN-Komplettversorgung der MS Seeshaupt.

WLAN-Ausfall mit Mini-Hotspot überbrücken

Das krasse Beispiel soll nicht gegen starke WLAN-Hotspots von professionellen WLAN-Providern argumentieren. Es soll nur zeigen – und Mut machen –, dass man nach Wegfall der WLAN-Störerhaftung auch schon mit handtellerkleinen LTE-to-WLAN-Routern ruckzuck brauchbare, öffentliche Hotspots aufspannen kann. Im Jahr 2015 hätte man also den WLAN-Ausfall mit zwei, drei kleinen LTE-to-WLAN-Routern weitgehend kompensieren und überspielen können. Dazu hätte man den SSID-Netzwerknamen in der Fritz!Box nur von der Werkseinstellung („Fritz!Box 6820 LTE“) auf den SSID-Namen „@BayernWLAN“ überschreiben müssen: Dann hätte kaum jemand gemerkt, dass der offizielle Hotspot wochenlang nicht funkte.



Quelle: Harald Karcher

Rechts oben in dem weißen Kasten hängt der offizielle WLAN-Hotspot der MS Bernried. Daraus kam beim Vergleichstest zwar genug WLAN-Strahlung. Unser LG G4 konnte von diesem @BayernWLAN aber keine IP-Adresse beziehen und somit auch kein Internet. Links unten auf der Sitzbank steht der eigentliche Testanlass, der kleine LTE-zu-WLAN-Router Fritz!Box 6820 LTE.

Regionen im Süden des Sees fiel der Durchsatz drastisch ab. Da schaltete der WLAN-Hotspot vermutlich von LTE auf UMTS herunter.

Der schwächste Wert kam zwischen Seeshaupt und Bernried mit 0,34 MBit/s im Download und 0,09 MBit/s im Upload bei lahmen Ping-Zeiten von 202 ms. Auf alle Fälle muss im Schiff ein LTE-zu-WLAN-Router verbaut sein, der bei Bedarf auf ältere Mobilfunknormen wie HSPA oder UMTS herunterschalten kann (siehe Kasten).

Testfahrt mit WiFi Analyzer

Am 18. Mai 2016 wollten wir mit dem WiFi Analyzer auf dem LG-G4-Handy mal hinter die Kulissen des @BayernWLAN-Hotspots auf der MS Seeshaupt schauen. Also same procedure as every year, große Rundfahrt Starnberg–Seeshaupt hin und zurück. Fahrzeit ohne Ausstieg, ohne Unterbrechung 13 bis 16 Uhr. Um 13:03 Uhr waren wir auf dem Zwischendeck im ersten OG angekommen. Das Handy meldete wieder: @BayernWLAN. Jetzt aber: Signalstärke ausgezeichnet.

Oha! So stark hatten wir das @BayernWLAN ja noch nie wahrgenommen. Hatte hier jemand das Netz optimiert? In allen wichtigen Bereichen der MS Seeshaupt, in denen sich die Passagiere länger aufhalten, fanden wir am 18. Mai eine recht brauchbare und fast lückenlose WLAN-Versorgung. Das @BayernWLAN stellte fast nonstop Internet mit einem guten Speed um die 2 MBit/s zur Verfügung, was den meisten Menschen zum Surfen, Mailen und für Social Media unterwegs reichen dürfte. Gelegentlich gab es auch Aussetzer beim Internet, was beim Surfen, Musik- oder Videostreaming stören kann, beim reinen Mail-Empfang dagegen kaum auffällt.

Bei unserem Test am 18. Mai 2016 war die MS Seeshaupt maximal zu einem Drittel mit Gästen besetzt. Augenscheinlich blickten an diesem Tag auch erfreulich wenig Leute nonstop in ihre Handys – und wenn doch, dann eher zum Fotografieren als zum Surfen. Es wäre aber spannend, wie der WLAN-Hotspot reagiert, wenn das Schiff mal voll mit 800 Leuten besetzt ist und die Hälfte davon sich die Sportschau oder ein YouTube-Video anschauen will.

Egal wie gut das Internet auf dem Schiff auch sein mag: Das Schönste ist am Ende aber immer noch der See, das Ufer und die Landschaft, besonders wenn die Sonne scheint und es einen klaren Föhnblick auf das Alpenpanorama gibt.

Dr. Harald Karcher,
freier Mobile-Communications-Tester

Breitbandausbau unter Zeitdruck

VDSL2-Vectoring ist schnell, kostengünstig und umstritten

Die Bundesregierung hat versprochen, dass bis 2018 allen Bundesbürgern ein schneller Internetzugang mit mindestens 50 MBit/s im Download zur Verfügung steht. Um das in weniger als zwei Jahren umsetzen zu können, bietet die Deutsche Telekom an, die bestehenden Kupferanschlüsse mit der Vectoring-Technik aufzurüsten.

Für Vectoring benötigt ein Betreiber jeweils einen exklusiven Zugang zu den Hauptverteilern (HVt) mit direkten A0-Teilnehmeranschlüssen sowie zu den Kabelverzweigern (KVz) im Nahbereich eines HVTs. Und nach dem Stand der Dinge wäre dies vornehmlich die Deutsche Telekom. Diese hat letztes Jahr bei der Bundesnetzagentur beantragt, die vorhandenen Kupferleitungen rund um ihre etwa 8000 HVt mit VDSL2-Vectoring nach ITU-T G.993.5 auszustatten. So könnten etwa 6 Millionen Haushalte in Städten einen schnellen Internetanschluss bis 100 MBit/s nutzen. Im ländlichen Raum sind es in der Regel 50 MBit/s, die maximal über 500 bis 650 m Kupferkabel übertragen werden können.

Die Bundesnetzagentur reichte den 300-seitigen, etwas überarbeiteten Antrag der Deutschen Telekom am 20. April bei der Europäischen Kommission zur Genehmigung ein. Diese hat im Mai ein sogenanntes „Serious-Doubts-Verfahren" dazu eingeleitet. Das gibt der EU-Kommission nun drei Monate Zeit zu prüfen, ob das geplante Vorgehen bei der Umstellung auf DSL2-Vectoring dem EU-Recht entspricht. Branchenverbände wie BREKO (Bundesverband Breitbandkommunikation e.V.) oder BUGLAS (Bundesverband Glasfaseranschluss e.V.) sehen darin eine Beschneidung des freien Wettbewerbs.

Eine Kostenfrage der Kabellängen

Denn Vectoring funktioniert nur für das komplette Kupferkabelbündel vom KVz zu den Teilnehmeranschlüssen. Dabei kompensiert das Verfahren das Übersprechen zwischen den einzelnen Kabeln im Bündel. Dazu werden die Übersprechsignale am Teilnehmerende der Kabel vom DSLAM aus gemessen und jeweils zusätzliche Signale erzeugt, die dieses Übersprechen praktisch auslöschen. Die so bereinigten VDSL-Signale können nicht nur 150 bis 300 m weit über Kupferleitungen übertragen werden, sondern bis zu 500 oder gar 650 m.

EXTRA-DSLAMS NACH KABELLÄNGE

Die für einen Landkreis exemplarisch ermittelten zusätzlich benötigten DSLAM-Standorte für den 50 MBit/s-Ausbau

Übertragungsart	Max. Distanz bei 50 MBit/s	Zusätzlich benötigte DSLAM-Standorte
VDSL pessimistisch	150 m	+ 750 %
VDSL optimistisch	300 m	+ 230 %
Vectoring pessimistisch	500 m	+ 65 %
Vectoring optimistisch	650 m	+ 20 %

Quelle: Dr. Roland Wessäly, Atesio Berlin; ITG-Fachtagung Berlin, April 2016

Diese Längenangaben für die Kupferleitungen sind laut Dr. Roland Wessäly von Atesio in Berlin die derzeit üblichen Annahmen. Er sprach auf der 10. ITG-Fachkonferenz des VDI Mitte April in Berlin über kostenoptimierte FTTx-Verkabelungen für Landkreise. Für genaue Längenangaben müsse man am verlegten Kabelbündel den Bit-Durchsatz messen, da die Dämpfung im Kabel von mehreren Parametern abhänge. Geht der Planer davon aus, dass 50 MBit/s mit Vectoring über Distanzen bis 650 m übertragbar sind, kann der Netzbetreiber gegenüber 500 m langen Distanzen fast 50 % an Investitionen einsparen. Stellt sich aber heraus, dass der Teilnehmer keine 50 MBit/s im Download erhält, ist dieser Netzausbau nicht förderungswürdig. Der Investor müsste dann die bewilligten Fördergelder zurückerstatten. Dr. Wessäly hat für einen Landkreis exemplarisch errechnet, dass bei maximal 500 m langen Kabeln etwa 65 % zusätzliche DSLAM-KVz notwendig wären. Bei maximal 650 m langen Kabeln seien es dagegen nur 20 %.

Nicht wirtschaftlich realisierbare Anschlüsse

In städtischen Bereichen mit einem dichten Verteilernetz ist Vectoring die am schnellsten und kostengünstigsten zu realisierende Technik, um dem Teilnehmer 50 MBit/s bereitzustellen. Doch die Deutsche Telekom geht davon aus, dass die Ausrüstung aller Hauptverteiler mit direkten Teilnehmeranschlüssen sowie der Kabelverteiler in deren Nahbereich rund 1 Milliarde Euro kosten wird und nicht überall wirtschaftlich realisiert werden kann. Wenn die Telekom oder ein Landkreis oder Zweckverband als Betreiber im ländlichen Raum ein Breitbandnetz plant, erhält der Betreiber für nicht wirtschaftlich realisierbare Anschlüsse Fördergelder. Doch dafür muss erst einmal ermittelt werden, welche Anschlüsse davon betroffen sind. In der Regel betrifft das etwa 10 bis 15 % aller Haushalte und Gewerbebetriebe in einem Verteilernetz.

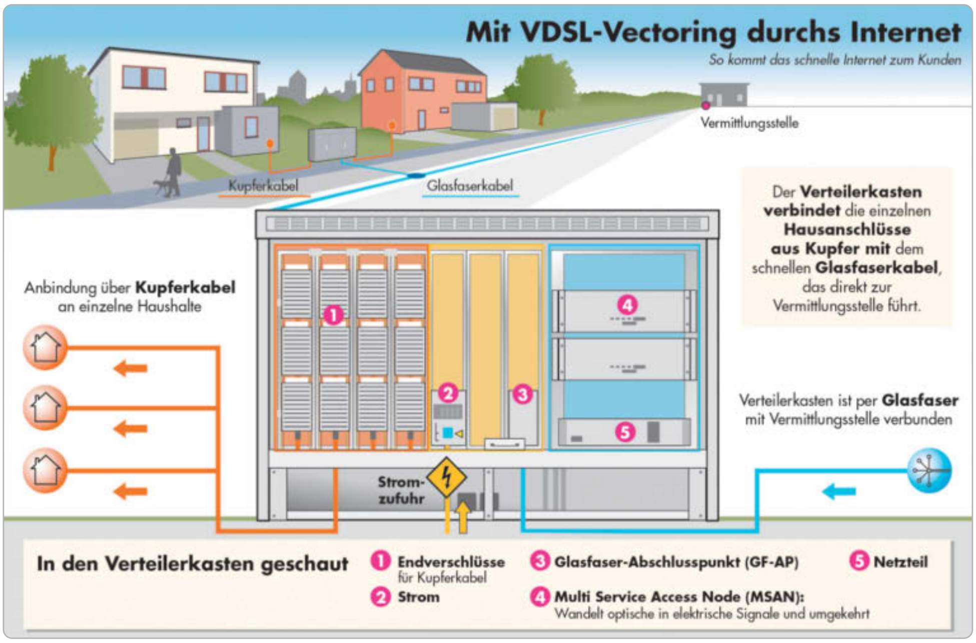
Für die Ermittlung ist ein Plan des bestehenden Verteilernetzes mit allen Anschlüssen und Verteilerpunkten notwendig. Dabei müssen anhand der bestehenden Trassenwege die Leitungswege der Kupferleitungen vom HVt bzw. KVz bis in die Häuser ermittelt werden. Betragen die Distanzen über 500 bzw. 650 m, müssen andere Verteilerpunkte mit DSLAM gesetzt werden. Dr. Wessäly stellte bei seinen Projekten jedoch fest, dass in der Regel die zusätzlichen Tiefbaumeter unter 1 % liegen, wenn die vorhandenen Trassen so weit als möglich genutzt würden.

Layer-2-Bitstrom statt Wettbewerb

Bei den so errichteten FTTC-Netzen (Fiber to the Curb) können dann jedoch keine Teilnehmeranschlussleitungen mehr an andere Netzanbieter vergeben werden. Diese erhalten nur noch einen Layer-2-Bitstrom als Zugangsprodukt. An diesen IP-Datenströmen kann der zusätzliche Netzanbieter nichts mehr modifizieren und darum auch keinen Mehrwert schaffen. Das ist ein Aspekt, der die Wettbewerber der Telekom verärgert.

Außerdem sieht der von der Bundesnetzagentur überarbeitete Antrag vor, dass der Netzanbieter, der bis zum 31. Januar 2016 mindestens die Hälfte aller KVz im Nahbereich eines HVts errichtet und mit DSL-Technik ausgestattet hat, den gesamten Anschlussbereich des HVts mit Vectoring betreiben darf. Hat die Deutsche Telekom ebenfalls 50 %, fällt dieser HVt an die Telekom. Außerdem erhält die Deutsche Telekom alle HVt ohne KVz im Nahbereich. Als Grundlage für diese Zuteilung führt die Bundesnetzagentur eine deutschlandweite Vectoring-Liste. Für abzugebende KVz erhält der Errichter eine Ausgleichszahlung vom künftigen Betreiber des gesamten HVTs.

Die deutliche Gewichtung zugunsten der Deutschen Telekom begründet die Bundesnetzagentur mit der Marktmacht dieses Netzanbieters. Damit sei es realistisch, dass der flächendeckende Breitbandausbau tatsächlich bis 2018 gelinge. Zudem will die Telekom zum 31. Mai 2016 eine notarielle Erklärung gegenüber der Bundesrepublik Deutschland abgeben und sich dabei einseitig dazu verpflichten, die KVz und A0-Anschlüsse der HVt innerhalb von 18 Monaten nach Abschluss des Überpüfungsverfahrens mit DSL-Technik auszubauen, um VDSL2-Vectoring nach ITU-T G.993.5 zu ermöglichen. Die Erklärung muss im Amtsblatt der Bundesnetzagentur veröffentlicht sein. Die bestehenden Leased Lines der Wettbewerber sollen zum 1. Dezember 2017 gekündigt werden. Es gibt dann nur noch den virtuell entbündelten Zugang zum Teilnehmeranschluss (Layer-2-Bitstrom-Zugang).



Quelle: Deutsche Telekom

Die Aufteilung in einem KVz-Verteilerschrank mit VDSL2-Vectoring

Brückentechnik im Wartestand

Grundsätzlich gerät der FTTB-Netzausbau (Fiber to the Building) damit ins Hintertreffen – und das, obwohl allen Marktteilnehmern bewusst ist, dass Vectoring nur eine Übergangslösung ist. Wenn im August die Prüfungen des Serious-Doubts-Verfahrens der Europäischen Kommission abgeschlossen sind, wird sich zeigen, ob und wie Deutschland auf diese Übergangstechnik setzen darf. Das verzögert natürlich zunächst den weiteren Ausbau.

Doris Piepenbrink,
freie Journalistin, München

Datenkanal statt Telefonleitung

Die Telekom stellt bis 2018 alle Anschlüsse auf die neue IP-Technologie um

Es ist noch gar nicht so lange her, da waren Internet und Telefon getrennte Welten. Das änderte sich, als die Deutsche Bundespost vor rund 20 Jahren das analoge Telefonnetz digitalisierte. Es war die Geburtsstunde von ISDN. Bis 2018 soll nun die Sprachübermittlung komplett in die digitale Welt umziehen.

Ein IP-Anschluss ist heute die Basis von allem, was miteinander kommuniziert und Daten austauscht: vom vernetzten Heim (Smart Home) über Connected Cars bis zu den Aktoren der Industrie 4.0. Zukünftige Netze müssen bis 2020 rund 50-mal so viele Daten transportieren wie heute. Das Internet-Protokoll als einheitlicher Übertragungsstandard für Daten jeglicher Art – Sprache, Video, Musik oder Text – bietet derzeit die optimale Lösung. IP stellt sicher, dass wir weltweit Datenpakete mit völlig unterschiedlichen Inhalten über eine einheitliche Netzplattform verteilen und mit verschiedenen Geräten wie Telefon, Smartphone oder PC nutzen können. Komplexe Netzinfrastrukturen wie in den Zeiten von ISDN, die mehrere Technologien gleichzeitig nutzen, stehen dieser Entwicklung im Weg. Selbst Gerätehersteller verabschieden sich Schritt für Schritt von der bisherigen Technologie, sodass Ersatzteile auf lange Sicht nicht mehr verfügbar sind.

Vorfahrt im Datennetz

So sind in der ISDN-Welt die Netze für die Übertragung der Daten in verschiedene Kanäle aufgeteilt, einer davon ist ausschließlich der Sprache vorbehalten. Das blockiert Bandbreite, auch wenn nicht telefoniert wird. Das IP-Netz dagegen nutzt für alle Datenformate einen gemeinsamen Kanal im Netz. Wird nicht telefoniert, steht die Bandbreite anderweitig zur Verfügung.

Damit es wegen zu geringer Bandbreite oder unterschiedlicher Auslastung bei der Übertragung von Echtzeitanwendungen wie Sprache oder Video nicht zu Störungen oder Abbrüchen kommt, stellt Quality of Service sicher, dass Sprache innerhalb des Internets mit höherer Priorität als Daten übertragen wird. Dazu werden Datenpakete mit Dienstklassen gekennzeichnet. Die Netzwerkservicequalität wird anhand der Parameter Bandbreite, Latenzzeit, Jitter und Paketverlustrate definiert. Priorisierte Datenpakete werden in Routern oder Switches somit bevorzugt weitergeleitet. Für IP-Telefonie etwa, die mit der Klasse 1 priorisiert ist, spielen die Latenz, der Jitter und die Verlustrate eine bedeutende Rolle, weil sie maßgeblich die Sprachqualität beeinflussen. Die Bandbreite hingegen steht nicht an erster Stelle. Bei Annex J etwa, dem splitterlosen Anschluss, ist IP-basierte Telefonie bereits mit DSL 384 möglich.

IM NORMALFALL OHNE UMSTÄNDE

Für Selbstständige und kleine Unternehmen ist die Umstellung auf IP meist wenig aufwendig. Splitter und das Netzabschlussgerät NTBA sind in der Regel überflüssig. In einigen Fällen benötigen Unternehmen einen neuen Router. Am Tag der Umstellung muss das Unternehmen nur die Verkabelung des Routers ändern, die Rufnummern mit gültigen Registrierungs- und Anmeldedaten im Router eintragen und die Festnetztelefonie im Router deaktivieren. Dann gilt es noch zu überprüfen, ob Sonderdienste wie Alarmanlagen, Frankiermaschinen für den automatisierten Postversand oder EC-Cash-Terminals über die Telefonleitung laufen und mit der IP-Technologie kompatibel sind.

Vermittlung und Verfügbarkeit

Das IP-Netz besteht aus drei Komponenten: Dem MSAN (Multi-Service Access Node), in dem Teilnehmeranschlussleitungen zusammenlaufen, dem BNG (Broadband Network Gateway) – der früheren Ortsvermittlungsstelle – und dem IMS (IP Multimedia Subsystem).

Während der MSAN optische in elektrische Signale umwandelt und umgekehrt (Glasfaser – Kupfer) und das IMS die Vermittlungsinstitution darstellt, ist das BNG das Intelligenteste am IP-Netz. Er ersetzt die ehemalige Ortsvermittlungsstelle des Fernsprechnetzes. Die BNGs sind per Glasfaser vermascht. Sie routen die Datenströme direkt zum Ziel-BNG, wodurch die Verfügbarkeit des Netzes steigt. Denn: Früher gingen Sprachdaten von einem Teilnehmer in Hamburg zur Ortsvermittlungsstelle, über die Fernvermittlungsstelle zur Ortsvermittlungsstelle in Köln und dann erst zum Empfänger. Fiel eine der Vermittlungsstellen aus, brach die Verbindung ab. Im IP-Netz gibt es weniger Vermittlungsstellen und damit weniger Verbindungsabbrüche.

Festnetz und Mobilfunk gehen zusammen

Ansonsten bietet IP-basierte Telefonie die gleichen Funktionen wie ein ISDN-Anschluss: zwei Sprachkanäle und standardmäßig drei verschiedene Rufnummern, die sich über den Router verwalten lassen. Rufumleitungen und Sperren lassen sich dank IP einfach selbst einrichten und konfigurieren – auch über das Smartphone, das überhaupt besser kompatibel wird: Bei Bedarf ist man auch auf dem Handy über seine Festnetzrufnummer erreichbar.

Die Einführung der IP-Technologie sorgt ohnehin dafür, dass Fest- und Mobilfunknetz stärker zusammenwachsen. Wurde bisher die Mobilfunktechnik LTE ausschließlich für die Datenübertragung mit hohen Geschwindigkeiten genutzt, laufen Telefongespräche seit einiger Zeit ebenfalls über das schnelle Datennetz (VoLTE).

Dabei ist die IP-basierte Telefonie genauso sicher wie die bisherige ISDN-Technik. Telefonie-Daten laufen über ein eigenes physisches Netz und die Anschlüsse sind registriert und authentifiziert. IP-Telefonie ist also nicht gleich Internet-Telefonie.

Klaus Müller,
Leiter Strategische Entwicklung Geschäftskunden,
Telekom Deutschland GmbH

Anruf im VoIP-LAN

Bei der Telefonie-Umstellung auf All-IP gibt es erwägenswerte Varianten

Die Deutsche Telekom stellt ihr Zugangsnetz nach und nach komplett auf DSL-Technik um. In absehbarer Zeit wird es dort nur noch Kommunikation auf IP-Basis geben. Unternehmen sollten die Migration auf All-IP jetzt angehen, damit sie nicht unter Druck geraten und eine teure Übergangslösung installieren müssen.

Unabhängig davon, auf welche Anbindung und welchen Provider ein Unternehmen migriert – es kann den eigenen Rufnummernblock weiter nutzen. Die Sprachqualität ist bei All-IP-Übertragungen mittlerweile stabil. Bei Verwendung von HD-Voice nach G.722 ist sie sogar besser als bei ISDN-Verbindungen.

Mit der Umstellung auf All-IP wird die Telefonie außerdem deutlich flexibler: Eine Telefonnummer lässt sich auf verschiedene Gerätetypen und Arbeitsplätze oder Standorte umleiten. Für Firmen bedeutet das, dass sie in vollem Umfang Lösungen für Unified Communication and Collaboration (UCC) einsetzen können, die in der Regel alle IP-basiert arbeiten. Das Ausfallrisiko lässt sich minimieren, indem ein Rufnummernblock auf mehrere Server und Standorte verteilt wird. Und verschlüsselte Übertragungen über das IP-Netz bieten zudem mehr Sicherheit als Gespräche im Festnetz.

VoIP-fähiges LAN als Basis

Probleme bereiten allerdings ISDN-Sonderdienste wie Gegensprechanlagen, Brandmeldeanlagen, Frankiermaschinen, Aufzugsysteme, Alarmanlagen sowie das Faxen. Hier müssen IP- oder mobilfunkbasierte Alternativen gefunden werden. Zudem können Analog- oder auch DECT-Geräte über entsprechende Adapter in das IP-Netz eingebunden werden.

Damit die Session-basierte IP-Telefonie im LAN störungsfrei funktioniert, muss dafür ausreichend Bandbreite reserviert sein, etwa über eine Priorisierung per VLAN. Viele Provider raten zu einem eigenen VLAN für die Sprachkommunikation. Damit genügend Bandbreite zur Verfügung steht, sollte das LAN durchgängig mindestens für 100 MBit/s ausgelegt sein. Bei der Einbindung eines WLANs ist es wichtig, dass die Access Points 802.1q (VLANs) und 802.1p (Quality of Service) unterstützen.

Da die Telefonie im LAN integriert ist, hängt ihre Verfügbarkeit direkt von der des LANs ab. Das heißt: Es sollte auf jeden Fall redundant aufgebaut sein, mit mehreren Verbindungen zum IP-Netz des Betreibers. Zudem sollten alle aktiven Netzkomponenten wie Switches, Router und die TK-Anlage mit einer unterbrechungsfreien Stromversorgung abgesichert sein. Das bietet sich auch für IP-Telefone mit PoE-Versorgung (Power over Ethernet) an.

Auf Kompatibilität achten

Fast alle Provider haben mehrere Möglichkeiten im Programm, um die Unternehmenstelefonie auf All-IP umzustellen. Oft kann man sogar die vorhandene TK-Anlage weiter verwenden. Bei einer reinen ISDN-Anlage gibt es zwar entsprechende Adapter zur Anbindung an ein IP-Netz, aber der Leistungsumfang würde sich so schmälern, dass das keine befriedigende Lösung ist. Andererseits haben viele TK-Anlagenhersteller ihre ISDN-Modelle bereits für IP-Technik vorbereitet und bieten entsprechende Module oder Line Cards zur Umstellung auf IP an. Allerdings muss diese Lösung nicht unbedingt kompatibel zum Vermittlungssystem des Providers sein.

Grundsätzlich unterscheiden sich IP-basierte TK-Anlagen sowohl im Funktionsumfang als auch bei der Protokollunterstützung oft ganz erheblich. Selbst die standardisierte SIP-Übertragung ist nicht wirklich einheitlich und führt zu Inkompatibilitäten.

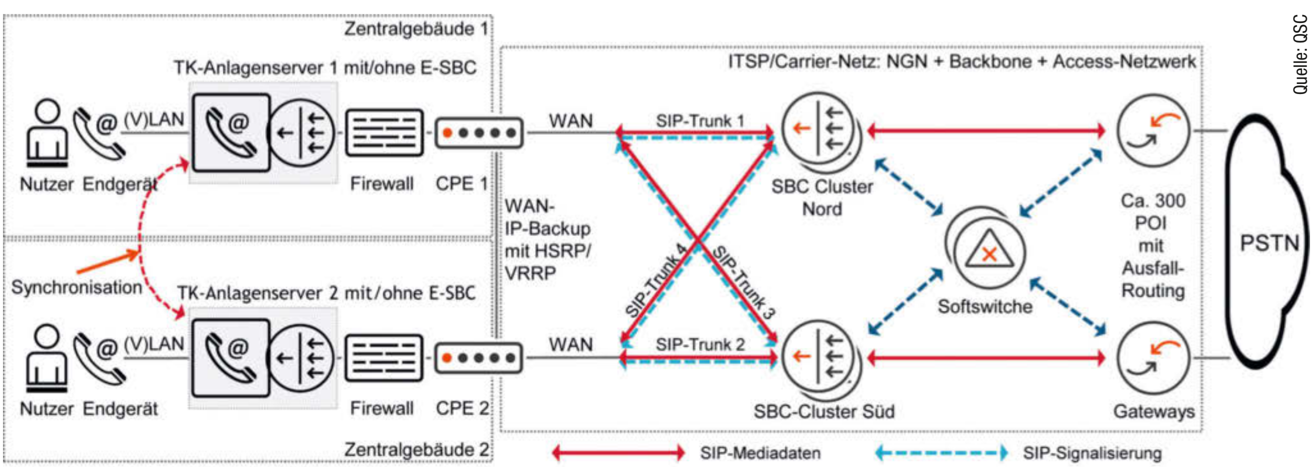
Eine bestehende IP-TK-Anlage lässt sich per SIP-Trunking an das Provider-Netz anbinden. Ein SIP-Trunk bündelt für einen Rufnummernblock und für eine definierte maximale Anzahl an parallelen Rufen die Verbindung zwischen dem Mediation-Server der TK-Anlage und dem SBC (Session Border Controller) am Übergabepunkt zum Provider-Netz. Eine entsprechende Firmware auf dem Mediation-Server und dem SBC regelt dabei die Kommunikation zwischen den beiden Komponenten.

Der SIP-Trunk des Providers kann zum einen über die Internet-Anbindung des Unternehmens geführt werden. In diesem Fall muss die TK-Anlage mit einer Firewall und/oder einem zusätzlichen Enterprise Session Border Controller (E-SBC) vor Internetangriffen geschützt werden. Dabei bleibt ein Port für den Voice-Stream offen. Besitzt die TK-Anlage einen separaten WAN- oder NG-Port, kann auch dieser direkt mit einem Voice-Port des WAN-Routers (Provider) verbunden werden. Die Internetdaten laufen wie gewohnt über die vorhandene Firewall, die in diesem Fall auch nicht umkonfiguriert werden muss. Die Sprach-Sessions gehen über die direkte Verbindung zwischen Voice-Port und TK-Anlage.

Für die Anbindung per SIP-Trunk ist entscheidend, dass TK-Anlage und Vermittlungssystem kompatibel sind. Ist dies der Fall, muss festgelegt werden, in welchen Schritten und mit welchen Schutzmechanismen (Schutzbedarfskategorien gemäß BSI) umgestellt werden soll. Grundsätzlich lässt sich dabei jeder Single Point of Failure beseitigen. Das ist bei einem klassischen ISDN-Anschluss selbst bei Mehrfachabstützung in diesem Maße nicht möglich.

Die Umstellung der TK-Anlage auf SIP-Trunking ist in der Regel ein Projektgeschäft und sollte von Fachleuten geplant und ausgeführt werden. Wenn das Zusammenspiel von TK-Anlage und Vermittlungssystem einmal läuft, wird die Verwaltung einfacher, weil die Telefonie dann ein Teil des LANs ist. Wer sich diesen Aufwand nicht antun möchte oder wessen Wartungsvertrag für die TK-Anlage sowieso gerade ausläuft, der kann auf Cloud-basierte Telefonie umsteigen. Diese Variante ist sehr flexibel, und das ohne Investition in teure Hardware. Wenn die Sicherheitsaspekte und die Einbindung von individuellen Besonderheiten geklärt sind, ist die Cloud-basierte TK-Anlage eines Providers – oft auch „Central PBX“ oder „IP-Centrex“ genannt – eine skalierbare Platform as a Service für praktisch alle Unternehmensgrößen.

Die Anzahl der verwendeten Accounts lässt sich individuell und bedarfsgerecht gestalten. Zudem hat der Anwender die Möglichkeit, andere Cloud-Anwendungen, etwa eine Videokonferenz- oder Groupware-Lösung, mit der TK-Anlagenfunktion zu verbinden. Die Abrechnung erfolgt in der Regel nach dem Pay-per-Use-Prinzip. Alle Anbieter versprechen, dass sich damit die Telefonkosten gegenüber einer herkömmlichen Anbindung per ISDN deutlich senken sollen. Der Kunde benötigt eine redundante Webanbindung und ein auf Voice over IP vorbereitetes LAN. Home Offices sowie kleine Filialen benötigen einen IP-fähigen Router.



CPE = Customer Premises Eqiuppment, HSRP = Hot Standby Router Protocol (Cisco), NGN = Next Generation Network,
ITSP = Internet Telephony Service Provider, PSTN = Public Switched Telephone Network,
SBC = Session Border Controller, VRRP = Virtual Router Redundancy Protocol (RFC 5798)

Bei einer Anbindung per SIP-Trunk lässt sich eine durchgängige Redundanz ohne Single Point of Failure realisieren.

Kriterien der Providerwahl

Bei dieser Lösung liegen verschlüsselte Kommunikation, Datensicherheit und Schutz der Personendaten, zusätzliche Dienste oder Software-Updates in der Hand des Providers. Deshalb ist ein umfassendes Sicherheits- und Verfügbarkeitskonzept des Providers unverzichtbar. Darüber hinaus sollte ein ITK-Verantwortlicher bei der Auswahl des Anbieters darauf achten, dass dieser seinen Sitz in Deutschland hat und nach den Richtlinien des Telekommunikationsgesetzes (TKG) sowie nach dem deutschen Bundesdatenschutzgesetz (BDSG) handelt. Um die Hochverfügbarkeit des Netzes zu gewährleisten, sollte er eine Autonome Systemnummer (AS-Nummer) wie ein ISP vorweisen können und zum Beispiel vom TÜV zertifiziert sein – und keinesfalls dem US-amerikanischen Patriot Act unterliegen. Da man sich gerade bei Spezialanpassungen langfristig an diesen Dienstleister bindet, sollte man nicht gerade ein Start-up wählen und sich Referenzen zeigen lassen.

Je nach Größe und Sicherheitsbedürfnis kann man sein LAN nicht übers Internet, sondern direkt mit dem Rechenzentrum des Providers verbinden (Private Cloud), etwa über eine Ethernet- oder eine MPLS-Verbindung. Da die Telekom in Deutschland das größte Netz hat, ist hier der Direktanschluss am einfachsten möglich. Gehärtete Firewall-Lösungen sind bei Cloud-Anbietern Standard. Einige Provider bieten zudem eine Ende-zu-Ende-Verschlüsselung vom Telefon bis zur Cloud-TK-Anlage an.

Ist das LAN entsprechend vorbereitet, funktioniert die Umstellung der Telefonie im LAN wie der Wechsel einer klassischen Telefonanlage. Der Administrator legt die Teilnehmer über eine webbasierte Oberfläche auf der Anlage an, verteilt die zugehörigen Endgeräte, schließt sie an und konfiguriert sie. Dann werden die Rufnummern von der alten TK-Anlage auf die neue umgestellt. Im Idealfall bekommt jeder User sein Endgerät aus der Gesamtlieferung, und nach der Eingabe eines Benutzernamens und eines Passworts zieht sich das Gerät die für den User vorgesehene Konfiguration selbst.

Spezielle Anpassungen oder die Einbindung von vorhandenen Geräten sind wie beim SIP-Trunking individuell zu lösen. Wie dort lassen sich zum Beispiel DECT-Telefone über entsprechende Adapter weiter nutzen. Für Faxdienste haben alle Provider eine Softwarelösung im Angebot. Viele Anbieter im Businessbereich integrieren analoge Endgeräte und analoge Faxgeräte über Analogadapter.

Da heute fast alle Provider sowohl Cloud-basierte TK-Anlagen sowie SIP-Trunking im Programm haben, kann eine bestehende IP-TK-Anlage weiter betrieben werden. Andere Liegenschaften werden dann über die Cloud angebunden. Ist die vorhandene Anlage kompatibel zur TK-Anlage des Netzbetreibers, ist sogar eine Hybrid-Lösung möglich. Dann können die beiden TK-Anlagen zum Beispiel Besetztlampenfeld-, also Präsenzinformationen austauschen und Rufe zwischen den Anlagen als interne Calls behandeln. Doch TK-Anlagen sind sehr individuelle Geräte. Die Hersteller haben dafür viele und sehr unterschiedliche Software-Releases entwickelt. Deshalb sind hybride Lösungen immer Projektgeschäft.

Doris Piepenbrink,
freie Journalistin, München

Bei Anruf erscheint der Datensatz

Integrierte UC-Systeme arbeiten direkt mit der Business-Software zusammen

Das volle Potenzial von Unified Communications schöpfen Unternehmen erst dann aus, wenn sie ihre Lösung tief in die geschäftlichen Anwendungen integrieren. Der Schlüssel liegt darin, sauber zu definieren, welche Abteilung welche Daten benötigt – und diese dann umfassend durchsuchbar und verfügbar zu machen.

Die richtigen Informationen zur richtigen Zeit können entscheidend sein. Im Unternehmensalltag sind sie vor allem eine Kostenfrage. Und das Potenzial, Zeit und Geld zu sparen, ist groß – bei jedem Telefonat, bei jedem Kommunikationsschritt überhaupt.

Geschäftsanwendungen wie ERP- oder CRM-Systeme sind die Basis nahezu jeder Interaktion mit Kunden, Lieferanten oder Partnern: Bestellungen werden über das ERP-System abgewickelt, vertriebliche Aktivitäten im CRM-System getrackt. Unternehmen, denen es gelingt, die Kommunikation mit ihren Geschäftspartnern direkt mit den zentralen Anwendungen zu verknüpfen, können nicht nur ihre Prozesse nachhaltig verschlanken, sondern auch die Mitarbeiter- und Kundenzufriedenheit signifikant erhöhen.

UC mit CRM und ERP gekoppelt

Das sieht dann zum Beispiel so aus: Das Telefon des Vertriebsmitarbeiters klingelt. Der Suchlauf zur Anruferidentifizierung findet den zugehörigen Kontaktdatensatz im CRM-System und identifiziert den Anrufer. Dem Mitarbeiter werden in seinem UC-Client nicht nur der Name und die Firma des Anrufers angezeigt; er sieht auch die Kundennummer, das Zahlungsziel und die letzten Bestellungen. Bei Bedarf kann er nun direkt aus dem Client eine neue Verkaufschance anlegen, einen Auftrag bearbeiten oder den Datensatz im CRM-System öffnen.

Ruft derselbe Kunde im Service an, werden dem Support stattdessen die Ticket-Historie und die Produktversionen angezeigt, die derzeit beim Kunden im Einsatz sind. Je nach Abteilung erhält so jeder Mitarbeiter genau die Information, die er für seine Aufgabe benötigt. Der Effekt: Die Fachkräfte müssen nicht erst das passende Programm öffnen, sich den Namen des Anrufers buchstabieren lassen und nach dem Kontakt suchen. Auf Kundenanfragen kann das Unternehmen deutlich schneller reagieren – und die Mitarbeiter sparen wertvolle Zeit.

Zentrale Voraussetzung, damit dieses Szenario Wirklichkeit werden kann, ist die Anbindung der Datenbanken, die den entsprechenden Anwendungen zugrunde liegen. Im nächsten Schritt müssen dann alle Daten, die für die Kommunikation relevant sind, indiziert und – z.B. über einen LDAP-Server – möglichst vielen Clients zugänglich gemacht werden.

Schritt 1: Datenbanken anbinden

Am Anfang stehen die Daten bzw. die Frage, in welchen Datenbanken die Informationen und Kontakte hinterlegt sind, die die Mitarbeiter benötigen. Die Anbindung der Datenbanken ermöglicht nicht nur die Anruferidentifizierung, sondern ebenso den zentralen Zugriff auf sämtliche Kontakte direkt über den UC-Client oder auch in Outlook. Je nach Bedarf kann man darüber hinaus alle relevanten Informationen, die in der Datenbank zu einem Kontakt hinterlegt sind, direkt für die Kommunikation verfügbar machen.

Wie aufwändig sich die DB-Anbindung gestaltet, hängt von der Art der Anwendung und der Serverumgebung ab. In einer Windows-Umgebung lassen sich Datenbanken beispielsweise in aller Regel unkompliziert via ODBC integrieren. Ausgereifte UC-Lösungen machen dem Administrator diese Aufgabe besonders leicht: Sie stellen einsatzfertige Interfaces zur Verfügung, über die sie alle benötigten Datenbanken via Drag and Drop anbinden können.

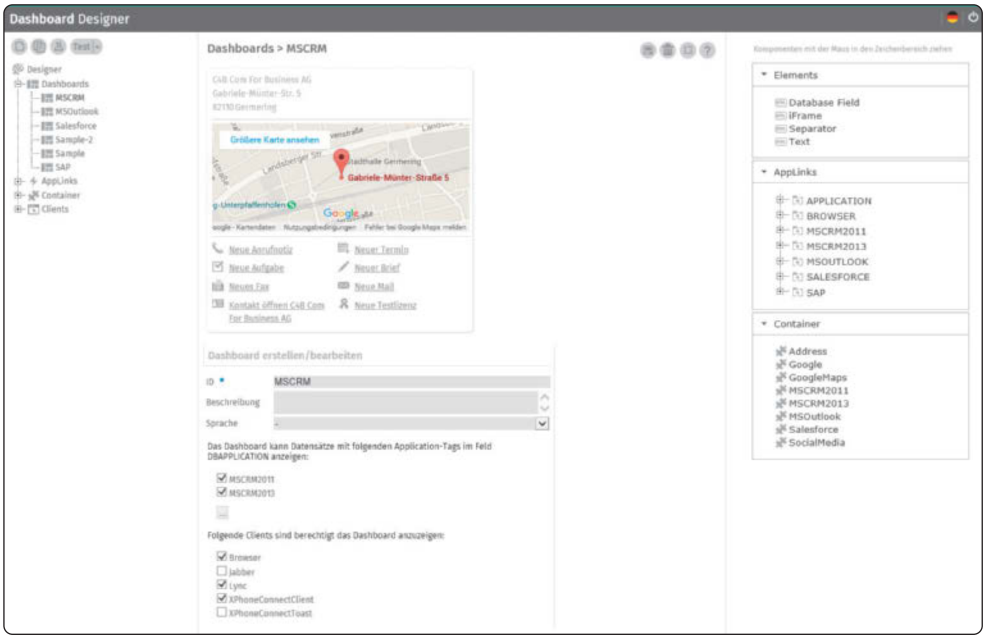
Schritt 2: Datensätze normieren

Jede Datenbank folgt ihrer eigenen Logik. Somit sind auch die Datensätze immer unterschiedlich strukturiert. Um die Daten UC-nutzbar zu machen, muss man sie zuerst normieren. Die einheitliche Darstellung erhöht zum einen den Komfort der Anwender, für die die Daten – unabhängig von der zugrunde liegenden Quelle – immer gleichartig aufbereitet werden. Zum anderen wird die Suche deutlich erleichtert, da die Mitarbeiter dann nur nach einer einzigen Schreibweise suchen müssen, statt diverse Kombinationen durchzuprobieren (z.B. +49 40, +49 (40), 040, (040) etc.).

Schritt 3: Verzeichnisdienst einrichten

Die gebündelten und normierten Daten werden im nächsten Schritt über einen zentralen Verzeichnisdienst zur Verfügung gestellt. Optimal geeignet ist hierfür ein LDAP-Server, vergleichbar dem Active Directory (AD). Da das AD allerdings ausschließlich Mitarbeiterinformationen enthält und keine Daten aus externen Quellen indizieren kann, muss ein zusätzlicher Verzeichnisdienst aufgebaut werden. Zugriffssteuerung und Berechtigungen für diesen zentralen Dienst lassen sich im Weiteren dennoch über das Active Directory steuern.

Der Vorteil von LDAP: Praktisch alle Anwendungen und Clients können auf LDAP zugreifen. Ob mobil mit Smartphone oder Tablet, mit den unterschiedlichsten PC-Clients (Cisco Jabber, Skype for Business, XPhone etc.) oder einem Festnetztelefon: Dank LDAP stehen die gewünschten Daten auch Clients zur Verfügung, die in Anwendungen wie zum Beispiel einem CRM-System keinen Datenabruf durchführen könnten.



Quelle: C4B Com For Business

Im XPhone Connect Dashboard Designer kann der Administrator für jede Anwendung unterschiedliche Dashboards anlegen: Hierzu werden einfach die gewünschten Datenbankfelder und Aktionen im WYSIWYG-Editor via Drag and Drop frei kombiniert.

Durch die zentrale Bereitstellung ist darüber hinaus gewährleistet, dass alle Datenabfragen an einer einzigen Stelle gebündelt werden, was sich wiederum positiv auf die Performance auswirkt. Nicht zuletzt schützt der LDAP-Server die Datenquellen: Der Server übernimmt als zwischengeschaltete Instanz die Funktion eines Gatekeepers und verhindert den direkten Zugriff auf die sensiblen Originaldaten. Darüber hinaus kann man den Zugriff auf die Daten auch benutzerbezogen sowie je nach Applikation oder Standort einschränken.

Schritt 4: Daten indizieren

In einem modernen Verzeichnisdienst ist eine Duplizierung der Datenquellen nicht notwendig: Analog zur Webseitensuche bei Diensten wie Google werden die Datensätze stattdessen indiziert. Die Indizierung erhöht zum einen die Datensicherheit und stellt durch den Zugriff auf die Originalquellen zum anderen sicher, dass stets die aktuellen Kontaktdaten angezeigt werden. Dabei steigt auch die Performance: Nach erfolgreicher Suche werden ausschließlich die Matches aus den angeschlossenen Systemen geholt. Durch diese gezielte Abfrage geraten die Datenbanken nicht unnötig unter Last.

Um die Performance weiter zu optimieren, werden Abfragen darüber hinaus idealerweise in einem Cache gespeichert, sodass eine gleichlautende Suche, die zum Beispiel binnen zehn Minuten gestartet wird, keine neue Abfrage auslöst.

Schritt 5: Daten und Kommunikation verbinden

Sind alle Anwendungen (SAP, Microsoft Dynamics, Salesforce etc.) angebunden und stehen die relevanten Daten gebündelt und normiert zur Verfügung, ist die technische Basis gelegt. Nun beginnt die Kür. Und die liegt in der Analyse der Kommunikationsprozesse der einzelnen Abteilungen und Teams: Welche Anwendung ist jeweils das zentrale Arbeitsmittel? Welche Daten sind die wichtigsten, die zum Beispiel am Telefon benötigt werden? Welche Aktionen sollen als Link bzw. Shortcut zur Verfügung stehen, um die tägliche Arbeit zu erleichtern?

Sind all diese Fragen beantwortet, kann das Unternehmen den Mitarbeitern alle relevanten Informationen zur Verfügung stellen. Je nach UC-Lösung gibt es hierzu unterschiedliche Ansätze und technische Umsetzungen. Eine Möglichkeit ist es, die Daten in Form von Dashboards aufzubereiten, die direkt im UC-Client angezeigt werden. Hierzu wird das Dashboard im ersten Schritt zum Beispiel mit Microsoft Dynamics CRM (oder einer anderen Anwendung) verknüpft. Ruft nun ein Kontakt an, den das CRM identifiziert, wird das entsprechende Dashboard automatisch direkt im Client angezeigt. Jeder Anwendung kann dabei ein eigenes Dashboard zugeordnet werden.

Im Dashboard selbst können sämtliche Datenbankfelder der angebundenen Anwendung eingefügt werden. Ebenso lassen sich Aktionen verknüpfen, die direkt in der angebundenen Anwendung ausgeführt werden („Neuer Termin", „Kontaktdatensatz öffnen" etc.).

Dieser Schritt – die Analyse der Kommunikationsprozesse – birgt naturgemäß einen gewissen Aufwand. Dafür profitieren Unternehmen von schlankeren Prozessen und einer signifikanten Zeiteinsparung.

Unified Customer Experience

Viel zu oft wird das wahre Potenzial von Unified Communications noch verkannt. Wer aber die Technologie richtig einsetzt und entsprechend tief integriert, kann seine Kommunikationsprozesse deutlich verschlanken, wertvolle Arbeitszeit sparen und die Kundenzufriedenheit signifikant steigern. Ausgereifte UC-Anwendungen stellen hierfür praktisch „schlüsselfertige" Lösungen zur Verfügung, bei denen sich die benötigten Datenbanken einfach via Drag and Drop anbinden lassen; sämtliche Daten werden dabei in einem Arbeitsschritt normiert und indiziert.

Und doch liegen die Möglichkeiten integrierter Kommunikation noch viel zu oft brach. Manche Unternehmen scheuen sicher den Aufwand, den eine genaue Analyse der Kommunikationsprozesse mit sich bringt. Vielleicht fehlt ihnen auch der geeignete Partner, der das notwendige fachliche Know-how mitbringt. Nicht zuletzt dürfte aber auch Unwissenheit einer der Hauptgründe für den Verzicht sein: Viele Unternehmen wissen schlicht und ergreifend noch nicht um das Potenzial, das die Integration von Kommunikation und Geschäftsanwendungen für sie bereithält.

David Williams,
Produktmanager,
C4B Com For Business AG

Dinge im Internet sind erst einmal öffentlich

IoT-Datenpunkte für den Mobilfunk müssen sicher und sparsam kommunizieren

Ein Großteil der Dinge im Internet of Things gelangt per Mobilfunk ins Netz. Moderne Machine-to-Machine-Kommunikation muss daher ganz andere Sicherheitsmaßnahmen ergreifen als früher. Neben allfälligen Angriffen auf öffentliche IP-Adressen besteht noch das Kostenrisiko ungewollten Datenverbrauchs.

Vor dem digitalen Zeitalter spielten Sicherheitsmaßnahmen bei M2M-Anwendungen lediglich eine untergeordnete Rolle. Maschinenkommunikation war meist point to point ausgelegt und Hardware-Module in der Maschine sprachen über private Netzwerke mit fest zugeordneter Software. Im Unterschied dazu nutzen IoT-Anwendungen heute in der Regel IP-basierte Mobilfunknetzwerke, um Informationen aus unterschiedlichen Datenquellen direkt an die Cloud oder eine angeschlossene Middleware-Plattform zu übermitteln.

Mobilfunkmodems sind in der Regel so konzipiert, dass sie sich im Netzwerk eines Anbieters anmelden, eine Datenverbindung herstellen und eine öffentliche IP-Adresse anfordern, um auf das Internet zuzugreifen. Über diese öffentlichen Adressen können Mobilgeräte so mit Servern im Netz kommunizieren. Diese Verbindungsart ist allerdings sehr anfällig für Angriffe und kann obendrein zu unbeabsichtigtem Datenverbrauch führen.

Sicherheitsaspekte im M2M-Mobilfunk

Zu den größten Sicherheitsherausforderungen zählen derzeit dynamische, öffentliche IP-Adressen, die Endgeräte selbst und dauerhafte Remote-IP-Verbindungen.

Über dynamische, öffentliche IP-Adressen sind nicht nur Mobilgeräte in der Lage, mit Servern im Netz zu kommunizieren. Gleichzeitig können möglicherweise feindliche Systeme im Internet eine Verbindung zu den Mobilgeräten herstellen. Durch die DNS-Abfrage mithilfe von Mobilfunknummern (DNS Lookup Facilities) haben Angreifer sogar die Möglichkeit, spezifische Geräte über die Telefonnummer zu identifizieren und anzugreifen.

Auf Geräteebene ist zu bedenken, dass vertraute Sicherheitskonzepte wie Firewalls oder Multlfaktorauthentifizierung darauf ausgelegt sind, den Zugang zu IP-Knoten, Systemen oder Geräten zu schützen. Sie verhindern allerdings nicht, dass der damit verbundenen Datenverkehr das Gerät erreicht und dadurch ein höheres Datenvolumen verbraucht. Brute-Force- oder DoS-Attacken (Denial of Service) nutzen diese Lücke, indem sie innerhalb kurzer Zeit zahlreiche Anfragen an das Gerät senden und damit die Verbindungskosten in die Höhe treiben oder eine Überlastung herbeiführen.

Viele M2M- bzw. IoT-Anwendungen brauchen eine IP-Verbindung zu den Geräten im Feld durch den Server. Um dies sicherzustellen, bleiben Mobilgeräte häufig dauerhaft über ihre IP-Adresse mit dem Mobilfunknetz verbunden. Das führt zu verschiedenen Problemen: Zum einen müssen die Geräte, um die Verbindung zum Server aufrechtzuerhalten, regelmäßig Datenverkehr übermitteln, um automatische Verbindungsunterbrechungen zu umgehen. Diese Keepalive-Signale führen zu einem höheren Datenverbrauch und somit zu Mehrkosten. Zum anderen steigt durch die dauerhafte Verbindung des Geräts über dieselbe IP-Adresse die Wahrscheinlichkeit einer Attacke aus dem Internet. Spezielle Scanner durchsuchen das Web nach solchen öffentlichen Adressen und nutzen sie für ihre Angriffe.

Maßnahmen der Risikominimierung

Angesichts dieser Risiken stellt die Zusammenführung älterer, aktueller und künftiger M2M-Produkte sowie -Anwendungen mit modernen Mobilfunktechnologien aus Security-Gesichtspunkten eine ernst zu nehmende Herausforderung dar. Für Organisationen ist dies stets eine Risk-versus-Reward-Entscheidung. Denn auf der einen Seite ermöglichen Mobilfunktechnologien eine schnellere und günstigere Anbindung von entfernten Geräten an das Internet. Auf der anderen Seite setzt man M2M- und IoT-Anwendungen einem höheren Sicherheitsrisiko aus.

Will man diese Risiken umgehen, so ist das häufig mit einem spürbaren zeitlichen und finanziellen Aufwand verbunden. Dennoch sollten Unternehmen bei der Anbindung der Geräte im IoT von Anfang an einige zentrale Sicherheitsaspekte beachten.

So kommunizieren Mobilgeräte in der Regel über öffentliche IP-Adressen. Die B2B-Datenübertragung kann allerdings auch per IP-Protokoll stattfinden, ohne das man das öffentliche Internet nutzen müsste. Private APNs (Access Point Names), die von einem oder mehreren Mobilnetzbetreibern bereitgestellt werden, fungieren als Brücke zwischen dem Mobilfunknetz und dem paketbasierten Datennetz. Die APN-Konfiguration regelt dabei alle Aspekte der Interaktion des Mobilgeräts mit dem Internet. Sie funktioniert in der Praxis ähnlich wie ein VPN, indem sie wie ein virtuelles privates Netzwerk ebenfalls eine sichere Verbindung bereitstellt.

Hostbasierte VPNs und private IP-Adressen

Hostbasierte VPNs verbinden einen oder mehrere Hosts mit einem M2M-/IoT-Lösungsanbieter oder einem Mobilnetzbetreiber. Der Vorteil solcher VPNs liegt darin, dass sie, im Gegensatz zu einem gerätebasierten VPN, üblicherweise den gesamten Datenverkehr von und zu allen über das Mobilnetz verbundenen Geräten eines bestimmten Subnetzes oder Kunden abdecken. Damit können Daten übertragen werden, ohne dass die Geräte direkt aus dem Internet erreichbar sind.

Mobilnetzbetreiber stellen meist nur sehr eingeschränkte VPN-Optionen in Verbindung mit privaten APNs bereit. Größere Flexibilität und mehr Optionen geben M2M-Lösungsanbieter. Auch entfallen hier die Komplexität und die Kosten für das Einrichten eines privaten APN.

Private IP-Adressen sind nicht im Internet zugelassen. Damit ein Netzknoten mit privater Adresse das Internet erreichen kann, muss seine Quelladresse aktiv in eine öffentliche Adresse übersetzt werden. Private Adressen tragen insofern zur Sicherheit bei, als eine dritte Komponente speziell konfiguriert werden muss, damit ein Knoten mit privater Adresse mit einem Rechner im Internet kommunizieren kann. Erst dann sind auch Angriffe von dort möglich.

Quelle: Telit Communication PLC

Lösungen wie das Telit-IoT-Portal ermöglichen die durchgängige Bereitstellung, Konfiguration und Verwaltung von IoT-Anwendungen in der Cloud.

Device-to-Device-Kommunikation

Üblicherweise kommunizieren alle Geräte innerhalb einer APN-Konfiguration über IP-Adressen, ohne das Mobilfunknetzwerk zu verlassen und ohne irgendeine Art von Firewall oder Zugangskontrollsystem zu passieren. Bei privaten APNs ist das nicht problematisch; dagegen kann es bei öffentlichen oder geteilten APNs zu gravierenden Sicherheitsrisiken führen. Die meisten Mobilnetzbetreiber sind zwar in der Lage, diese Kommunikation zwischen den Geräten auf APN-Level sowohl in privaten als auch in geteilten APNs zu blockieren.

Allerdings erfordern bestimmte Applikationen die Kommunikation zwischen definierten Geräten innerhalb des Netzwerks. Anwender sollten daher darauf achten, dass M2M-Lösungsanbieter, die eine solche Device-to-Device-Kommunikation unterbinden, Ausnahmen für speziell definierte Geräte zulassen.

Mit zunehmender Zahl der M2M- und IoT-Geräte wird es außerdem immer wahrscheinlicher, dass Netzanbieter Richtlinien gegen den Netzwerkmissbrauch durchsetzen. Dies betrifft insbesondere den Fall, dass Geräte dauerhaft mit dem Netz verbunden sind und über lange Zeiträume sehr wenige oder gar keine Daten übertragen. Mit großer Wahrscheinlichkeit wird dies unter anderem zu einer Verkürzung der zulässigen Inaktivitätsintervalle sowie zu einer veränderten, weniger günstigen Relation im Hinblick auf den Datenverkehr im Zeitverlauf führen. Damit sind wirtschaftliche Auswirkungen in Form vermehrter Nutzung und Probleme bei der Gerätekonnektivität unvermeidbar, unabhängig vom tatsächlichen Maßnahmenpaket. Geräte, die sich über lange Zeiträume (Stunden, Tage, Wochen) mit dem Netz eines Anbieters verbinden – nur für den Fall, dass ein Server eine Verbindung aufbauen könnte – bilden langfristig kein tragfähiges Konzept.

Vernetzte Steuerung

Die Antwort darauf sind Methoden der Verbindungsaktivierung, die Geräte nur dann mit dem Netz des Betreibers verbinden, wenn es erforderlich ist – und die Verbindung wieder trennen, sobald sie nicht mehr benötigt wird. Wichtig ist dabei, dass die Verbindung lediglich den Kontakt zwischen Gerät und Server ermöglicht. Sie bezieht sich nicht auf die eigentliche Kommunikation. Diese wird von der Anwendung gesteuert und kann von jeder Seite initiiert werden.

Häufig genutzte Aktivierungsarten sind ereignis- und zeitgesteuerte sowie SMS-basierte Aktivierungen: Die ereignisgesteuerte Aktivierung stellt eine Verbindung her, wenn ein oder mehrere vorkonfigurierte Ereignisse lokal auf dem über das Mobilnetz angebundenen Gerät eintreten. Die zeitgesteuerte Aktivierung baut zu vorab festgelegten Zeitpunkten am angebundenen Gerät eine Verbindung auf; die Zeitangabe kann relativ, über einen einfachen Timer, oder absolut, durch Festlegung eines bestimmten Datums und der Uhrzeit, erfolgen. Die SMS-basierte Aktivierung wiederum baut die Verbindung dann auf, wenn das Gerät eine SMS von einem externen Absender erhält. SMS-Mitteilungen nutzen ein Nachrichtenprotokoll und können zur Signalisierung unterschiedlicher Aktionsarten von vielen verschiedenen Absendern genutzt werden.

Bei allen Aktivierungsarten ist es wichtig, ein Abschaltverfahren vorzusehen, um eine ordnungsgemäße Trennung vom Netz sicherzustellen. Die Trennung erfolgt dabei entweder nach einer bestimmten Zeit, bei Inaktivität oder wenn der Kommunikationsvorgang seitens der Anwendung abgeschlossen ist.

Intelligentere Netznutzung im IoT

Die Rahmenbedingungen für die Kommunikation im M2M- und IoT-Bereich werden sich in den kommenden Jahren dynamisch verändern. Aktuelle Anwendungen sind in der Regel darauf ausgelegt, dass die Datennutzung im Mobilfunk künftig noch günstiger sein wird. Vor diesem Hintergrund und angesichts der zunehmenden Zahl von vernetzten Mobilfunkgeräten im Internet der Dinge müssen wir Wege finden, die Mobilfunknetzwerke effizienter zu nutzen, um dem zukünftigen Bedarf mit den verfügbaren Bandbreiten und Netzwerkressourcen beizukommen.

Sicherheit und Datenschutz sind in diesem Zusammenhang jedoch unabdingbar. Kritische Sicherheitsmerkmale unterschiedlichster Technologien und Anwendungsbereiche sind dabei unter anderem die Vertraulichkeit der Daten und die Authentifizierung, die Zugriffskontrolle innerhalb des IoT-Netzwerks, der Datenschutz und das Vertrauen zwischen Benutzern und unter den im IoT vernetzten Gegenständen sowie die Durchsetzung von einheitlichen Sicherheits- und Datenschutzrichtlinien.

Lawrence Miller,
Principal Network Architect, Telit IoT Connectivity

WiFi-Hotspot unterm Mobilfunkmast

Im Test spannt die AVM Fritz!Box 6820 LTE rasch ein tadelloses Netz auf

Vom rechtlichen Risiko einmal abgesehen – rein technisch kann man einen offenen WLAN-Hotspot auch ohne große IT-Kenntnisse in 10 bis 20 Minuten einrichten. Das wollen wir am Beispiel des kleinen LTE-zu-WLAN-Routers AVM Fritz!Box 6820 LTE stellvertretend für die ganze Gattung zeigen.

Der folgende Bericht fasst stark verkürzt die Praxiserfahrungen zusammen, die sich über mehrere Monate hinweg aus diversen Einsatzszenarien ergeben haben, mit unterschiedlichen SIM-Karten, im Büro und im Freien und mehreren Geräten.

Anbindung per LTE, UMTS, LAN, WLAN

Die Fritz!Box 6820 LTE holt sich das Internet per LTE bis 150 MBit/s oder per UMTS bis 42 MBit/s aus der Mobilfunkluft. Vor Ort gibt sie das Internet entweder drahtgebunden per LAN-Kabel mit bis zu 1 Gbit/s und/oder drahtlos per WLAN bis 450 MBit/s an die lokalen Endgeräte weiter. Das können Laptops, Tablets, Smartphones, Internet-Fernseher, IP-Telefone, IPTV-Boxen, IPTV-WLAN-Sticks, Gaming-Konsolen und vieles mehr sein. Die Endgeräte müssen entweder LAN oder WLAN verstehen, um die Fritz!Box als Internetzugang zu nutzen. Der kleine LTE-WLAN-Router überzeugt nicht zuletzt mit der weithin beliebten und leicht verständlichen Betriebssystemsoftware Fritz!OS. Seit Ende 2015 ist er lieferbar. Der Straßenpreis lag im Mai 2016 bei 199 Euro.

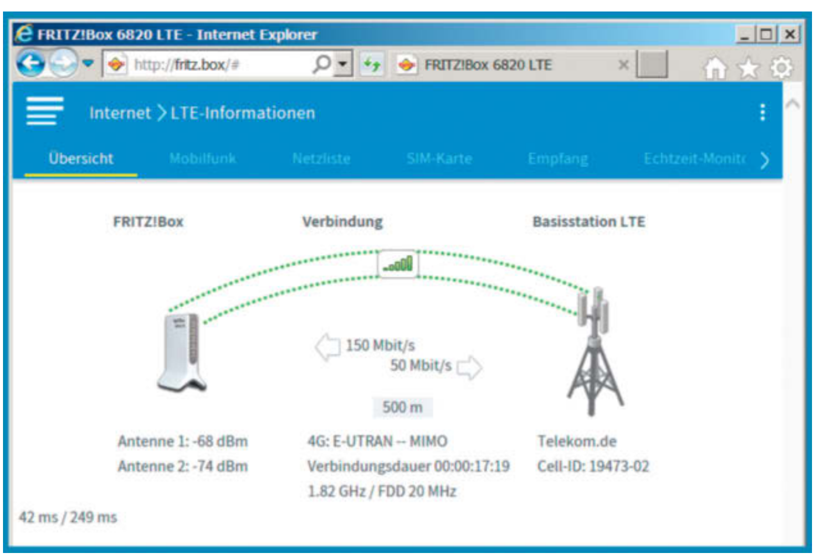
Die Fritz!Box 6820 LTE kann also einen DSL-Anschluss ersetzen – oder ihn zumindest im Sinne einer Ausfallreserve ergänzen, sofern am Einsatzort erstens eine hinreichend gute UMTS-/LTE-Versorgung besteht und zweitens auch die Kosten der UMTS-/LTE-Nutzung in einem angemessenen Verhältnis zum Nutzen stehen. Dafür ist die Fritz!Box 6820 LTE viel mobiler als ein DSL-Anschluss. Man kann sie überall betreiben, wo eine 230-V-Steckdose und 2G-3G-4G-Versorgung zur Verfügung stehen.

LTE-Cat4-Frequenzen (4G) versteht der kleine Router auf Band 1 bei 2,1 GHz, auf Band 3 bei 1800 MHz, auf Band 5 bei 850 MHz, auf Band 7 bei 2600 MHz, auf Band 8 bei 900 MHz und auf Band 20 bei 800 MHz. Das heißt, dass auch alle derzeit wichtigen deutschen LTE-Frequenzen dabei sind, nämlich: 800 MHz für die Versorgung großer Flächen, etwa auf dem Lande, 1800 MHz für die Versorgung von dichter bebauten Gebieten, etwa von größeren Städten, sowie 2600 MHz für die Versorgung von sehr dicht bevölkerten Gebieten und Gebäuden, etwa von Bahnhöfen, Flughäfen und Messegeländen.

Funknetzwahl und Anschlüsse

UMTS- und GSM-Frequenzen (3G und 2G) versteht die kleine LTE-zu-WLAN-Box bei 850 MHz, 900 MHz sowie bei 2100 MHz. Damit holt sie laut AVM maximal 42 MBit/s im Downstream aus dem Internet. Die Fritz!Box 6820 LTE schaltet selbstständig in das am jeweiligen Standort verfügbare Mobilfunknetzwerk 4G, 3G oder 2G um. Man ist also nicht nonstop auf eine LTE-Versorgung angewiesen. Die Automatik kann der User aber auch durch eine manuelle Funknetzwahl ersetzen.

Die AVM Fritz!Box 6820 LTE funkt das Internet über 11n-WLAN-3×3-MIMO mit bis zu 450 MBit/s brutto an die lokalen Endgeräte weiter. Zusätzlich hat sie an der Rückseite eine LAN-Buchse. Damit können Desktop- oder Tower-PCs per Kabel mit bis zu 1 GBit/s brutto verbunden werden. Da jedoch das Internet per LTE „nur“ mit maximal 150 MBit/s hereinkommt, dürften sich weder das 11n-WLAN und schon gar nicht das Gigabit-LAN als Engpass bei der Weiterverteilung an die Endgeräte bremsend auswirken. Falls allerdings das 11n-WLAN vor Ort unter starken Störungen leidet, so bringt ein Anschluss über das Ethernet-LAN-Kabel oft eben doch die besseren und stabileren Durchsatzmesswerte.



Quelle: Harald Karcher

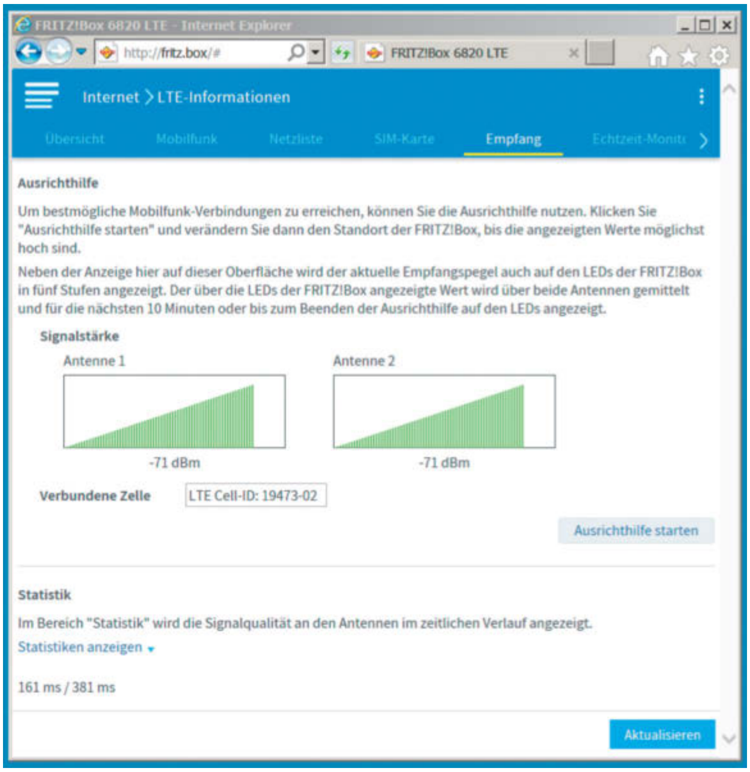
Hier hat die Fritz!Box 6820 LTE unweit der Messe München ein bis zu 150 MBit/s schnelles 4G-LTE-Netz der Deutschen Telekom im 1,8-GHz-Band gefunden.

SIM einsetzen, Provider-Profil wählen

Zurzeit gibt es auf dem Markt vier SIM-Kartengrößen: Nano-SIM, Micro-SIM, Mini-SIM sowie Full-Size-SIM im Scheckkartenformat. Die Fritz!Box 6820 LTE benötigt eine (relativ große) Mini-SIM-Karte. Beim ersten Test hatten wir gerade nur eine (relativ winzige) Nano-SIM von Vodafone zur Hand. Diese steckten wir in den von Vodafone mitgelieferten Plastikadapter und drückten sie danach bis zum Einrasten in den Mini-SIM-Slot an der Unterseite der Fritz!Box. Danach schlossen wir den Router über das mitgelieferte Netzteil an den 230-V-Strom an: Voilà! Der neue LTE-zu-WLAN-Router fuhr hoch, und im WLAN-Programm des Laptops erschien ein neues WLAN-Netzwerk mit dem SSID-Namen „Fritz!Box 6820 LTE“.

Die WLAN-Verbindung zwischen der Fritz!Box und dem Laptop kam ruckzuck und ohne weiteres Zutun zustande, allerdings lieferte die Fritz!Box dem Rechner zu diesem Zeitpunkt noch kein Internet. Das musste erst noch konfiguriert werden. Dazu öffneten wir den Browser und gaben http://fritz.box/ in die Adresszeile ein. Damit wurde die Begrüßungsseite der Fritz!Box 6820 LTE aufgerufen. Als Internetzugang wählten wir das Profil „Vodafone DataGo“ in der Fritz!Box und tippten die vierstellige SIM-PIN ein. Damit landeten wir dann auch umstandslos per Mobilfunk im Internet.

Quelle: Harald Karcher



Dank dieser schönen Ausrichthilfe kann man die Fritz!Box 6820 LTE so lange drehen, bis beide Mobilfunkantennen möglichst hohe Signalstärken melden. Die LTE-Antennen sind von außen unsichtbar in der Fritz!Box verbaut, die WLAN-Antennen ebenso.

Speed-Test: Vodafone und Telekom

Im Indoor-Test, hinter den massiven Wänden im Münchener Büro des Autors, meldete die Fritz!Box 6820 LTE mit eingesteckter Vodafone-SIM-Karte meist nominale Bruttodatenraten von 42,2 MBit/s im Downlink und 5,8 MBit/s im Uplink, also kein LTE. Rein netto kamen damit Downloads von 6 bis 11 MBit/s, Uploads von 2 bis 8 MBit/s sowie recht flotte Pingzeiten von 31 bis 37 ms.

Von Outdoor-Tests erwarten wir uns allerdings höhere Durchsatzwerte. Also maßen wir noch einmal auf einem Parkplatz unweit vom Eingang West an der Messe München. Dabei stand die Fritz!Box auf dem Armaturenbrett des Pkw. Das Netzteil steckten wir in einen 12-auf-230-V-Wandler.

Bei den ersten Outdoor-Messungen mit Vodafone war die Fritz!Box 6820 LTE zunächst noch im 3G-Modus mit HSPA+ und DC-HSDPA unterwegs, und zwar auf der typischen UMTS-Frequenz um die 2100 MHz und in relativ schmalen FDD-Bändern von 5 MHz. Damit kamen nominale Bruttodatenraten von 42,2 MBit/s im Download und 5,6 MBit/s im Upload. Netto kamen damit knapp 8 MBit/s im Download und gut 4 MBit/s im Upload.

Wenig später meldete sich dann auch eine schnelle Vodafone-LTE-Zelle auf 2,63 GHz mit einer üppigen FDD-Bandbreite von 20 MHz aus 300 m Entfernung im Router. Damit konnte die Fritz!Box 6820 LTE endlich auf nominale Datenraten von 150 MBit/s im Download und 50 MBit/s im Upload hochschalten. Und siehe da: Es kam auch gleich ein Nettodurchsatz von gut 94 MBit/s im Download und fast 28 MBit/s im Upload zustande. Das heißt: Die Fritzbox 6820 beherrscht auch 2600-MHz-LTE. Je länger man misst und Messplätze sucht, desto größer wird die Wahrscheinlichkeit, hohe Messwerte zu bekommen. Das wollen wir aber nicht übertreiben, sonst werden die Werte zu praxisfern.

Wir entnahmen danach eine Nano-SIM der Deutschen Telekom aus einem Apple iPhone 6 Plus und steckten sie von unten via SIM-Adapter in die Fritz!Box 6820 LTE. Mit dem von AVM vorkonfigurierten Provider-Profil „Telekom Mobile Data“ klappte der Internetzugriff.

Beim Indoor-Test im Büro kamen damit recht stabile Netto-Downloads mit circa 25 bis 27 MBit/s. Die Uploads lagen zwischen 4 und 5 MBit/s netto. Das alles bei zackigen Pingzeiten von 26 bis 28 ms. Die nominale Bruttodatenrate lag bei den meisten Inhouse-Messungen zwischen der Fritz!Box 6820 LTE und der Telekom-Basisstation bei 150 MBit/s im Download und 50 MBit/s im Upload. Laut LTE-Monitor der AVM-Box war die Basisstation nur 1 km vom Büro entfernt.

LTE-tauglich bis 1800 MHz

Die ausgesprochen schöne LTE-Übersichtsgrafik der Fritz!Box 6820 LTE attestierte Frequenzen im Bereich um circa 1800 MHz mit einer FDD-Bandbreite von 20 MHz. Das ist die typische LTE-Versorgungsvariante der Telekom in allen größeren Städten Deutschlands. Das heißt: Die Fritz!Box 6820 beherrscht auch 1800-MHz-LTE. Das ist erwähnenswert, weil das nicht immer alle LTE-Router in unseren Tests konnten, auch nicht die frühen Modelle von AVM.

Im Outdoor-Test im Kfz unweit der Messe München fand die Fritz!Box 6820 LTE mit eingesteckter Telekom-SIM recht gute LTE-Verbindungen mit 20 MHz breiten FDD-Kanälen im 1800-MHz-Band. Laut Fritz!Box-Monitor war die LTE-Basisstation der Telekom nur 400 m vom Armaturenbrett entfernt.

Die Fritz!Box meldete bei den Telekom-Messungen nonstop nominale Datenraten von 150 bis 50 MBit/s. Speedtest.net gab dazu Pingzeiten um die 25 ms aus, was stimmen dürfte, weil sich das Surfen unter den Fingern auch wirklich zackig anfühlte. Der beste Netto-

Download lag bei knapp über 85 MBit/s. Der beste Netto-Upload bei knapp 40 MBit/s.

Speed-Tests mit E-Plus und O_2

Auch weitere Tests mit SIM-Karten von E-Plus und O_2 klappten mit den von AVM vorkonfigurierten Internet-Zugangsprofilen an der Fritz!Box 6820 LTE ruckzuck. Das heißt: Der User muss bei Inbetriebnahme des LTE-zu-WLAN-Routers nur noch Pulldown-Menüs und Auswahlfelder richtig anklicken. So kann der Hotspot schon wenige Minuten nach dem Auspacken mehrere User per LTE-und WLAN-Funk mit mobilem Internet versorgen.

Zum Vergleich: Bei manch anderen (teuren) LTE-Routern aus dem Profilager mussten wir die Netzwerkprofile selber konfigurieren und detaillierte Zugangsparameter eintragen – oder fehlerhaft ausgefüllte Provider-Profile nachkorrigieren. Bei modernen Smartphones geht aber alles noch viel einfacher: Die erkennen selber, welche SIM-Karte welches Netzbetreibers gerade im Handy steckt, und laden das passende Provider-Profil auch für den Datenverkehr vollautomatisch. Smartphones müssen bei den deutschen Netzbetreibern scharfe Tests durchlaufen, bevor sie in den Vertrieb gehen. Bei den professionellen LTE-Routern darf sich dagegen oft der Systemintegrator um die Profile kümmern. Da gibt es keine Endkunden, die einen Router mit fehlerhaften oder fehlenden Profilen postwendend zurücksenden würden.

LTE-to-WLAN-Test mit elf WiFi-Geräten

In einem Haushalt, Büro oder öffentlichen WLAN-Hotspot will man ja mehrere Geräte gleichzeitig mit Internet versorgen. Also wollten wir prüfen, wie viele Rechner oder Smartphones gleichzeitig über WLAN einen Internetzugang von der Fritz!Box 6820 LTE bekommen. Für diesen Test suchte der Autor alle verfügbaren WLAN-Devices zusammen und verband insgesamt elf WLAN-Geräte mit der Fritz!Box 6820 LTE drahtlos. Das packte die Fritz!Box 6820 offenbar mit links. Für einen kleinen WLAN-Hotspot reicht es auf alle Fälle.

Mehr Hotspots in Eigenregie

Wenn ab Herbst 2016 die WLAN-Störerhaftung in Deutschland wirklich wegfällt, dann ist man auch in Deutschland, zumindest bei kleineren WLAN-Hotspots, nicht mehr so arg wie bisher auf die Hilfe von professionellen WLAN-Providern angewiesen. Die großen Hotspots wird man aber sicher auch in Zukunft von Spezialfirmen bauen lassen.

Wenn man aber sieht, wie problemlos die Fritz!Box 6820 LTE in unseren Tests funktioniert hat, dann wundert es schon, warum die Profi-Hotspots doch öfter Probleme machen. Mit dem Public WLAN auf dem Starnberger See etwa (dort testeten wir auch die Fritz!Box 6820 LTE zum Vergleich – siehe Seite 11) hat der Autor dieser Story seit Sommer 2015 wiederholt Verbindungsprobleme, Konfigurationsschwächen und die Abschaltung des @BayernWLAN nicht nur auf der großen MS Seeshaupt, sondern auch auf der großen MS Starnberg (Katamaran) und auf dem kleineren 300-Leute-Schiff MS Bernried erlebt.

Die Kapitäne und die Mannschaft auf den Schiffen können nichts für die gelegentlichen Probleme mit dem @BayernWLAN. Das Personal auf den staatlichen Schiffen ist extrem freundlich und immer hilfsbereit. Die Durchsagen zu den Sehenswürdigkeiten sind wirklich interessant, und manch ein Ansager hat einen grandiosen bayerischen Humor, der bei vielen Schiffsgästen sehr gut ankommt. So reagierte einer der Kapitäne nach einem erfolglosen Neustart seines @BayernWLAN auf seinem Schiff mit feinem Humor: „Schaun S' her. Ich bin im Internet.“ Dazu der Autor: „Wie haben Sie denn das geschafft?“ Der Kapitän: „Ich hab halt LTE auf meinem Handy, ich brauch kein WLAN.“

Dr. Harald Karcher,
freier Mobile-Communications-Tester

Impressum
Themenbeilage Kommunikation und Netze

Redaktion just 4 business GmbH
Telefon: 08061 34811100, Fax: 08061 34811109,
E-Mail: tj@just4business.de

Verantwortliche Redakteure:
Thomas Jannot (v.i.S.d.P.), Ralph Novak; Florian Eichberger (Lektorat)

Autoren dieser Ausgabe:
Dr. Harald Karcher, Lawrence Miller, Thomas Molkenbur, Klaus Müller, Doris Piepenbrink, David Williams

DTP-Produktion:
Enrico Eisert, Matthias Timm, Hinstorff Verlag, Rostock

Korrektorat:
Kathleen Tiede, Hinstorff Verlag, Rostock

Titelbild:
hunthomas, Shutterstock, Inc.

Verlag
Heise Medien GmbH & Co. KG,
Postfach 61 04 07, 30604 Hannover; Karl-Wiechert-Allee 10, 30625 Hannover;
Telefon: 0511 5352-0, Telefax: 0511 5352-129

Geschäftsführer:
Ansgar Heise, Dr. Alfons Schräder

Mitglieder der Geschäftsleitung:
Beate Gerold, Jörg Mühle

Verlagsleiter:
Dr. Alfons Schräder

Anzeigenleitung (verantwortlich für den Anzeigenteil):
Michael Hanke (-167), E-Mail: michael.hanke@heise.de, www.heise.de/mediadaten/ix

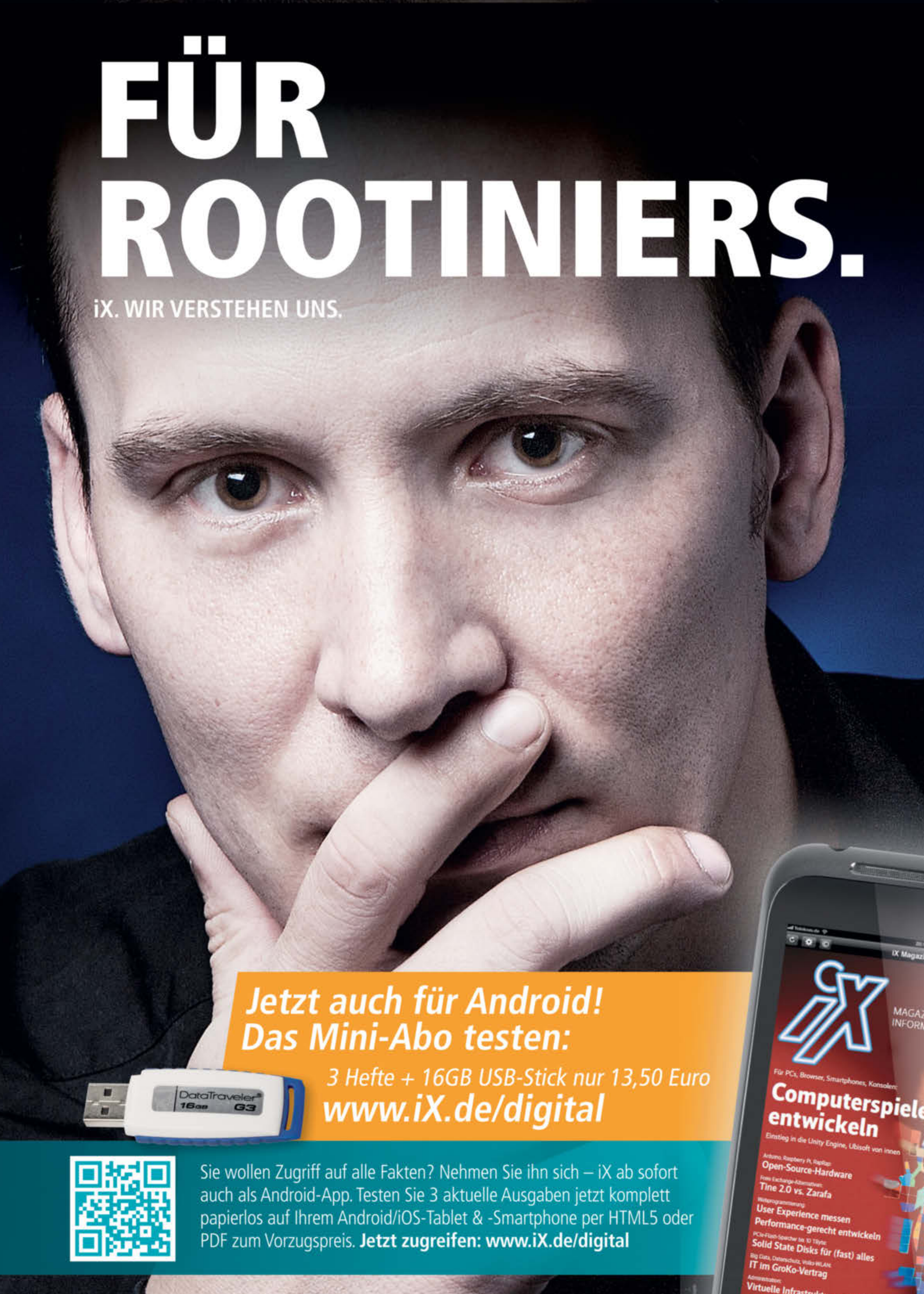
Leiter Vetrieb und Marketing:
André Lux

Druck:
Dierichs Druck + Media GmbH & Co. KG, Frankfurter Straße 168, 34121 Kassel

Die Inserenten

Die hier abgedruckten Seitenzahlen sind nicht verbindlich.
Redaktionelle Gründe können Änderungen erforderlich machen.

Aldi Nord	www.aldi-nord.de	S. 2
Auerswald	www.auerswald.de	S. 7
Bintec elmeg	www.bintec-elmeg.com	S. 5
Easybell	www.easybell.de	S. 9
Intec	www.argus.info	S. 15
Keymile	www.keymile.com	S. 11


FÜR
ROOTINIERS.
iX. WIR VERSTEHEN UNS.
Jetzt auch für Android!
Das Mini-Abo testen:
3 Hefte + 16GB USB-Stick nur 13,50 Euro
www.iX.de/digital
DataTraveler
16GB G3
Sie wollen Zugriff auf alle Fakten? Nehmen Sie ihn sich – iX ab sofort auch als Android-App. Testen Sie 3 aktuelle Ausgaben jetzt komplett papierlos auf Ihrem Android/iOS-Tablet & -Smartphone per HTML5 oder PDF zum Vorzugspreis. **Jetzt zugreifen: www.iX.de/digital**
iX
Für PCs, Browser, Smartphones, Konsolen:
entwickeln
Einstieg in die Unity Engine, Ubisoft von innen
Open-Source-Hardware
Tine 2.0 vs. Zarafa
User Experience messen
Performance-gerecht entwickeln
Solid State Disks für (fast) alles
IT im GroKo-Vertrag