ComConsult Research

Der Netzwerk Insider

Januar 2009

Systematische Weiterbildung für Netzwerk- und IT-Professionals

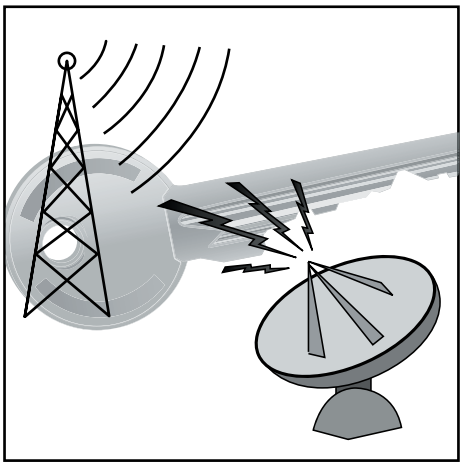
Schwerpunktthema

Sicherheitsaspekte öffentlicher Mobilfunknetze

Teil 2: Maßnahmen zur Sicherung der mobilen Kommunikation

von Dominik Zöller, Dr. Michael Wallbaum, Dr. Frank Imhoff

Wie im ersten Teil dieses Artikels in der Insider-Ausgabe Dezember 2008 beschrieben, lauern bei der Verwendung von öffentlichen Mobilfunknetzen eine Reihe von Gefahren. Daher gilt es zu bedenken, welche konkrete Risiken der Datensicherheit man als Privatperson oder Unternehmen in Kauf zu nehmen bereit ist. Die nicht tolerierbaren Risiken müssen isoliert und durch entsprechende Gegenmaßnahmen ausgeräumt werden.



Freie Netzwahl

Im Falle der zugrundeliegenden Netztechnologie hat das einzelne Unternehmen nur geringe bis keine Einflussmöglichkeiten. Die Absicherung des Netzes gegen Angriffe von außen oder gegen Innentäter liegt ausschließlich in den Händen der Betreiber. Zudem ist - auch bei der Nutzung von Mobiltelefonen mit UMTS oder einer der möglichen Nachfolgetechnologien - nicht sichergestellt, dass die gesamte Infrastruktur diese Technik unterstützt. Die Umrüstung geschieht - den wirtschaftlichen Zwängen geschuldet - schrittweise und immer mit Rücksicht auf Abwärtskompatibilität. Für den Einzelnen ist es im Zweifelsfall nicht erkennbar, ob eine Netzinfrastruktur sicher ist oder nicht.

weiter auf Seite 20

Zweitthema

40 GBASE-T

von Dr. Franz-Joachim Kauffels

Die Erfahrung lehrt, dass eine neue Geschwindigkeitsstufe vom Markt erst dann in breiterem Maße akzeptiert wird, wenn es auch eine Variante für Twisted Pair gibt. Bis vor Kurzem konnte niemand sagen, ob eine 40 Gigabit-Ethernet Variante auch auf Twisted Pair möglich ist. Das hat sich mittlerweile geändert, es wird definitiv 40 GBASE-T geben. Auch wenn ein entsprechender Standard noch ein paar Jahre dauert, können wir heute schon sagen, welche Art der Verkabelung für diesen Zweck mit Sicherheit geeignet ist. Das ist ein sehr wichtiges Ergebnis vor dem Hintergrund der Lebensdauer von Verkabelungssystemen. Natürlich blicken wir in diesem Artikel auch auf die Möglichkeiten für die Transceivertechnik.

Die Standards für 10 GbE über Glasfaser gibt es schon seit 2003. Zunächst haben sich aber nur wenige Anwender dafür interessiert. Das änderte sich erst mit der Verfügbarkeit einer Version über Twisted Pair, eben 10 GBASE-T. Auch wenn viele Betreiber bei der Einführung von 10 GbE schließlich doch zur Faser neigen, scheint alleine die Existenz einer Twisted Pair Version eine erhebliche Beruhigung zu sein.

weiter auf Seite 10

Neuer Kongress

Verkabelungs- und Infrastrukturforum 2009

ab Seite 8

Geleit

Netzwerk-Technologie 2009: wohin geht der Weg?

ab Seite 2

Kongress des Jahres 2009

Netzwerk-Redesign Forum 2009

ab Seite 4

Zum Geleit

Netzwerk-Technologie 2009: wohin geht der Weg?

Die Analyse von ComConsult Research: Netzwerk-Technologie 2009 wird die Basis der Keynote für unser diesjähriges Netzwerk-Redesign Forum im März sein. Wir geben in diesem Geleit Ausschnitte der auf dem Forum anstehenden Diskussion wieder.

Die Verbesserung der Wirtschaftlichkeit und die Erhöhung der Arbeitseffizienz stehen zur Zeit ganz oben auf der Aktionsliste von Unternehmen und Behörden. Die technologischen Ansätze, um dies zu erreichen, sind weitreichend und betreffen ganz unterschiedliche Technologien:

- Neue Formen von Anwendungsarchitekturen basierend auf Webtechnologien (der Browser als moderne Laufzeitumgebung?)
- Umsetzung einer an Geschäftsprozessen orientierten Kommunikation mit Unified Communications und anderen Technologien
- Unterstützung von Team-Prozessen mit Portalen wie Sharepoint oder durch eine Mischung aus Webdesign, Blogs, Wikis und WebDAV
- Redesign von Rechenzentren, weitere Konzentration von Rechenleistung durch neue Formen virtueller Infrastrukturen, durch verbessertes Loadbalancing und Standort-übergreifende Architekturen
- Konsolisierung von Speicher- und Server-Technologie
- gezielte Untestützung mobiler Mitarbeiter durch sichere Bereitstellung von Daten und Applikationen unabhängig vom Ort der Nutzung
- Plattformneutrale und Versions-unabhängige Nutzung kritischer Applikationen durch Applikations- und Desktop-Virtualisierung

Die Liste könnte sicher ohne Probleme weiter verlängert werden. Tatsächlich bieten uns neue Technologien heute weitreichende Möglichkeiten, um effizienter und wirtschaftlicher zu arbeiten.

Dabei haben alle angesprochenen Themen und Projekte etwas gemein:

- sie stellen neue und erweiterte Anforderungen an bestehende Netzwerke
- sie verändern noch einmal unser Verständnis von Verfügbarkeit

Zwei Beispiele sollen das unterstreichen:

- Fast alle neuen Technologien setzen die Verfügbarkeit eines Netzwerk-Zugangs voraus, hier seien insbesondere Web-Applikationen, UC und Server-/Speicher-Konsolidierung in Kombination mit Virtualisierung genannt. Die Zeiten, in denen bei Ausfall eines Netzwerks an einem Fat-Client weiter gearbeitet werden konnte, sind bis auf Basis-Anwendungen deutlich vorbei. Ohne Netzwerk geht nichts mehr und dieser Trend wird sich noch weiter verstärken
- Neue Formen von Kommunikation inklusive der traditionellen Sprach- und Video-Kommunikation stellen immer mehr die Frage, ob es akzeptabel ist, wenn ein Netzwerk-Fehler zum Abbruch einer laufenden Kommunikation führt. Bisher hat man diese Anforderung auf Hochverfügbarkeit auf isolierte Nutzungspunkte wie die High-End-Videokonferenz des Vorstands reduziert. Aber mit einer Ausweitung dieser Art von Kommunikation auf immer mehr Teilnehmer und mit immer mehr wichtigen Kommunikations-Vorgängen stellt sich die Frage, in welchem Umfang ein Netzwerk hochverfügbar sein muss (dabei erfolgt die Definition von Hochverfügbarkeit immer aus der Sicht der Anwendung und dem Ausmaß der Beeinträchtigung für eine einzelne Anwendung)

Betrachtet man die Anforderungen an Netzwerke, dann fallen besonders folgende Bereiche auf:

- Wir laufen in eine neue Layer-2 und Layer-3-Diskussion. Bestehende Layer-2-Bereiche dehnen sich gerade in Rechenzentren und auch in Industrieumgebungen immer weiter aus. Dies wird kombiniert mit dem Wunsch, räumlich verteilte Layer-2-Bereiche zu verbinden
- Die im Layer-2 bestehenden genormten Redundanzverfahren sind auf einfache Formen der Datenübertragung optimiert. Sie haben für Sprach- und Videoübertragung sowie im Umfeld von Rechnenzentren und Produktionsumgebungen klare Nachteile. Für die Konsolidierung von Speichernetzen sind sie gar komplett ungeeignet. Einzelne Hersteller haben geeignete Technologien zur Beseitigung dieses Problems vorgestellt, aber auch diese Technologien sind nicht allgemein nutzbar und sie sind Hersteller-spezifisch
- Seit dem Beginn der Datenkommunikation gibt es den Effekt, dass Teile von Provider-Lösungen in die normalen LAN´s und WAN´s absinken und dort neue und technisch sehr leistungsfähige Lösungen bieten. Nun steht mit Carrier Ethernet eine Technologie vor der Tür, die nur unwesentlich teurer ist als bestehende Backbone-Technologie und die neue Türen für hochverfügbare Netzwerke aufstösst. Doch Carrier Ethernet ist eine Layer-2-Technologie und hat zudem einige Handhabungsnachteile. Wie können wir die ohne Frage bestehenden Potenziale dieser Technologie nutzen?
- Die zunehmende Konzentration im Server-Bereich und die Konsolidierung von Speicher- und Server-Technologien erfordert neue Dimensionen von Bandbreiten. Parallel ist 10 Gigabit-Ethernet in die Normalität eingetreten und wird von einer Reihe von Blade-Herstellern direkt On-Board unterstützt. Mit der Konsolidierung von Speicher-Netzwerken werden diese Bandbreiten in virtualisierten Umgebungen auch genutzt werden. Damit ist zumindest für den Kern unserer Netzwerke der Sprung in die nächste Bandbreiten-Generation gekommen. Die Hersteller haben mit

Das sind Werte, die die von bisher bekannten Kabeln erheblich in den Schatten stellen. Zum Vergleich siehe Abbildung 1.

Der ANEXT-Wert ist sensationell. Eine Schwierigkeit bei 10 GBASE-T war es, das für ein Kabel relativ empfindliche Signal vor den von außen kommenden Störeinflüssen zu retten. In anfänglichen Versionen konnte das Signal auch schon mal völlig untergehen. Erreicht wird diese Qualität durch eine S/FTP-Konstruktion mit vier geschirmten Paaren und einem Gesamtschirm.

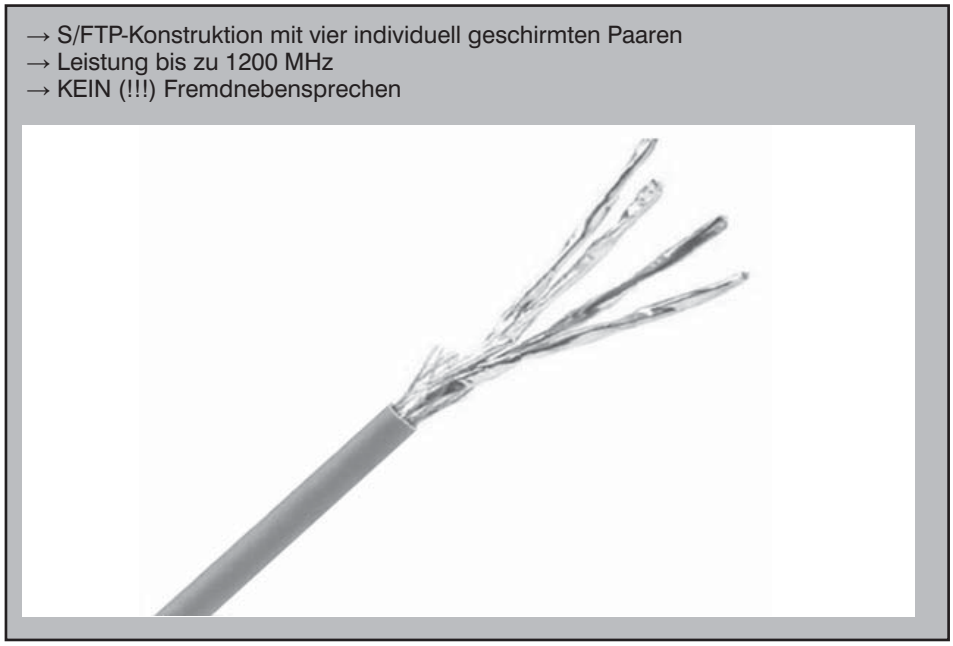


Abbildung 2: Cat. 7A-Kabel

Nun brauchen wir noch den passenden Stecker. Da bietet sich der GG45-Stecker an. Der GG45-Stecker hat 12 Kontakte. Der „2in1“ Connector kombiniert RJ45 und GG 45. Dadurch entstehen zwei Modi:

- RJ45 Modus bis 500 MHz für 1 und 10 GBASE-T
- GG45-Modus bis 1000 MHz für 40 GBASE-T

Der GG45-Stecker passt zu Cat 7A-Kabeln. Er ist bereits jetzt völlig standardisiert ISO/IEC 60603-7-7. Der RJ45-Modus ist zwingend nach ISO 11801 für die Gewährung von Rückwärtskompatibilität. (siehe Abbildung 3)

Ein alternativer Stecker wäre der IEC 61076-3-104-Stecker, der von Siemon entwickelt wurde. Er hat ein neues Steckergesicht und ist deshalb nicht rückwärtskompatibel. Außerdem wurde das eingangs genannte Ergebnis mit einer Kombination des LANmark 7A-Kabels und GG45-Steckern erzielt. Wir beziehen und im Folgenden also ausschließlich darauf.

Anwendungen für 40 GBASE-T

Was sind mögliche Anwendungen für 40 GBASE-T? Zunächst geht es um eine Marktverbreiterung für 40 Gigabit Ethernet schlechthin. Auch bei Gigabit Ethernet und 10 GbE war es ja schließlich so, dass der Markt erst dann richtig zugegriffen hat, als die Kupferversionen verfügbar waren. Komischerweise wurden dann auch massenhaft Glasfaserschnittstellen gekauft. Der Markt ist nicht wirklich logisch, aber hinsichtlich seiner grundsätzlichen Mechanismen ganz gut durchschaubar. Über die Anwendungsmöglichkeiten von 40 Gigabit Ethernet habe ich schon vielfach berichtet, aber natürlich gibt es hier im Standard trotz der vielen PHY-Varianten eine schmerzliche Lücke. Wenn man einmal genau hinsieht, gibt es zwar Schnittstellen für die Überwindung hunderter Kilometer, aber nur vergleichsweise wenig, was man im Datencenter wirklich brauchen kann. Und wenn wir über 40 Gigabit Ethernet sprechen, sprechen wir auch über 40 Gigabit Fiber Channel, weil dieser Standard zwar ein anderes Paketformat benutzt, sich ansonsten heute aber bei den physikalischen Schnittstellen an den 10 GbE-Definitionen orientiert, wenn auch teilweise mit kleinem Formfaktor. Es gibt keinen Grund, warum die FC-Arbeitsgruppen von dieser bislang sehr erfolgreichen Strategie abweichen sollten. Schließlich diskutieren wir ja auch noch über FCoE, dann ist es von der Technik her ohnehin identisch.

Wo ist denn nun im 40/100 Gigabit-Standard die Lösung, mit der man wirklich preiswert unter Nutzung bestehender Verkabelung Server untereinander zusammenschalten kann oder Server mit Speichern verbindet? Die vierkanalige Variante 40 GBASE-LX-4 für die Nutzung von 10 km Singlemodefaser ist für das RZ nicht wirklich befriedigend und die eigentlich immer „vergessene“ vierkanalige Twinaxversion 40 GBASE-CX-4 mit ihren 10 Metern Reichweite erst recht nicht. Die Multimodevariante 40 GBASE-SR hat nach Standard noch keine elektronische Dispersionskompensation. Hersteller wie AMCC können das aber schon heute realisieren. Also wird es früher oder später noch eine Variante 40 GBASE-LRM geben, in Analogie zu 10 GBASE-LRM. Das wäre die einzig geeignete RZ-Variante. Wenn man eine millionenschwere SAN-Investition tätigt, macht die Anschaffung einiger Meter neuer Glasfasern auch schon nichts mehr. Aber was ist mit den vielen anderen Fällen, wo man z. B. einen einzelnen File-Server, der 85 m weg steht, ordentlich einbinden möchte? Wo man SAP-Applikationsserver miteinander verbinden möchte? Wo man eines dieser wunderschönen

Abbildung 3: GG45-Stecker Foto: GG45-Alliance

40 GBASE-T

neuen Tapedecks einbinden möchte? Was passiert, wenn man plötzlich“ merkt, dass die Virtualisierung dazu führt, dass die 10 GbE-Lösung nicht mehr ausreicht? Es ist ja nett von den Komponentenherstellern, schon jetzt preiswerte Transceiver und Serverboards in Aussicht zu stellen, wirklich hilfreich ist es aber nur für den Besitzer einer strukturierten Glasfaserverkabelung mit den „richtigen“ Fasern. Also, Anwendungsbereiche hin und her, ohne sinnfällige Kupfervariante ist der Standard für 40 Gigabit Ethernet ziemlich unvollständig und nützt z. Zt. hauptsächlich Metronetz-Providern. Weil ich ja immer etwas böse bin, möchte ich sogar hinzufügen, dass der Standard in seiner jetzigen Form der Schaffung einer glatten, hochperformanten Netzwerk-Infrastruktur eher schadet als nützt, weil wegen des Fehlens einer brauchbaren Kupferversion (und diese ist auch durch eine Low Cost Fiberversion nicht zu ersetzen) im Markt momentan noch eine Zurückhaltung zu verspüren ist, die in letzter Konsequenz zu recht ungesundem und teuren Fummeln mit anderen Lösungen führt.

Blickt man etwas nach vorne, wird wie bei 10 Gigabit Ethernet auch, die überwiegende Mehrheit der installierten Basis von 40 Gigabit Ethernet in den Datencentern zu finden sein. Hier möchte man die installierte Basis an Rechnern einfach unter Nutzung der installierten Basis an strukturierter Verkabelung besser und performanter unterstützen. Dies umfasst nicht nur die Server-zu-Server oder Server-zu-Speicher-Kopplung, sondern auch den Übergang zu Switches und DWDM-Systemen für die Realisierung von Fernverbindungen. Seit mindestens zwei Jahren sprechen wir vom Wachstum der 10 Gigabit-Schnittstellen für Server. Hier ist es einfach die normative Kraft des Faktischen, die zu einer autosensenden 1000/10000 Chipsatz-Generation führt und alleine aus Erwägungen der Stückzahl werden sich die Chiphersteller darauf kaprizieren, unabhängig davon, ob ein Anwender diese Datenrate wirklich benötigt. Es geht einfach nur um den Preis und die Stückzahl. Angesichts dieser Entwicklung bleibt momentan nur übrig, im Etagen- und Steigbereich mit allerbrutalstem Oversubscribing zu arbeiten. Wie bei Shared Medium System selig hofft man inständig, dass alle Benutzer schlafen mögen und ja nicht auf die Idee kommen, die mögliche Leistung zum Endgerät zu nutzen. Widersinnigerweise verlegt man zwar Kat. 7 Kabel, damit das Gigabit auch ja heil bis zum nächsten Verteiler kommt, verbindet die Etagen untereinander aber auch nur mit einem Gigabit, weil es nichts anderes gibt, was man bezahlen könnte.

Ein weiterer Standard, der allen Unkenrufen zum Trotz dabei ist, sich langsam aber sicher immer weiter zu verbreiten, ist iSCSI, die Abbildung von Speicherblocktransfers auf IP-Päckchen und - Netze. Sieht man sich die Leistungsgrenzen heutiger Geräte an und entwickelt sie, wie das so üblich ist, gemäß Moore´s Law weiter, werden wir binnen 4 - 5 Jahren eine Leistungsverzehnfachung haben. Plötzlich packen wir etwas aufs Netz, was dort vorher nicht war: den Fileserver-zu-Fileserver, Filerserver-zu-Application Server und Fileserver-zu- Backupmedium-Verkehr. Da gehen schon einmal einige Gigabit durch den Schornstein. Dann packen wir noch ein paar Wireless-VLANs drauf, hier darf man pro Zelle, also pro 11n-Access Point, demnächst auch mit 500 Mbit/s. rechnen und bei hochperformanten Zellen dürfen diese nicht zu groß werden, also ergeben sich summa summarum hunderte Zellen mit je ca. 4 - 8 Benutzern, und schon wieder haben wir eine Backboneleistung von 10 Gigabit verwurschtelt. Verzeihen Sie mir die flapsige Ausdrucksweise, aber vom vornehmen Ausdruck wird es auch nicht weniger.

Das sind die Dinge, die Sie kennen. Aber das ist noch nicht alles. Ich rechne in absehbarer Zeit vor allem im Zuge der Virtualisierung noch mit folgenden Tendenzen: Hardware-unterstütztes CPU Load Balancing wird sich nicht mehr auf Prozessoren beschränken, die zufällig in einem Gehäuse wohnen, sondern auch via Highspeednetz zumindest in benachbarte Rechner übergreifen. Hier benötigen wir Reaktionszeiten im Submikrosekundenbereich und jede Menge rohe Performance. Es wird so genannte TCP/IP Offloader geben, die nichts weiter tun, als alle Aufgaben, die im TCP/IP-Umfeld anfallen, zu übernehmen. Da wir alles mit TCP/IP machen, wird das viel Arbeit. Die Netzprozessoren können komplett TCP/IP auf einem Chip abarbeiten und damit ist es nicht mehr hinzunehmen, wenn z. B. ein Server allzulange über TCP/IP-Fragen überlegt. Wir bekommen einen Vorgeschmack darauf bei den iSCSI-Hardwarebeschleunigern. Insgesamt wird sich die Verarbeitungsgeschwindigkeit für Protokolle durch die Hardwareprozessoren und die Offloader dramatisch erhöhen, so dass sich ein Netz nicht mehr darauf verlassen kann, dass die kommunizierenden Recherchen schon so langweilig an den Protokollen herumrechnen, dass sie nur relativ langsam und mit langen Pausen Daten ausspucken können. Schließlich gibt es noch so nette Neuigkeiten wie RDMA, das Remote Direct Memory Access Protokoll, was, wie der Name schon sagt, DMA auf einem fremden Rechner unterstützt.

Ziele für eine Standardisierung von 40 GBASE-T werden sein:

- Überwindung von 100 m Distanz auf Cat 7/7A oder besseren Twisted Pairs
- Bewahrung existierender Investitionen in Verkabelung in Datencentern und strukturierten Verkabelungsbereichen
- Unterstützung von 10 GBASE-T und 40 GBASE-T mit einer einzigen PHY mit

Seminar

Internetworking: optimales Netzwerk-Design mit Switching und Routing
09.02. - 13.02.09 in Aachen

Dieses 5-Tages-Intensiv-Seminar vermittelt Netzwerkbetreibern und Planern Methoden und Technologien zur erfolgreichen Strukturierung von Enterprise Netzwerken. Dabei wird das komplette Spektrum vom L2/L3 Switching über Redundanz/Routing bis hin zu Themen wie VLAN, WLAN-Integration, Multicast-Routing, VPN, MPLS, abgedeckt. Es werden sowohl die theoretischen Hintergrundkenntnisse als auch die Konsequenzen für den praktischen Betrieb von Netzwerken dargestellt.

Referenten: Dipl.-Inform. Petra Borowka, Markus Geller
Preis: € 2.290,- zzgl. MwSt.

Buchen Sie über unsere Web-Seite **www.comconsult-akademie.de**

Schwerpunktthema

Dominik Zöller ist seit 2006 Berater bei der ComConsult Beratung und Planung. Während seines Studiums konzentrierte er sich auf die Themengebiete der Kommunikationsnetze und der Betriebssysteme. Bei ComConsult ist er vorwiegend mit der Evaluierung, Planung und Ausschreibung professioneller Unified Communications, Kollaborations- und Videokonferenz-Systeme befasst.

Dr. Michael Wallbaum ist Senior Consultant der ComConsult Beratung und Planung GmbH. Er blickt auf jahrelange Projekterfahrung in Forschung, Entwicklung und Betrieb im Bereich mobiler Kommunikationssysteme, Voice-over-IP und Groupware zurück. Zu diesen Themenbereichen sind von ihm zahlreiche Veröffentlichungen und Buchbeiträge erschienen.

Dr. Frank Imhoff ist technischer Direktor und Senior Consultant der ComConsult Beratung und Planung GmbH. Er blickt auf jahrelange Erfahrung in Forschung, Entwicklung und Betrieb von lokalen Netzen, Voice-over-IP, Wireless Local Area Networks sowie anderen Mobilfunk- und Telekommunikationssystemen zurück. Zu diesen Themenbereichen sind von ihm bereits zahlreiche Veröffentlichungen erschienen und Seminare betreut worden.

Sicherheitsaspekte öffentlicher Mobilfunknetze Teil 2: Maßnahmen zur Sicherung der mobilen Kommunikation

Fortsetzung von Seite 1

Die einzige Möglichkeit, die sich dem Kunden bietet, ist, bei der Auswahl des Providers nicht alleine nach Kostengesichtspunkten vorzugehen. Der Nachweis sicherer Infrastrukturen kann von den Betreibern durch regelmäßige Sicherheits-Audits und Zertifizierungen durch unabhängige Sachverständige erbracht werden. Doch auch wenn der Kunde sich im Vorfeld informiert und bei dem Betreiber auf solche Nachweise drängt - ein tiefgehender Einblick in die Sicherheitsaspekte des Netzes wird ihm in der Regel verwehrt bleiben. Auch personelle und organisatorische Risikofaktoren im Betreiberunternehmen entziehen sich in der Regel seiner Kenntnis. Als Grundannahme muss also - ähnlich dem Internet - immer die Unsicherheit des verwendeten Mobilfunknetzes unterstellt werden. Die Sicherheitsproblematik der Mobilfunknetze - von unzuverlässigen Verschlüsselungsverfahren bis zur Ortung von Endgeräten durch Unbefugte - macht deutlich, dass Unternehmen, deren Mitarbeiter auf die Nutzung mobiler Endgeräte angewiesen sind, ihrerseits Schutzmaßnahmen ergreifen müssen.

Dienstabstinenz

Trotz geringer Einflussmöglichkeiten auf die Sicherheit des Netzes selbst, lassen sich einige Vorsichtsmaßnahmen treffen. Diese betreffen in erster Linie Komfortmerkmale der Endgeräte sowie vom Netz erbrachte Dienste. Ein Beispiel wäre die Ortung von Endgeräten durch externe Dienstleister. Innerhalb des Netzes ist immer eine Zuordnung von Benutzer (IMSI) und Endgerät (IMEI) zu einem Aufenthaltsort (LAI) möglich. Die im Netz verfügbaren Informationen können bei Bedarf, die Zustimmung des Teilnehmers vorausgesetzt, von externen Dienstanbietern für die Lokalisierung von Endgeräten genutzt werden. Hierfür gibt es viele sinnvolle Anwendungsgebiete, wie etwa die Ortung medizinischer Notfälle oder das Auffinden von mit GSM-Geräten ausgestatteten Fahrzeugen im Falle eines Diebstahls.

Das Endgerät muss für die Nutzung solcher Dienste registriert werden. Die Freischaltung geschieht durch zwei SMS, eine an eine Servicerufnummer des Providers und eine an die des Dienstanbieters. Danach kann das Handy, z.B. per Webinterface, geortet werden. Befindet sich ein Angreifer kurzzeitig im Besitz des Endgerätes, so kann es für die Ortung frei geschaltet und die verräterischen Bestätigungs-SMS gelöscht werden. Nicht jeder Dienstanbieter informiert den Endgerätebesitzer per SMS über einen Ortungsvorgang. So ist eine Ortung ohne Zustimmung oder Kenntnis des Besitzers möglich. Das Deaktivieren eines Ortungsdienstes geschieht, wie auch die Frei-

Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 2

schaltung, per SMS. Jedoch gibt es für den Anwender keine automatisierte Möglichkeit, sich über den aktuellen Status solcher Freischaltungen zu informieren. Eine Nachfrage beim Mobilfunkanbieter kann hierüber im Zweifel Aufschluss geben. Eine generelle Deaktivierung solcher Funktionen ist nicht vorgesehen und muss - wenn überhaupt möglich - separat mit dem Netzbetreiber vereinbart werden. Falls das nicht möglich ist, können im konkreten Verdachtsfall an bekannte Servicenummern des Netzbetreibers SMS zur Deaktivierung geschickt werden. Hierdurch wird eine erneute Aktivierung aber nicht verhindert. (siehe Abbildung 1)

Abbildung 1: Nach Freischaltung per SMS ist eine (grobe) Ortung per Webinterface möglich

Den besten Schutz vor Ortung bietet die Anonymisierung. Zum Beispiel existieren Tauschbörsen für Endgeräte und Prepaid-Verträge, wodurch die eindeutige Zuordnung von Orts- und Personeninformationen erschwert wird. Den mit solchen Tauschverfahren verbundenen Aufwand halten in der Regel jedoch nur Drogendealer und Mafiosi für gerechtfertigt - für Unternehmen und Organisationen ist dieser Ansatz unpraktikabel.

An diesem Beispiel sieht man, dass durch eine Vielzahl von Diensten – so nützlich sie auch in ihrer ursprünglichen Intention sein mögen - Gefährdungen für den Schutz von Daten und Privatsphäre entstehen können. Es ist daher für Unternehmen und Behörden sinnvoll, sich im Vorfeld beim jeweiligen Mobilfunkbetreiber über Dienste und Leistungsmerkmale zu informieren. Die Angaben der Betreiber, ob Dienste generell deaktiviert werden können, weichen voneinander ab. Falls die Möglichkeit besteht, sollten in jeden Fall alle nicht benötigten Dienste abgeschaltet werden. Dazu zählen Ortungsdienste gleichermaßen wie Push-To-Talk (PTT) oder ähnliche Leistungsmerkmale.

Ein weiterer wichtiger Aspekt bei der Planung einer sicheren Kommunikationsumgebung, neben Wahl und Konfiguration des Netzes, ist die Endgerätesicherheit. Wie in Unternehmensnetzen die Clients besonderer Aufmerksamkeit bedürfen, so trifft dies im selben Maße auch auf mobile Endgeräte zu. Was nutzen sichere Netze, wenn ihre Endpunkte Angriffen schutzlos ausgeliefert sind? Sie dienen als Ein- und Ausgabegerät, zur Datenverarbeitung ebenso wie zur Kommunikation. Es werden Daten und persönliche Informationen auf ihnen gespeichert und die Kontrolle über ein Endgerät zu erlangen kommt in mancher Hinsicht der Übername der Identität des Besitzers gleich. Und eines unterscheidet sie vom herkömmlichen Arbeitsplatzrechner: sie sind klein, leicht und transportabel. So ist die Gefahr besonders groß, dass sie unbemerkt verloren oder entwendet werden. Es ist also insbesondere wichtig, mobile Endgeräte vor unbefugtem Zugriff, Datendiebstahl und Manipulation zu schützen.

Vorspiegelung falscher Tatsachen

Das Endgerät wird durch die Personal Identification Number (PIN) vor Zugriff geschützt. Das jedenfalls ist der Eindruck, der sich dem Benutzer eines Mobiltelefons aufdrängt. In Wahrheit wird nicht das Endgerät vor Zugriff geschützt, sondern die PIN dient lediglich zur Authentisierung des Benutzers am Subscriber Authentication Module (SIM). Das SIM ist ein funktionaler Bestandteil der SIM-Karte und enthält die zur Authentisierung des Benutzers notwendigen Informationen, also International Mobile Subscriber Identity (IMSI) sowie das Shared Secret, welches, wie im ersten Teil dieses Artikels beschrieben, als Schlüssel für die Authentisierung dient. Die neuere Variante Universal Subscriber Identification Module (USIM), die im Zuge von UMTS eingeführt wurde, bietet ein sichereres Design der implementierten Authentisierungsmethoden. Es nimmt aber dieselbe Rolle in der Authentisierung ein wie die SIM, weshalb hier nicht weiter zwischen beiden Modulen unterschieden wird. Per PIN authentisiert sich also der Benutzer gegenüber seiner (U)SIM und kann daraufhin auf Grundlage der darin implementierten Funktionen die Authentisierung gegenüber dem Mobilfunknetz vornehmen. Das geschieht standardmäßig beim Einschalten des Mobiltelefons,

Kongress

Netzwerk-Redesign Forum 2009
09. - 12.03.09 in Königswinter

Netzwerke sind der Lebensnerv unserer Unternehmen. Sie unterliegen einer permanenten Weiterentwicklung und Veränderung. Aus einem Mix aus Bedarf und technischen Möglichkeiten muss das individuelle Optimum für ein Unternehmen gefunden werden. Dieses Optimum muss zugleich an der Zukunft orientiert sein, da Netzwerk-Komponenten über einen langen Zeitraum stabil und ohne permanente Änderungen betrieben werden müssen.

Hier setzt das ComConsult Netzwerk-Redesign Forum 2009 an. Es analysiert die wichtigsten Bedarfsentwicklungen, stellt diesen die neuesten Netzwerk-Technologien gegenüber und erarbeitet Empfehlungen für ein erfolgreiches Netzwerk-Design, eine zukunftsorientierte Auslegung und einen stabilen und zuverlässigen Betrieb.

Moderation: Dr. Franz-Joachim Kauffels, Dr. Jürgen Suppan
Preis: € 2.290,- zzgl. MwSt. bzw. € 1.890,- zzgl. MwSt

Bestellen Sie über unsere Web-Seite **www.comconsult-research.de**