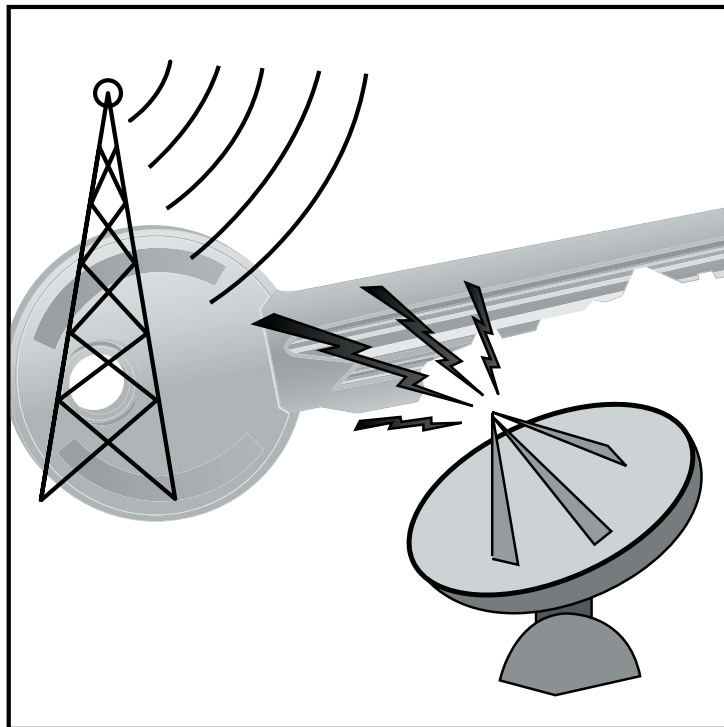


# Sicherheitsaspekte öffentlicher Mobilfunknetze

## 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.

## Schwerpunktthema



Dominik Zöllner 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 Video-Konferenz-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

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 Dienstleistern 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 Servicenummer 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 jedem 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 Übernahme 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, weshalb der

**Jetzt Leser werden**

**Der Netzwerk Insider**

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.



Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:

<http://www.comconsult-akademie.de/de/Registrierung.php>

Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 2

Eindruck entsteht, der Anwender authentisiere sich für den Zugriff auf das Endgerät. Die Inhalte und Funktionen des Endgeräts werden hierdurch aber in keiner Weise geschützt.

**Identität im Netz**

Da die SIM ab dem Zeitpunkt der Anmeldung im Netz die „digitale Identität“ des Teilnehmers gegenüber dem Netz darstellt, ist ein umsichtiges Management der SIM-Karten in Unternehmen und Behörden erforderlich. Insbesondere müssen abhanden gekommene SIM-Karten umgehend beim Provider gesperrt werden, da ansonsten ein Missbrauch der SIM zur Vortäuschung einer falschen Identität nicht auszuschließen ist. Besonders dringend ist aber ein vorsichtiger Umgang mit der PIN geboten, da sie die SIM vor Missbrauch schützt. Gleiches gilt für den Personal Unblocking Key (PUK), der dem Nutzer das Zurücksetzen der PIN erlaubt. Dem Anwender werde sowohl PIN als auch PUK von seinem Mobilfunkbetreiber zugewiesen, weshalb dieser zunächst keinen Einfluss auf deren Beschaffenheit haben. Allerdings sollten beim Zurücksetzen der PIN darauf geachtet werden, dass die PIN nicht leicht zu erraten ist. Da eine PIN immer eine vierstellige Zahl ist, können zwar nicht dieselben Maßstäbe an die Komplexität gestellt werden, um ein alphanumerische Passwörter (siehe z.B. „Regelungen des Passwortgebrauchs“, IT-Grundschutzkatalog des BSI <http://www.bsi.de/gshb/deutsch/m/m02011.htm>). Grundregeln, wie die Verwendung von Zufallszahlen und die sichere Aufbewahrung der PIN gelten aber universell. Beispielsweise sind Unterlagen, die PIN oder PUK enthalten, gesichert aufzubewahren oder - falls möglich - umgehend zu vernichten. Unternehmen müssen, falls PIN und PUK der Firmenhandys zentral verwaltet werden, die betroffenen Unterlagen als schutzbedürftig einstufen und den Zugriff auf einen autorisierten Personenkreis beschränken. Einige Endgeräte bieten das Abspeichern der PIN aus Komfortgründen um zum Beispiel den Wechsel der SIM-Karte im laufenden Betrieb komfortabler zu machen. Hierdurch wird aber der Zugriffsschutz auf das Netz unterminiert.

Da die PIN also den Zugriff auf das Netz schützt, nicht aber den auf das Endgerät, muss für dieses unbedingt ein Passwort gesetzt werden. Die meisten Endgeräte bieten diese Möglichkeit. Falls möglich, sollte ein alphanumerisches Kennwort unter Berücksichtigung der Empfehlungen des IT-Grundschutzkataloges (<http://www.bsi.de/gshb/index.htm>) gewählt werden,

zumindest aber ein von der PIN verschiedener Code. Zu bemängeln ist, dass dieses Kennwort meist nur beim Einschalten eines Endgeräts abgefragt wird. Die flächendeckend vorhandene Tastensperre für den laufenden Betrieb lässt sich aber in den seltensten Fällen durch ein Passwort sichern. So ist das Endgerät zwar vor der Weiterverwendung nach einem Diebstahl geschützt, dem Dieb steht aber zunächst einmal der Zugriff auf sämtliche Daten offen. Falls das Mobiltelefon zudem den Wechsel der SIM-Karte im laufenden Betrieb erlaubt, ohne auf erneute Eingabe des Passwortes zu bestehen, so ist auch die Weiterverwendung eines gestohlenen Endgerätes möglich. Bietet das Betriebssystem die Wahl, so sollten Abstriche im Komfort in Kauf genommen werden und sämtliche Änderungen am Endgerät passwortgeschützt werden. (siehe Abbildung 2)

**Zugang verweigern**

Was für die Benutzeroberfläche des Endgerätes gilt, trifft in ähnlicher Weise auch auf die Vielzahl möglicher Schnittstellen zu. Zum einen gibt es die herstellerspezifischen Schnittstellen, die zum Anschluss externen Zubehörs wie etwa Headsets oder zur Synchronisation mit dem PC per USB dienen. Darüber hinaus ist oft die Peripherieanbindung und Datenübertragung mittels Infrarot-Schnittstelle oder Bluetooth möglich. Der beste Weg, diese Schnittstellen zu sichern, ist, sie komplett abzuschalten. Das ist nicht immer möglich oder erwünscht. Eine temporäre Aktivierung bei Bedarf stellt aber einen guten Kompromiss dar. Nach Möglichkeit sollten diese Schnittstellen mit einem separaten Passwort gesichert werden. (siehe Abbildung 3)

Im Falle von Bluetooth empfiehlt sich die Nutzung des „unsichtbaren“ Modus, in dem die Endgeräte-Kennung nicht über die Funkschnittstelle gebroadcastet wird. In jedem Fall ist zu beachten, dass die momentan eingesetzten Versionen 1.2 und 2.0 nur eine einseitige Authentisierung verwenden, die Man-in-Middle-Attacken ermöglichen. Verschlüsselung findet

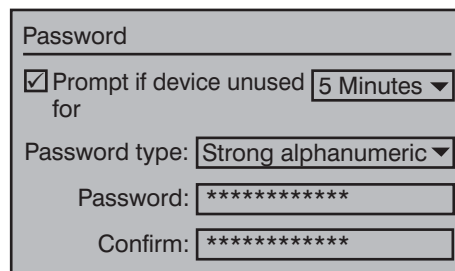


Abbildung 2: Endgeräte sollten durch ein starkes, alphanumerisches Passwort geschützt werden

bei diesen Versionen nur auf Grundlage einer nutzerdefinierten PIN oder eines gerätespezifischen Schlüssels statt. Erst die Version 2.1 wird mit Secure Simple Pairing, dass auf einem Public Key Verfahren basiert, einen wirksamen Schutz vor Man-in-the-Middle bieten. Bis zur flächendeckenden Verfügbarkeit von Version 2.1 sollte bei erhöhtem Schutzbedarf auf die Verwendung von Bluetooth verzichtet werden. Im Fall von Bluetooth-Headsets empfiehlt sich alternativ, auf Modelle zurückzugreifen, die den Datenstrom vor der Übertragung über die Luftschnittstelle zusätzlich verschlüsseln.

**Taschendiebe**

Sind alle Schnittstellen gesichert, so verbleibt trotzdem ein Restrisiko für Datendiebstahl. Wer kennt es nicht: Man steht kurz auf und lässt das Handy am Platz liegen. Ob aus Vergesslichkeit oder dem Gefühl heraus, dass während der kurzen Abwesenheit ja nichts passieren könne. Ein unbemerkter Handgriff und der Datendieb ist im Besitz des Endgeräts. Selbst falls der Zugriff auf das Endgerät per Passwort genügender Stärke gesichert ist, muss das Endgerät nicht entwendet werden, um in langwieriger Arbeit die Passwortmechanismen außer Kraft zu setzen. Zum einen hat die Datenmenge, die auf Endgeräten durchschnittlich gespeichert wird, so zugenommen, dass sie in der Regel nicht mehr auf internem Flash-Speicher des Endgeräts - geschweige denn auf der SIM-Karte - untergebracht werden kann. Da der Einbau eines sehr großen Flash-Speichers fes-

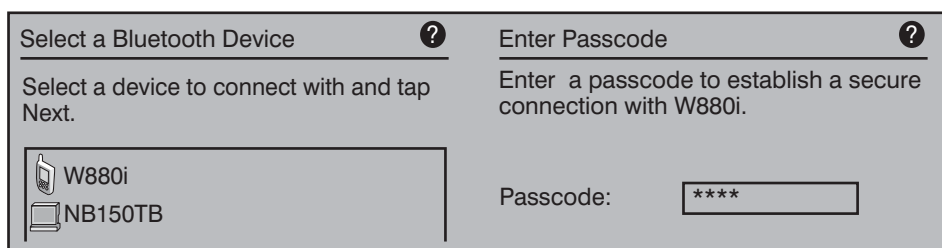


Abbildung 3: Bluetooth unterstützte in frühen Versionen nur die Authentisierung per PIN

## Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 2

ter Größe unwirtschaftlich und unflexibel ist, wird zumeist auf auswechselbare Speicherkarten zurückgegriffen. Sie bieten dem Anwender höheren Komfort und mehr Flexibilität bei der Verwaltung von größeren Datenmengen und das zu einem sehr günstigen Preis. Und nicht nur Musikdateien, Klingeltöne, Videos, Fotos und andere im Consumer-Segment sehr verbreitete Datenformate werden auf solchen Karten abgelegt. Auch Kontakte, Kurzmitteilungen, Zusatzapplikationen und andere - eventuell sensible - Daten können hierauf gespeichert werden. Der große Nachteil ist, dass eine solche Speicherkarte mit ein paar Handgriffen entnommen und kopiert oder ausgetauscht werden kann.

## „Forensik“

Der nächstliegende Gedanke zur Sicherung sensibler Daten wäre also, diese ausschließlich auf dem kleineren, fest verbauten Flash-Speicher des Endgeräts abzulegen. Doch angesichts der Tatsache, dass heutzutage große Datenmengen in Form von Emails mit Anhängen, Grafiken und Dokumenten aller Art auf dem mobilen Endgerät zum Arbeitsalltag gehören, ist das eine kaum gangbare Methode. Auch kann man den Einschub für Speicherkarten kaum physikalisch gegen Entnahme der Speicherkarten sichern. Zudem lässt sich über die herstellereigene Synchronisationschnittstelle ein physikalisches Abbild der im Endgerät vorhandenen Speichermedien machen. Hierfür kann entweder ein Standard-PC mit passendem Adapterkabel und einer entsprechenden Software für den „forensischen“ Einsatz verwendet werden. Alternativ bieten Hersteller von Produkten für „mobile forensics“ mittlerweile kompakte Geräte mit ähnlichen Abmessungen wie ein mobiles Endgerät. (siehe Abbildung 4)



Abbildung 4: Forensische Hardware von Paraben

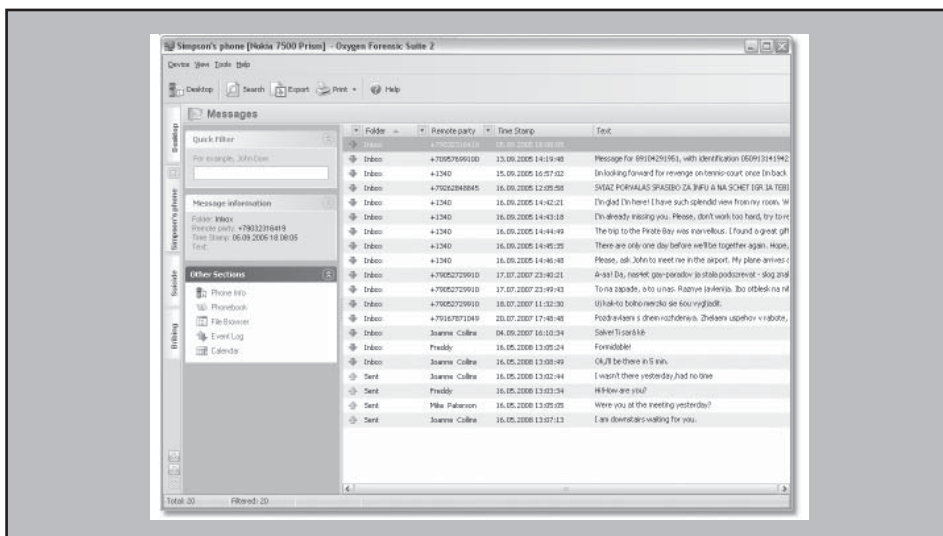


Abbildung 5: Analysesoftware von Oxygen Forensics

Mit Hilfe solcher Werkzeuge kann unauffällig ein Speicherabbild zur späteren Analyse an einem leistungsfähigen Rechner erstellt werden. Sowohl diese Geräte als auch die Software zur Analyse der so gewonnenen Daten haben die legale Intention der Datenwiederherstellung und der digitalen Beweisführung für Unternehmen und Behörden. Der Erwerb ist problemlos möglich, der beschriebene Einsatz zum Datendiebstahl stellt allerdings in Deutschland einen Straftatbestand dar. Industriespione oder Betrüger, die es auf sensible Daten abgesehen haben, wird das wohl kaum abschrecken. (siehe Abbildung 5)

## Verschlüsselter Datenbestand

Da bleibt dem Nutzer schließlich nur eine Wahl: wenn er die Daten schon nicht vor dem Zugriff Dritter schützen kann, muss er durch Verschlüsselung dafür sorgen, dass sie für Unbefugte nutzlos sind. Aktuelle Verschlüsselungsverfahren mit Block- und Schlüssellängen von 128 bis 2048 Bit wie z.B. das, auch als Advanced Encryption Standard (AES) bekannte, Rijndael-Verfahren, bieten dem aktuellen Erkenntnisstand nach einen zuverlässigen Schutz. AES ist beispielsweise auch für höchste behördliche Geheimhaltungsstufen zulässig. Darüber hinaus ist der Algorithmus bei korrekter Implementierung performant genug, um Prozessoren aktueller Smartphones nicht über die Maßen auszulasten. Dennoch sind immer leichte, wenn auch vielleicht nicht wahrnehmbare, Performanceeinbußen zu erwarten. Die Verschlüsselung insbesondere sensibler Daten ist trotzdem unverzichtbar. Darunter fallen:

- Persönliche Informationen
- Kontaktdaten
- Nachrichten sensiblen Inhalts
- Passwörter und Zertifikate

Diese Informationen stellen das absolute Minimum der zu schützenden Daten dar. Hinzu kommen Dateien aus Office- und Unternehmensanwendungen. Da der Anwender nicht immer im laufenden Betrieb zwischen sensiblen und weniger sensiblen Informationen unterscheiden kann, sollten der Einfachheit halber sämtliche Daten bzw. das komplette Speichermedium verschlüsselt werden. Die einzige Ausnahme sollten Daten sein, die in Echtzeitanwendungen zum Einsatz kommen und nicht mit der notwendigen Geschwindigkeit vom Endgerät entschlüsselt werden können. Deren Inhalt darf allerdings nicht sensibel sein. Ein Beispiel sind privat genutzte Musikdateien. (siehe Abbildung 6)

Einige moderne Endgeräte bieten die Möglichkeit, sämtliche enthaltenen Daten zu verschlüsseln. Wenn dies nicht der Fall ist, oder falls die gebotenen Verschlüsselungsmechanismen keine ausreichende Sicherheit bieten, kann die Verschlüsselung durch Drittanbieterapplikationen implementiert werden. Für die sichere Speicherung von Passwörtern und Zertifikaten zur Authentisierung stehen ebenfalls verschiedene Software-Lösungen zur Verfügung, die den Zugriff durch ein oder mehrere Masterpasswörter regulieren. Produkte zur Verschlüsselung sorgen dafür, dass benötigte Daten im laufenden Betrieb - ohne Zutun des Nutzers - entschlüsselt werden. Idealerweise sind die Daten auch während dieser Nut-

Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 2

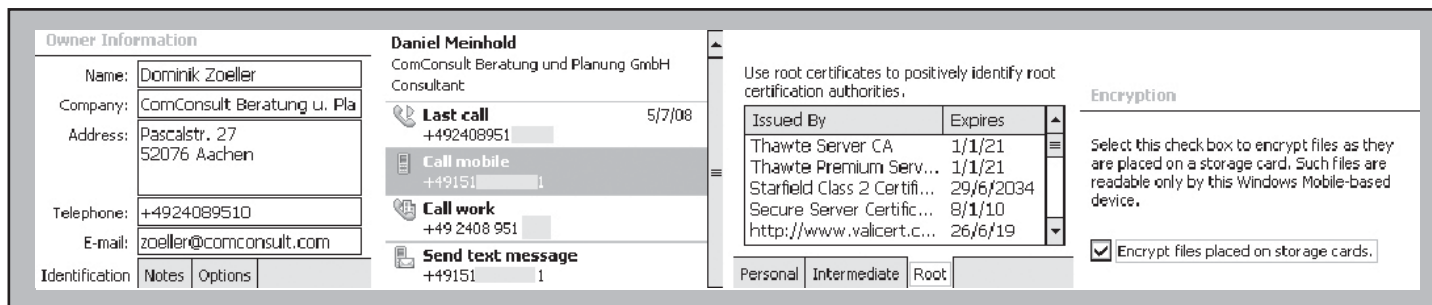


Abbildung 6: Kontaktdaten und andere sensible Daten werden durch Verschlüsselung geschützt

zungszeiträume weiterhin vor Zugriff geschützt, zum Beispiel durch konkrete Freigabe für bestimmte Applikationen. Weiterer Vorteil einer solchen, applikationsbasierten Freigabe ist es, dass ein zusätzlicher Schutz vor eventuell von außen eingeschleppter Schadsoftware geschaffen wird.

**Einheitlich anfällig**

Aktuelle Smartphones sind kleine Computer mit eigenem Betriebssystem. Ob Symbian, Windows Mobile, ob Mac OS.X in der iPhone-Variante oder Googles Android - auch wenn sich die Zahl der Viren und Trojaner noch in Grenzen hält, wird mit der steigenden Verbreitung intelligenter Telefone die Zahl solcher Schadprogramme zunehmen. Das liegt zum einen an der häufigeren Nutzung von Mobiltelefonen im Allgemeinen und den vielen Sicherheits-Schwachstellen, die die Endgeräte in Folge sehr kurzer Entwicklungs- und Produktzyklen mit sich bringen. Zum anderen benötigen Schadprogramme immer eine möglichst einheitliche Plattform zu ihrer Verbreitung. Diese Basis wird

erst durch die Nutzung geräteunabhängiger Betriebssysteme geschaffen. Was allerdings auf der einen Seite eine größere Angriffsfläche für Schadprogramme bietet, ist in vieler Hinsicht ein sicherheitstechnischer Vorteil. Durch die geräteunabhängige Weiterentwicklung wird der Nachteil der kurzen Produktzyklen teilweise kompensiert. Zudem befördert es auch die einfachere Entwicklung robuster und sicherer Applikationen, welche unabhängig vom Endgerät eingesetzt werden können. (siehe Abbildung 7)

Zu diesen Applikationen zählen auch Instrumente für den Schutz der Endgeräte, allen voran Virens Scanner und Software zum Aufspüren von Spyware und Trojanern. Hier bieten viele namhafte, teils bereits aus dem PC-Bereich bekannte Hersteller entsprechende Produkte an. Selbiges gilt für Personal Firewalls, die sich bei der Verwendung mobiler Daten Dienste empfehlen und einen wirksamen Schutz vor unbefugtem Zugriff über die Netzwerkschnittstellen bieten können.

**Zentralkomitee**

Die Absicherung der Endgeräte setzt, neben der Installation von Zusatzapplikationen, die Konfiguration einer Vielzahl von Parametern voraus. Hinzu kommen Deployment von Betriebssystem, Zertifikaten und nutzerspezifischen Konfigurationen. Um in großen Unternehmen und Organisationen dem einzelnen Anwender eine manuelle Konfiguration zu ersparen, empfiehlt sich der Einsatz einer Lösung für das Mobile Device Management (MDM). So kann die versehentliche oder absichtliche Fehlkonfiguration von Endgeräten vermieden und der Technische Support entlastet werden. Solche Lösungen sind von vielen Herstellern verfügbar (z.B. RIM, iAnywhere, Synchronica, ubitexx) und erlauben die Verwaltung verschiedenster Endgeräte und Betriebssysteme. Die Kompatibilität mit dem gewünschten Betriebssystem und den Endgeräten muss im Einzelnen vor Anschaffung geprüft werden.

Vor Einführung eines MDM muss eine detaillierte Richtlinie für die Endgerätesicherheit erstellt werden. Insbesondere sollten folgende Punkte erfasst werden (siehe Abbildung 8):

- Benutzergruppen und -hierarchie
- Kategorisierung sensibler Daten
- Richtlinien zur Speicherung und Verschlüsselung von Daten
- Einschränkung benötigter und genehmigter Zusatzapplikationen
- Einschränkung benötigter Dienste und Leistungsmerkmale
- Konfiguration für den Zugriff auf die Unternehmensinfrastruktur
- Festlegung unveränderlicher Konfigurationsparameter

Diese Richtlinie wird dann anhand des MDM als Templates für alle Benutzergruppen und Endgerätetypen umgesetzt. Weiterer Vorteil einer solchen Lösung ist, dass die verwalteten Mobiltelefone im laufenden Betrieb administriert werden können. Sobald eine Datenverbindung

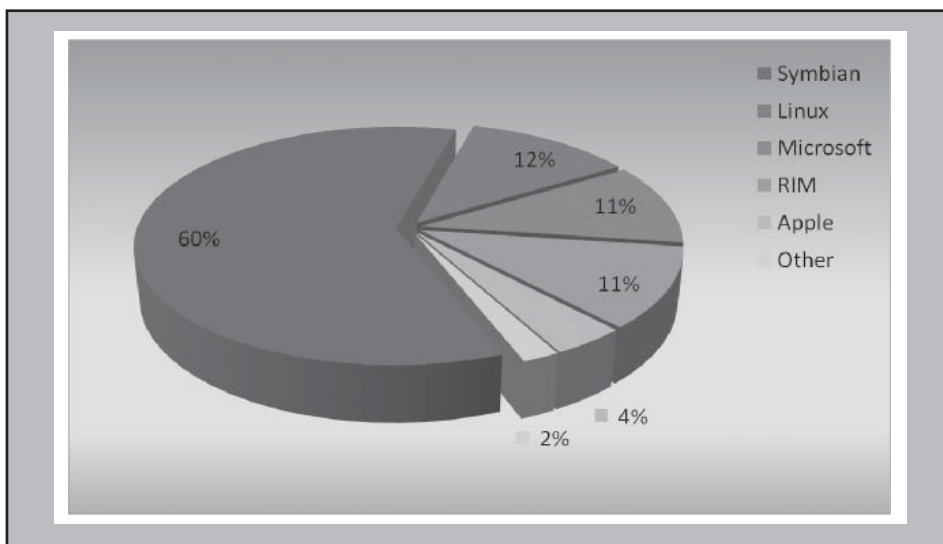


Abbildung 7: Einige wenige Betriebssysteme teilen sich den Markt der mobilen Endgeräte (Quelle: Symbian Foundation, Stand Q1/2008)

Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 2

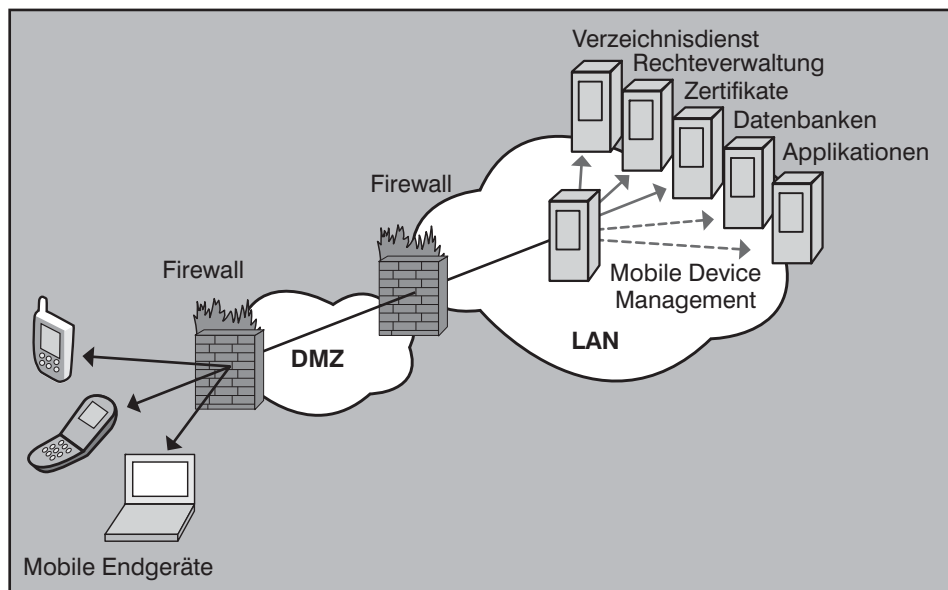


Abbildung 8: Mobile Device Management verwaltet Endgeräte und Zugriffsrechte

verfügbar ist, können Konfigurationsdaten zentral verwaltet und so Nachbesserungen an den Sicherheitsrichtlinien schnell umgesetzt werden. Außerdem ist das Zurücksetzen des kompletten Mobiltelefons auf den Werkzustand möglich. Des Weiteren erlauben einige Lösungen, die Daten auf verloren gegangenen Endgeräten per Fernzugriff zu vernichten, so dass die Gefahr eines Datendiebstahls verringert wird. Diese Möglichkeiten wiegen den Aufwand und die Kosten der notwendigen Infrastruktur auf und machen MDM für Unternehmen mit vielen mobilen Mitarbeitern sehr attraktiv.

**Überwachung des Luftraums**

Sind die Endgeräte gegen den direkten Zugriff gesichert, stellt sich immer noch die Frage der Übertragungssicherheit. Einige Endgeräte bieten die Möglichkeit, den Verschlüsselungsstatus der Luftschnittstelle anzeigen zu lassen. In der Regel wird eine verschlüsselte Verbindung durch ein kleines Schloss-Symbol im Display angezeigt. Das bietet dem Anwender zumindest eine gewisse Transparenz in Bezug auf die Verbindungssicherheit. Wünschenswert wäre auch eine Anzeige, welche Form der Verschlüsselung verwendet wird, also A5/1, A5/2 oder das momentan als sicher geltende Kasumi. Nachteil der grafischen Signalisierung ist, dass sich der Status auch während eines Gesprächs ändern kann, beispielsweise beim Zellwechsel oder beim Roaming durch verschiedene Betreiber netze. Eine solche Änderung wird von einigen Endgeräten zusätzlich akustisch mitgeteilt. Aber auch das Wissen um die Ver-

schlüsselung der Luftschnittstelle kann die Abhörgefahr nur eindämmen, nicht aber ausräumen. Wie im ersten Teil beschrieben, endet die Verschlüsselung der Sprach- und Datenkommunikation bei Eintritt in das Providernetzwerk. Da ist es am Unternehmen, eine einheitliche Lösung für die Ende-zu-Ende-Verschlüsselung der Kommunikation ihrer Mitarbeiter bereitzustellen. Hier stehen verschiedene Varianten zur Verfügung.

**Sichere Klassiker**

Die wohl wasserdichteste Möglichkeit, die Sprachkommunikation abzusichern, ist der Einsatz von speziellen Kryptographie-Endgeräten. Verschiedene Hersteller wie z.B. die Rohde & Schwarz SIT GmbH bieten solche mit speziellem Kryptographiechip ausgestattete Mobiltelefone. Das Betriebssystem des als Basis verwendeten Standard-Mobiltelefons wird derart angepasst, dass sich die Verschlüsselung der Sprachdaten einschalten lässt, falls die Gegenseite über ein gleichartiges Verschlüsselungssystem verfügt. Alle namhaften Hersteller garantieren durch Zertifizierungen für die Sicherheit der eingesetzten Verfahren. Allerdings ist die sichere Kommunikation damit in der Regel auf Endgeräte desselben Herstellers beschränkt. Zudem ergibt sich durch die hardwareseitige Realisierung ein weiterer Nachteil: die Implementierung findet auf Basis bereits auf dem Markt befindlicher, bewährter Endgeräte statt. Die technische Basis des Endgeräts hinkt also dem aktuellen Stand der Technik immer ein wenig hinterher. Neben den technischen Einschränkungen, die sich hieraus ergeben, stellt sich hier die Frage der Akzeptanz im Unternehmen. Gerade im geschäftlichen Umfeld ist das Handy heute nicht nur Kommunikationsmittel, sondern immer auch Prestige-Objekt und Spiegel der technischen Aktualität des Unternehmens. Auch wenn es unter Sicherheitsaspekten sinnvoll sein mag, wird kaum ein Vorstandsmitglied gerne sein iPhone gegen ein TopSEC GSM auf Basis des zu-

**Jetzt Leser werden**

**Der Netzwerk Insider**

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.



Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:

<http://www.comconsult-akademie.de/de/Registrierung.php>

Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 2

verlässigen, aber betagten Siemens S35i eintauschen. Die Abhängigkeit vom verwendeten Endgerät kann also die Einführung deutlich erschweren. Hinzu kommt ein vergleichsweise hoher Preis der Endgeräte, der den flächendeckenden Einsatz im Unternehmen unwirtschaftlich werden lässt.

**Von Ohr zu Ohr**

Unabhängig vom mobilen Endgerät sind kryptographiefähige Headsets. In der Festnetz-Telefonie werden bei erhöhtem Schutzbedarf gerne so genannte „Kryptographie-Boxen“ eingesetzt. Diese Hardware verschlüsselt die Sprachdaten im Zusammenspiel mit einer weiteren Crypto Box auf der Gegenseite. So entsteht ein virtueller, gesicherter Sprachkanal. Kryptographiefähige Headsets funktionieren nach einem ähnlichen Prinzip. Während der eigentliche Übertragungskanal unbeeinflusst bleibt, werden die übermittelten Sprachdaten verschlüsselt. Dies geschieht bereits im Headset, so dass selbst im Endgerät die Sprachdaten niemals unverschlüsselt vorliegen. So ist, sogar bei Kompromittierung der Übertragungswege oder des Endgeräts, die Sicherheit der Sprachdaten immer gewährleistet. Das Problem dieser Lösung liegt darin, dass die Gegenstelle meist über ein identisches Headset verfügen muss. Zwar kommen standardisierte Verfahren für Schlüsseltausch und Verschlüsselung zum Einsatz, die Kompatibilität ist aber in der Regel auf Geräte desselben Typs, zumindest aber Produkte desselben Herstellers beschränkt. Das führt zu dem organisatorischen Problem, sämtliche Gesprächspartner mit der notwendigen Technik auszustatten. Der Aufwand lohnt in der Regel nur für abgeschlossene Personenkreise, die regelmäßig untereinander sensible Informationen austauschen. Bestes Beispiel wären Mitglieder der Geschäftsleitung oder Unternehmensvorstände. (siehe Abbildung 9)

Eine weitere Möglichkeit unter Einsatz



Abbildung 9: Crypto-Hardware von DICA

von Kryptographie-Hardware sind spezielle Speicherkarten im SD-Format (Secure Digital), welche für den mobilen Einsatz in unsicheren Umgebungen konzipiert sind. Sie bieten eine Reihe von Sicherheitsfunktionen, wie z.B. verschlüsselter Speicherplatz, interne Schlüsselgenerierung und sichere Speicherung von Schlüsseln und Zertifikaten. Auf Basis dieser Funktionen wird dann ein Kommunikationsframework aufgesetzt, welches für die automatische Aushandlung der Verschlüsselung übertragener (Sprach-)Daten sorgt. Die notwendige Software wird oft für mehrere Betriebssysteme angeboten, so dass der Einsatz nicht auf Mobiltelefone beschränkt ist. Auch ein Einsatz auf Notebooks mit SD-Card Leser ist möglich. Des Weiteren erlauben verschiedene Lösungen auch das zentrale Management solcher SD-Karten. So ist ein unternehmensweiter Einsatz leichter zu implementieren. Auf diesem Verfahren können verschiedene Software-Lösungen für verschlüsselte Sprach- und Datenkommunikation realisiert werden. (siehe Abbildung 10)

**Unified Security**

Der software-basierte Ansatz ist wohl die flexibelste Variante verschlüsselter Telefonie. Es wird eine Kommunikationssoftware eingesetzt, die sämtliche Sprachdaten vor der Übertragung verschlüsselt. Hier stehen diverse Produkte zur Auswahl. Nahezu jeder Voice-over-IP (VoIP) Client besitzt die Fähigkeit zur Verschlüsselung. Der Vorteil liegt in



Abbildung 10: Crypto-Headset von Rohde&Schwarz

der Verfügbarkeit solcher Lösungen für eine Vielzahl von Endgeräten und Betriebssystemen. Der Einsatz ist nicht alleine auf mobile Endgeräte beschränkt, was eine Integration in die Kommunikationsinfrastruktur eines Unternehmens erleichtert. Zu beachten ist, dass die Sprachdaten dann aber nicht, wie im Fall von Kryptographie-Endgeräten oder -Headsets, über die Sprachkanäle des Mobilfunknetzes übertragen werden. Hierfür werden - im Falle von VoIP - IP-fähige Datenkanäle wie GPRS, EDGE oder UMTS verwendet. Dabei können Daten zur Signalisierung zwischen Client und Kommunikationsserver, also beispielsweise SIP oder H.323, auf dem kompletten Übertragungsweg durch Verwendung von Protokollen wie TLS (Transport Layer Security) geschützt werden. Da die Sprachdaten, im Gegensatz zu den Signalisierungsdaten, bei VoIP mittels Real Time Protocol (RTP) direkt zwischen

**Jetzt Leser werden**

**Der Netzwerk Insider**

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.



Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:

<http://www.comconsult-akademie.de/de/Registrierung.php>

## Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 2

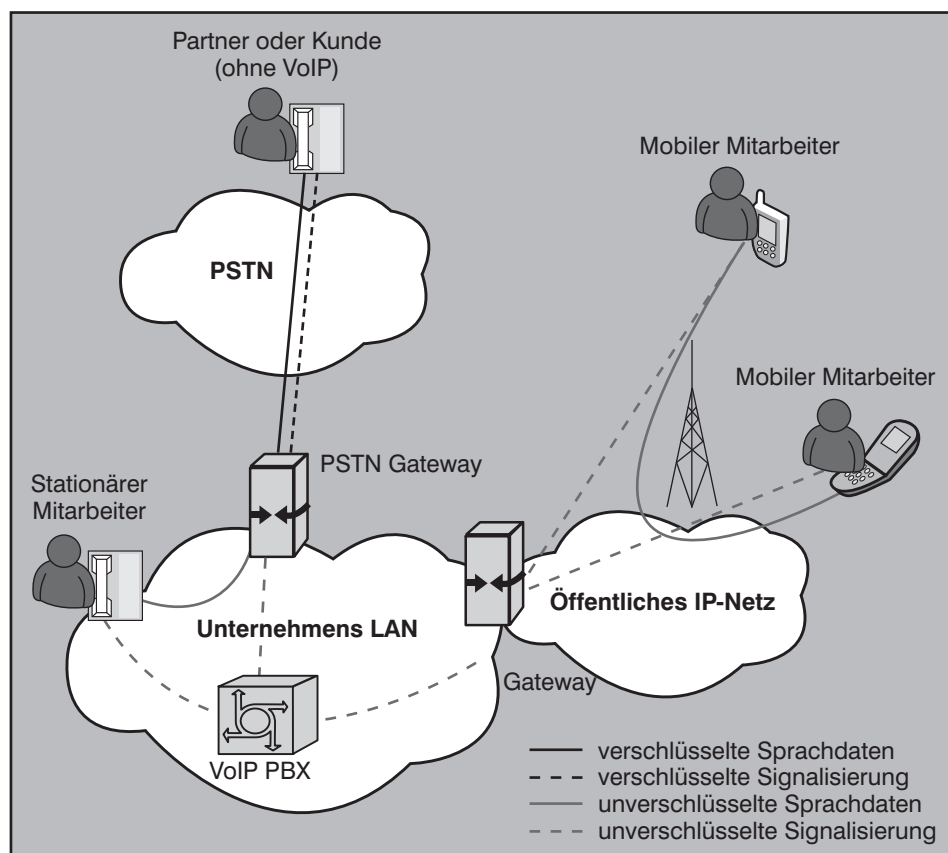


Abbildung 11: Verschlüsselte VoIP-Telefonie ermöglicht sichere Kommunikation im Mobilfunknetz

den Teilnehmern geroutet werden, muss man diese separat verschlüsseln. Hierfür kommt die Variante Secure Real-Time Protocol (SRTP) zum Einsatz, die auf dem AES Algorithmus basiert. Der Schutz der notwendigen Zertifikate und gespeicherten Zugangsdaten muss - unabhängig von der eingesetzten Kommunikationssoftware - durch verschlüsselte Datenträger, spezielle SD-Cards oder Applikationen zur Aufbewahrung von Passwörtern erfolgen. (siehe Abbildung 11)

Nachteil einer solchen Lösung sind die - je nach Tarif deutlich höheren - Gebühren, die für die Übertragung über Datenkanäle anfallen. Ohne entsprechende Datentarife oder Flatrates ist eine solche Lösung kaum wirtschaftlich zu betreiben. Hinzu kommt, dass für die Telefonie ins öffentliche Telefonnetz (Public Switched Telephony Network, PSTN) Gateways benötigt werden. Während Privatanwender und kleinere Unternehmen hier auf Dienstanbieter für IP-Telefonie zurückgreifen können, bietet es sich für mittlere und große Unternehmen an, solche Gateways im Rahmen der unternehmensweiten Kommunikationslösung im eigenen Haus bereitzustellen. Allerdings fallen in beiden Fällen zusätzliche Verbindungsgebühren

für den Übergang ins öffentliche Telefonnetz an. Zudem ist zu beachten, dass der RTP-Strom am PSTN-Gateway neu kodiert wird. Die Verschlüsselung endet somit beim Übergang ins öffentliche Telefonnetz. Ende-zu-Ende Verschlüsselung liegt also nur dann vor, wenn das Gespräch zwischen zwei SRTP-fähigen VoIP-Clients geführt wird. Ab dem Gateway können dann - für ausgewählte Verbindungen - bei Bedarf dieselben Verfahren eingesetzt werden, wie sie auch bislang zur Verschlüsselung von Festnetz-Telefonie angewendet wurden.

Trotzdem bleibt der Vorteil, dass vom Endgerät bis zum Gateway, welches sich optimalerweise in einer abgeschotteten Netzwerkumgebung befindet, die Sprachdaten hinreichend geschützt sind. Zudem kann bei unternehmensweiter Einführung von VoIP und den zugehörigen Verschlüsselungsverfahren die Sicherheit der gesamten internen Kommunikation erhöht werden. Ein weiterer Vorteil ist, dass man ohne großen Mehraufwand, anstelle reiner VoIP-Lösungen, umfangreiche Unified Communications Produkte einsetzen kann. Diese bieten neben der Telefonie weitere nutzbringende Kommunikationsformen wie Instant Messaging, Presence

oder Videokonferenz. Instant Messaging (IM) kann hier als Alternative zur Verwendung von Kurzmitteilungen (Short Message Service, SMS) dienen. Andernfalls müssten diese, um ihre Vertraulichkeit zu wahren, ebenfalls einer Inhaltsverschlüsselung unterzogen werden, da - wie auch bei der Sprachkommunikation - netzseitig keine Ende-zu-Ende Verschlüsselung möglich ist. IM kann im Rahmen einer unternehmensweiten Unified Communications Lösung sicher übertragen werden und stellt somit eine Alternative zu SMS innerhalb des Unternehmens dar. Unter Verwendung einer Unified Communications Lösung wird das Mobiltelefon also zum integralen Bestandteil der Unternehmenskommunikation, statt einer ungesicherten Insel und ein Einfallstor ins Unternehmensnetz zu bilden.

## Datentunnel

Neben der Telefonie ist auch die mobile Datenkommunikation besonderen Gefährdungen ausgesetzt. Der Zugriff auf das Unternehmensnetzwerk - sei es zum Abrufen von Emails oder für den Zugriff auf sensible Daten - muss daher zusätzlich geschützt werden. Hierfür empfiehlt sich der Aufbau eines Virtual Private Network (VPN). Dabei stellt der Client, nach erfolgreicher Authentisierung, eine gesicherte Verbindung ins Unternehmensnetz her und erhält eine IP-Adresse aus diesem Netz zugewiesen. Durch diese Verbindung werden dann sämtliche Daten „getunnelt“, der Client befindet sich vermeintlich innerhalb des Unternehmensnetzwerkes. Hieraus ergeben sich einige Vor- und Nachteile. Nachteil von VPN-Tunneln ist die im Vergleich zu unverschlüsselten Verbindungen reduzierte effektive Datenrate. Der durch VPN entstehende Overhead treibt das übertragene Datenvolumen in die Höhe, was die Nutzbarkeit schmalbandiger Datendienste wie GPRS deutlich einschränkt. Zudem entstehen dadurch erhöhte Kosten, so dass ein Einsatz von VPN nur bei gelegentlicher Nutzung oder aber entsprechenden Datentarifen in Frage kommt. Nachteilig ist mit Sicherheit auch, dass das Endgerät zur Schwachstelle des Unternehmensnetzes wird. Ist es nicht ausreichend gesichert, so besteht die Gefahr, dass ein Angreifer sich des Endgeräts bemächtigt und so Zugriff auf die Daten des Unternehmens erhält. (siehe Abbildung 12)

Hiergegen kann man eine Reihe von zusätzlichen Vorsichtsmaßnahmen ergreifen. Idealerweise werden den Endgeräten IP-Adressen aus einem gesonderten Subnetz zugewiesen, welches von den

Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 2

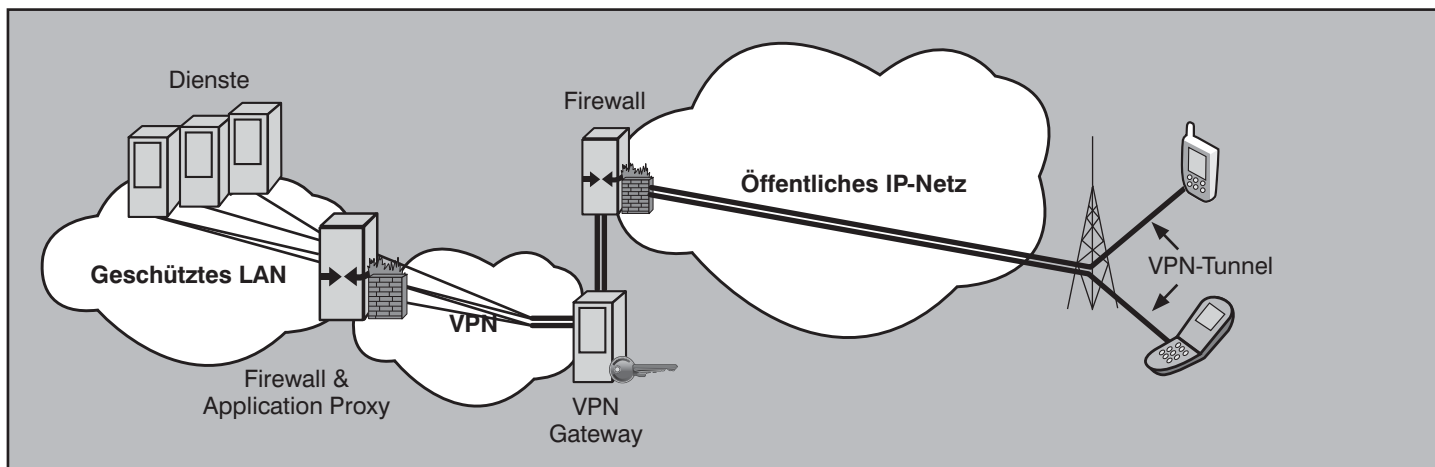


Abbildung 12: Mögliche Architektur einer VPN-Lösung für den mobilen Zugriff

sensiblen Subnetzen des Unternehmens durch eine Firewall getrennt wird. Diese reguliert den Zugriff auf die für die mobilen Endgeräte zugänglichen Daten und Dienste im Unternehmen. Diese Dienste können zusätzlich von vorgelagerten Proxy Servern erbracht werden, so dass kein direkter Zugriff auf die sensiblen Subnetze notwendig ist und somit das Produktivnetz vor eventuell kompromittierten Endgeräten geschützt wird. Als Schutz vor verlorenen oder gestohlenen Endgeräten empfiehlt es sich, zum Aufbau des Tunnels IPsec mit zertifikatsbasierter Authentisierung zu nutzen. Die Zertifikate können zentral verwaltet und im Verlustfall einfach gesperrt werden. Das Subnetz für den VPN-Zugang kann - bis auf den VPN-Server - vom WAN vollständig getrennt werden, oder aber durch eine Firewall und weitere Komponenten, wie einen Web Proxy, einen kontrollierten Zugang auf das WAN erlauben. So ist es auch möglich, den Zugriff auf Dienste im Internet generell über das Unternehmensnetzwerk umzuleiten und durch Proxies die Nutzung der Dienste entsprechend der Unternehmensrichtlinien einzuschränken. Die Bereitstellung weiterer Infrastruktur wie WAP Proxies und Synchronisationsserver für Push Mail sind eine sinnvolle Ergänzung einer solchen Infrastruktur.

**Schutz vor Dritten**

All diese Maßnahmen dienen dazu, die Benutzung der Endgeräte im täglichen Gebrauch sicherer zu machen. Während man solche Maßnahmen für sämtliche Endgeräte innerhalb von Unternehmen und Organisationen relativ problemlos realisieren kann, gibt es keine Möglichkeit diese Maßnahmen auf Endgeräte anzuwenden, die von Partnern, Kunden oder Besuchern in die Firmenumgebung

mitgebracht werden. So besteht prinzipiell immer die Möglichkeit, dass schlecht administrierte und dadurch anfällige Endgeräte Dritter die Vertraulichkeit von Informationen gefährden. Das gilt insbesondere für schützenswerte Bereiche in Unternehmen und Behörden wie etwa Entwicklungsabteilungen, Vorstandsbüros, Rechenzentren und Konferenzräume in denen vertrauliche Besprechungen stattfinden. Da man nicht sicher stellen kann, dass Personen, die solche Umgebungen betreten, ihre Endgeräte entsprechend umsichtig konfiguriert haben, muss die Verwendung von Mobilfunk in solch sensiblen Bereichen unterbunden werden. Ansonsten wäre es möglich, dass ein Angreifer das Endgerät eines Anwesenden zum Abhören von Besprechungen oder für den Diebstahl von Daten aus geschützten Umgebungen verwendet. (siehe Abbildungen 13 und 14)

Der einzig wirksame Schutz hiervoor ist es, klare Verhaltensmaßregeln und Richtlinien für die Verwendung von mobilen Endgeräten im Unternehmen zu erstellen. Eine Zutrittskontrolle, bei der jeder Anwesende auf das Mitführen eines Endgeräts untersucht wird, ist in der Regel weder

wirtschaftlich noch organisatorisch sinnvoll durchzuführen. Sie lohnt nur in Bereichen besonders hoher Gefährdungsstufe und selbst hier verkommen entsprechende Vorschriften meist zu reiner Symbolik. Alle Autoren dieses Artikels verfügen über mindestens zwei aktiv genutzte Mobilfunkgeräte - für Industriespione dürfte das gleiche gelten. Unter diesen Umständen fällt es leicht ein Alibi-Gerät beim Pförtner zu hinterlassen. Ohne zumindest stichprobenartige Taschenkontrollen und Leibesvisitationen wird jedes Handyverbot zur Farce.

Ein anderer denkbarer Weg wäre das Unterbinden sämtlicher Mobilkommunikati-



Abbildung 13: Passiver GSM-Detektor (Quelle: Starport international)



Abbildung 14: GSM-Jammer OMS-105T (Quelle: Omnis)

## Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 2

on durch aktive Störsender (engl. „jammer“). Der Einsatz ist allerdings für die Privatwirtschaft in Deutschland nicht zugelassen und auch im behördlichen Umfeld nur äußerst eingeschränkt möglich. Die Abschirmung von Räumen gegen elektromagnetische Strahlung und somit auch gegen die Funkwellen der Mobilfunknetze ist technisch unproblematisch möglich, aber sehr aufwändig und teuer. Auch diese Maßnahme ist nur für Räumlichkeiten mit sehr hoher Geheimhaltungsstufe sinnvoll. Da bleibt nur die Möglichkeit, eingeschaltete und eventuell sendende Endgeräte mithilfe von Detektoren aufzuspüren, um die Einhaltung der Sicherheitsrichtlinien zu überprüfen. Mobilfunkdetektoren unterscheiden sich in aktive und passive Geräte. Aktive Detektoren senden selbst, wie auch eine Basisstation des Mobilfunknetzes, Statusanfragen, die durch eingeschaltete Endgeräte auch im Stand-By Modus beantwortet werden. Solche Detektoren sind in Deutschland, wie auch aktive Störsender, nicht zulässig. Einzig die Nutzung passiver Detektoren, die Endgeräte mit einer aktiven Verbindung aufspüren können, können auch im privatwirtschaftlichen Umfeld eingesetzt werden. Sie bieten damit Schutz vor aktivem Abhören durch eine stehende Sprachverbindung oder der Übertragung von Daten aus dem Unternehmen heraus. Allerdings können sie keine Endgeräte detektieren, die eingeschaltet sind und eventuell ein vertrauliches Gespräch aufzeichnen, um diese zu einem späteren Zeitpunkt zu übertragen.

## Klare Richtlinien

Ob die Absicherung von geschützten Bereichen, die Konfiguration und das Management der Endgeräte oder die Auswahl der genutzten Netze und Dienste - Unternehmen, Organisationen und Behörden müssen gleichermaßen klare Richtlinien für den Umgang mit mobilen Kommunikationsmitteln schaffen. Diese Richtlinien müssen dem technischen Stand bei Einführung entsprechen und die Sicherheitserfordernisse der verwendeten Dokumente in den verschiedenen Nutzergruppen widerspiegeln. Hierzu sollte auf einer bestehenden Klassifizierung unternehmensinterner Dokumente aufgesetzt werden. Anhand der Nutzergruppen und ihrer Aufgabengebiete lassen sich dann Anforderungen an Netze, Endgeräte und Software definieren und die notwendige Infrastruktur aufbauen. Analog sollten diese Richtlinien auf bestehende Mobilfunklösungen angewendet und diese einer Revision unter Sicherheitsaspekten unterzogen werden.

Aufgrund der rasanten technischen Entwicklung und nutzergetriebener Innovation in diesem Sektor fällt es schwer, diese Richtlinien immer dem aktuellen technischen Stand von Netzen und Endgeräten anzupassen. Umso wichtiger wäre es, die Mitarbeiterschaft davon zu überzeugen, dass Sicherheitskonzepte nur durch ihr aktives Zutun wirksam werden können. Jenseits aller technischen Schutzmaßnahmen ist es immer noch der Mensch, der täglich mit dieser Technik arbeitet. Problembewusstsein und ein adäquates Basiswissen zum Umgang mit sensiblen Daten sind daher ebenso wichtig wie technische Maßnahmen. Die Praxis sieht leider meist anders aus. Vorsorge dieser Art ist auf Dauer jedoch immer preiswerter, als das Risiko von unkontrolliert versickernden Informationsströmen.

## Quellen &amp; Literaturhinweise

Broschüre „Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte“, Bundesamt für Sicherheit in der Informationstechnik, <http://www.bsi.de/literat/doc/oefms/index.htm> (zuletzt überprüft: 22.09.2008)

Maßnahmenkatalog Organisation, M2.188 „Sicherheitsrichtlinien und Regelungen für die Mobilfunknutzung“, Bundesamt für Sicherheit in der Informationstechnik, <http://www.bsi.bund.de/gshb/deutsch/m/m02188.htm> (zuletzt überprüft: 15.10.2008)

Report „VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung“, ComConsult-Research / ComConsult Technologie-Information GmbH, [http://www.comconsult-research.de/de/vpn\\_r.htm](http://www.comconsult-research.de/de/vpn_r.htm) (zuletzt überprüft: 15.10.2008)

Artikel „Passwörter und PINs auf dem Handy sicher speichern“, Bernd Reder, [www.networkcomputing.de / CMP-WEKA Verlag GmbH & Co. KG](http://www.networkcomputing.de/CMP-WEKA), <http://www.networkcomputing.de/passwoerter-und-pins-auf-dem-handy-sicher-speichern/> (zuletzt überprüft: 15.10.2008)

Artikel „Wie man Spitzel austrickst“, [www.stern.de / stern.de GmbH](http://www.stern.de), <http://www.stern.de/computer-technik/telefon/Kryptografie-Wie-Spitzel/631568.html> (zuletzt überprüft: 15.10.2008)  
Artikel „Verschlüsselte Mobiltelefonie“, [www.compliancemagazin.de / PMK Presse, Messe & Kongresse Verlags GmbH](http://www.compliancemagazin.de), <http://www.compliancemagazin.de/produkte/verschlueselung/rohdeschwarz230307.html> (zuletzt überprüft: 15.10.2008)

## Jetzt Leser werden

## Der Netzwerk Insider

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.



Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:

<http://www.comconsult-akademie.de/de/Registrierung.php>