WissenHeute Jg. 60 11/2007

Das Thema im Überblick

Mobile Datenkommunikationslösungen erfordern einen ganzheitlichen Ansatz in Bezug auf Sicherheitsaspekte. Es können nicht nur einzelne Komponenten einer mobilen Datenkommunikationslösung betrachtet werden, sondern das gesamte System muss als Einheit gesehen und entsprechend gesichert werden.

Sicherheitskonzepte für mobile Datenlösungen

Mobile Datenlösungen durchdringen heute alle Bereiche der Wirtschaft. Angefangen von Einwahllösungen für den Vertriebsaußendienst über Dispositionssysteme für Service-Mitarbeiter bis hin zu Spezialanwendungen im Bereich Logistik (beispielsweise ein Flottenmanagement) oder der Automatisierung. In allen Fällen werden sensible Daten erhoben, gespeichert und übertragen. Mobile Endgeräte in unterschiedlichen Bauformen und Leistungsmerkmalen mit einer Vielzahl von Schnittstellen, die neben der Tastatur und dem Display auch Anschlüsse zu den verschiedenen Mobilfunknetzen, dem Festnetz oder Nahbereichskommunikation zulassen, erhalten Zugang zu geschützten Unternehmensnetzen. Hieraus ergeben sich vielfältige Risiken, die bereits in der Konzeption von mobilen Datenlösungen berücksichtigt werden müssen. Ein wirkungsvoller Schutz kann nur unter Einbeziehung aller Systemkomponenten erzielt werden.

Der Autor

Dipl.-Ing. Stefanus Römer studierte Allgemeine Elektrotechnik an der RWTH in Aachen und ist seit 1994 im Konzern Deutsche Telekom als Produktmanager tätig. Seit April 2001 arbeitet er bei T-Mobile als Produktmanager für mobile Datenlösungen und Mobilfunksicherheit. Er hat bereits zahlreiche Beiträge in WissenHeute sowie ein Fachbuch über mobile Datenkommunikation veröffentlicht.

1 Einsatzfelder

Für die Unternehmen ist es wichtig, gezielte Informationen zur richtigen Zeit am richtigen Ort und in der richtigen Form zur Verfügung zu stellen. Die wachsende Bedeutung des Produktionsfaktors Information in allen Bereichen der Wirtschaft zwingt sie zu einer umfassenden Vernetzung entlang ihrer gesamten Wertschöpfungskette, und zwar angefangen mit den Lieferanten über die internen Unternehmensbereiche bis hin zu den Kunden. Wer in den dynamischen Märkten von heute bestehen möchte, muss schnell und flexibel auf veränderte Bedingungen reagieren können. Der verschärfte Wettbewerb erfordert insbesondere eine größere Kundennähe mit deutlich verkürzten Reaktionszeiten bei Akquisition und Service. Die Qualität der Kundenbetreuung wird somit zum entscheidenden Wettbewerbsfaktor und bedingt den verstärkten Einsatz von Außendienstmitarbeitern und deren flexible Anbindung an das vorhandene Kommunikationsnetz. Mobile Datenlösungen bieten unter anderem folgende Vorteile:

- Steigerung der Produktivität durch Nutzung von bisher unproduktiven Arbeitszeiten z. B. während einer Dienstreise,
- Steigerung der Wettbewerbsfähigkeit durch verbesserten Kundenservice,
- Kosteneinsparung durch effizientere Kommunikationsabläufe oder
- schnellere Entscheidungsprozesse.

Mobile Datenkommunikationslösungen kommen in den verschiedensten Bereichen zum

Einsatz. Neben speziellen Lösungen für bestimmte Wirtschaftszweige wie beispielsweise Transport und Logistik oder die Energiewirtschaft findet man auch branchenübergreifende Lösungen. Häufig werden durch den Einsatz mobiler Datenkommunikation nicht nur die Kosten gesenkt und die Effizienz gesteigert, sondern auch neue Einsatzmöglichkeiten erschlossen, die mit bisheriger Technik und Arbeitsweise nicht denkbar waren. Nachfolgend werden beispielhaft einige typische Anwendungsszenarien beschrieben.

1.1 Lösungen für den Vertriebsaußendienst

Vertriebsmitarbeiter müssen kurzfristig und kompetent auf Kundenanfragen reagieren können und im Kundengespräch stets auskunftsfähig sein. Mobile Einwahllösungen ermöglichen es, jederzeit und unabhängig vom Ort auf zentrale Daten zuzugreifen. Hierzu gehören beispielsweise:

- Kundendaten (Verträge, Historie, Rechnungsdaten),
- Produktdaten (Beschreibungen, Präsentationen, Preise, Lieferzeiten, Verfügbarkeiten) und
- Auskünfte zu aktuellen Bestellvorgängen.

Der Vorteil liegt in einer unmittelbaren Steigerung des Vertriebserfolgs. Der Vertriebsmitarbeiter ist jederzeit kompetent und kann dem Kunden sofort alle nötigen Informationen beschaffen, um einen Auftrag abzuschließen.

1.2 Lösungen für den technischen Kundendienst

Der technische Kundendienst muss schnell auf Serviceaufträge reagieren können und Störungen umgehend beseitigen. Insbesondere im Investitionsgüterbereich wird eine schnelle Verfügbarkeit von Servicetechnikern und eine professionelle Instandsetzung in kurzer Zeit vorausgesetzt. Durch den Einsatz mobiler Einwahllösungen lassen sich gegenüber der herkömmlichen Arbeitsweise erhebliche Effizienzgewinne realisieren. Ohne den Einsatz von mobilen Dispositionslösungen fahren Servicetechniker im Außendienst gewöhnlich zu Beginn ihres Arbeitstages in die Einsatzzentrale, um sich ihre Arbeitsaufträge für den Tag abzuholen. Es folgt die Anreise zum Kunden, dann die Serviceleistung selbst. Arbeitszeiten, gefahrene Kilometer, durchgeführte Wartungsarbeiten, Ergebnisse und Ersatzteilbestellungen werden handschriftlich festgehalten. Zwischendurch melden sich die Techniker allenfalls per Mobiltelefon, um nach weiteren Aufträgen zu fragen. Informationen über Ersatzteilverfügbarkeit, Lieferzeiten und Preise sind jedoch in der Regel vor Ort nicht verfügbar und können dem Kunden erst am nächsten Tag mitgeteilt werden. Am Ende des Arbeitstages geht es wieder zurück in die Zentrale, um die Daten manuell in das Warenwirtschaftssystem einzugeben. Lösungen zur Optimierung und Beschleunigung des technischen Service ermöglichen demgegenüber

- eine strukturierte Disposition der Servicetechniker (sofortige Auftragsweiterleitung, Routenplanung, sofortige Leistungsverrechnung) und
- einen Zugriff auf Lagerbestände, Preisauskunft und sofortige Bestellung.

Diese Vorteile sind eine deutliche Verkürzung von Reaktions- und Entstörzeiten, eine signifikante Kostenreduktion sowie insbesondere eine erhöhte Kundenzufriedenheit.

1.3 Automatisierungslösungen (Maschine-zu-Maschine)

Die Vernetzung von technischen Anlagen wie Maschinen, Zählern, Automaten oder Fahrzeugen mit einer zentralen Steuerungs- und Überwachungsstelle wird im industriellen Bereich zunehmend erfolgskritisch.

Beispiel eines Energieversorgers
Energieversorger unterhalten eine Vielzahl geografisch verteilter Zähler und Stellwerke (Utilities), die notwendig sind, um das Energieversorgungssystem zu überwachen und zu steuern. Für diese Utilities gibt es eine Reihe von Anwendungsfeldern:

- Zählerfernabfrage, die heute zunehmend auf GPRS-Lösungen (General Packet Radio Service) umgestellt wird, um aktuelle und genaue Verbrauchsdaten für die Kunden zu bekommen,
- Service und Maintenance[1],
- Remote Management der Messgeräte,
- Echtzeitabfrage aller Zähler (quasi-gleichzeitig), anstatt zeitaufwendiger und teurer Abfragen über leitungsvermittelte Modemverbindungen.

Die Vorteile sind Kostenersparnis und Produktivitätssteigerungen der jeweiligen Anlagen sowie Qualitätssteigerungen und die Erschließung neuer Nutzungsmöglichkeiten (z.B. die Teilnahme am Stromhandel auf der Basis zeitgenauer Zustandsdaten).

Beispiel für Transport und Logistik
Lösungen für Auftragsmanagement, Sendungsverfolgung, Fahrzeugdaten- und Statusübermittlung sowie für die Ortsinformation von Fahrzeugen oder Containern auf Basis von SMS (Short Message Service) stehen seit vielen Jahren zur Verfügung. Die deutlichen Kostenvorteile durch Einsatz dieser Lösungen lassen sich mit der GPRS-Technik noch weiter steigern.

2 Sicherheit

Laut Aussage des BSI (Bundesamtes für Sicherheit in der Informationstechnik) nehmen die Sicherheitsrisiken sowohl in Quantität als auch in Qualität deutlich zu. Das Thema Sicherheit gewinnt daher für viele Unternehmen zunehmend an Bedeutung. Viele Unternehmen und Privatpersonen haben bereits eigene Erfahrungen mit Online-Bedrohungen und deren Folgen gemacht (Bild 1). Oft sind es nur Belästigungen durch Spammails, aber auch Datenverlust oder ein Systemausfall kann die Folge von Sicherheitsverletzungen sein. Die Zahlen der sich im Umlauf befindlichen Computerviren, Trojaner und Würmer steigen seit Jahren exponentiell an (Bild 2). Gleichzeitig werden immer mehr geschäftskritische Unternehmensprozesse auf das Internet verlagert.

Durch die Einbeziehung von Mobilfunkgeräten in geschäftskritische Datenlösungen er-

[1] **Maintenance:** Wartung.

geben sich grundsätzlich die gleichen Bedrohungen wie bei der Nutzung von stationären Rechnern. Auf Grund der Mobilität und der speziellen Bauform dieser Geräte entstehen jedoch zusätzliche Risiken durch Gerätediebstahl oder verlorene Geräte, weil oftmals sensible Daten unverschlüsselt in den Geräten selber gespeichert werden und nach einem Geräteverlust offen zugänglich sind. Trotz der bereits vielfach implementierten Sicherheitsmechanismen der Geräte und Anwendungen bestehen noch viele Schwachstellen, die bei der Erarbeitung eines Sicherheitskonzepts gezielt beachtet werden müssen. Wichtig ist grundsätzlich jedoch, dass alle beteiligten Personen, sowohl Nutzer als auch Administratoren, über die möglichen Gefahren informiert und für die einzelnen Schutzmaßnahmen sensibilisiert werden, um einen wirkungsvollen Schutz zu gewährleisten.

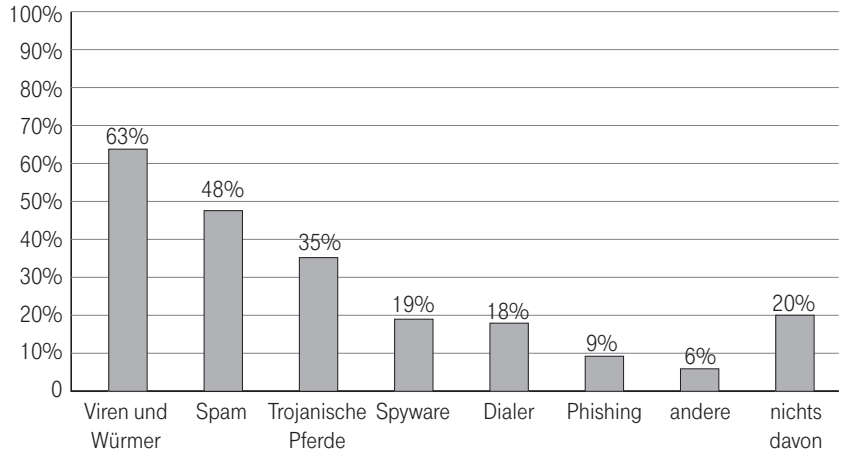
3 Vorgehensmodell

Das grundlegende Vorgehensmodell zur Erstellung eines Sicherheitskonzepts umfasst die folgenden Teilschritte (Bild 3):

- Schutzbedarf ermitteln
- Schutzmaßnahmen bestimmen
- Schutzmaßnahmen umsetzen
- permanente Erfolgskontrolle

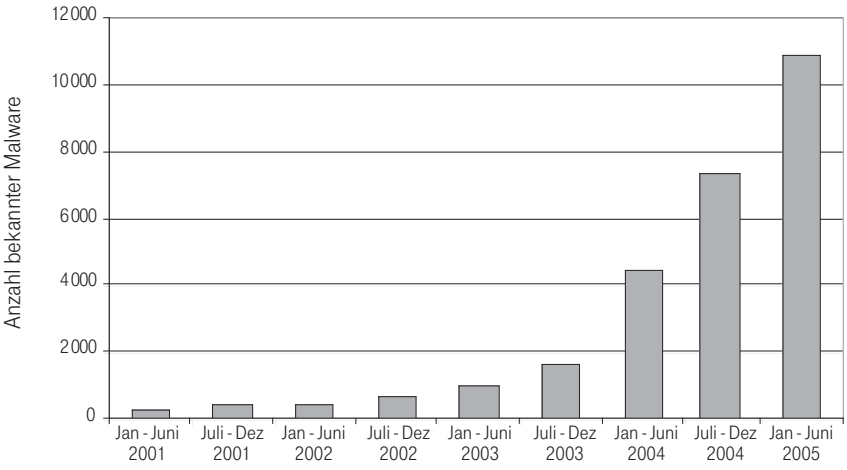
Zu Beginn einer Sicherheitskonzeption steht zunächst eine allgemeine Analyse des Gesamtsystems mit allen Einzelkomponenten und darauf aufbauend die Ermittlung des allgemeinen Schutzbedarfes. Ein Sicherheitskonzept muss alle Komponenten einer mobilen Datenlösung einbeziehen. Eine punktuelle Sicherheitsmaßnahme ohne Berücksichtigung des Gesamtsystems und ohne Analyse des allgemeinen Schutzbedarfs ist häufig wirkungslos und kann von einem Angreifer in der Regel leicht umgangen werden. Der jeweilige Schutzbedarf richtet sich nach der Kritikalität[2] des jeweiligen Anwendungsszenarios und nach der jeweiligen Systemkonfiguration. Beispielsweise können periodisch wiederkehrende anonyme Ortsinformationen eines Messgeräts weniger kritisch und damit schutzwürdig sein als der E-Mail-Verkehr eines leitenden Angestellten einer Firma.

Bild 1 Persönliche Erfahrung mit Online-Bedrohungen



Quelle: Bundesamt für Sicherheit in der Informationstechnik, Bürger-Umfrage 2006

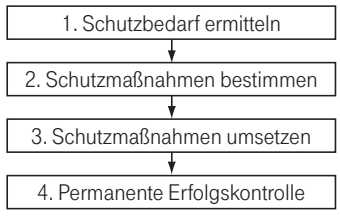
Bild 2 Bedrohung durch Viren, Würmer und Trojaner



Quelle: Symantec Internet Security Report, September 2005

Basierend auf dem ermittelten Schutzbedarf werden die einzelnen konkreten Schutzmaßnahmen festgelegt und implementiert. Entscheidend für einen dauerhaften Schutz ist allerdings eine permanente Kontrolle, weil sich durch den technischen Fortschritt jederzeit neue, noch unbekannte Angriffsmöglichkeiten eröffnen können (Erosion der Sicherheit), die eine Anpassung des Sicherheitskonzepts erforderlich machen.

Bild 3 Vorgehensmodell zur Erstellung eines Sicherheitskonzeptes



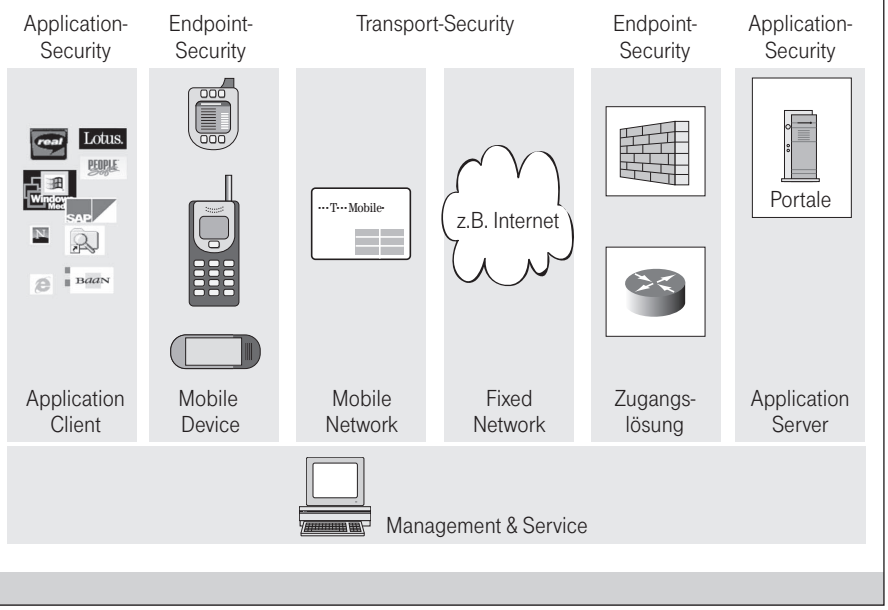
4 Allgemeine Risikoanalyse

Eine mobile Datenlösung umfasst im Allgemeinen folgende Komponenten[3] (Bild 4):

[2] **Kritikalität:** Bezeichnung für die direkten und indirekten Auswirkungen bei Fehlverhalten von Personen und/oder Geräten.

[3] Siehe hierzu „Leitfaden zur mobilen Applikationsentwicklung", Stefanus Römer, Books on Demand, Februar 2007.

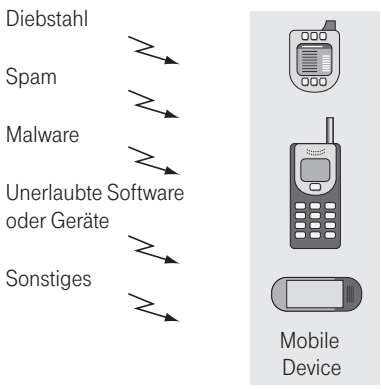
Bild 4 Elemente einer mobilen Datenlösung



- Die Anwendung, bestehend aus Server-Teil und Client-Teil
- Die mobile Endgeräteplattform, bestehend aus Rechner, Betriebssystem und mobilem Endgerät
- Das Mobilfunknetz, basierend auf GPRS oder UMTS (Universal Mobile Telecommunications System)
- Eine Festnetzverbindung zwischen Mobilfunknetz und Unternehmensnetz
- Eine Zugangslösung zum Unternehmensnetz
- Ein übergreifendes Netz-Management

Jede dieser Einzelkomponenten muss im Rahmen der Sicherheitsanalyse auf mögliche Angriffspunkte hin untersucht und berücksichtigt werden. Da sich die Anwendung selbst und damit das Sicherheitskonzept auf Anwendungsebene einer allgemeinen Betrachtung entzieht, wird diese Komponente nachfolgend nicht weiter beschrieben.

Bild 5 Bedrohungen für mobile Endgeräte



5 Risikoanalyse Mobilfunkgerät

Mobilfunkgeräte wie zum Beispiel Smart-Phones und PDAs (Personal Digital Assistants) haben sich inzwischen zu leistungsstarken Computern entwickelt, deren Rechenleistung und Speicherkapazität von mehreren hundert Megabyte mit den PC-Standards früherer Jahre durchaus vergleichbar ist. Über immer breitbandigere mobile Datendienste können diese Endgeräte nahezu überall mit dem Internet oder einem Unternehmensnetz verbunden werden. Dadurch entstehen weitere Gefahren für die einzelnen Unternehmensnetze (Bild 5). Da immer mehr sensible Daten auf diesen Endgeräten gespeichert werden können, ergibt sich ein zusätzliches Risiko beispielsweise durch deren Verlust oder eventuellen Diebstahl.

Moderne Mobilfunkgeräte mit offenen Betriebssystemen[4] sind grundsätzlich den gleichen Gefahren ausgesetzt wie stationäre Arbeitsplatzrechner. Hierzu gehören beispielsweise:

- Bedrohung durch Viren, Würmer und Trojaner (Malware)[5] mit den möglichen Folgen wie erhöhten Kommunikationskosten, eingeschränkte Gerätenutzung, erhöhte Support-Kosten, Ausspähung vertraulicher Daten, Datenmanipulation oder Datenverlust.
- Bedrohung durch unerwünschten Nachrichtenempfang mittels E-Mail oder MMS (Multimedia Messaging Service) mit den möglichen Folgen wie beispielsweise erhöhte Kommunikationskosten bei E-Mail-Empfang und eingeschränkte Gerätenutzung.
- Bedrohung durch Installation und Nutzung unerlaubter Software mit dem möglichen Einschleusen von Malware in das Unternehmensnetz, eingeschränkte Gerätenutzung und erhöhte Support-Kosten.

Hinzu kommen auf Grund der Bauform das zusätzliche Risiko eines Geräteverlusts und der damit verbundenen Gefahr eines unbefugten Zugriffs auf sensible Daten, die lokal auf dem Gerät gespeichert sind.

6 Risikoanalyse Transportnetz

Das Transportnetz innerhalb einer mobilen Datenlösung unterteilt sich in den Bereich des Mobilfunknetzes und in einen Festnetzanteil, über den die Verbindung zwischen Mobilfunknetz und Unternehmensnetz realisiert wird. In vielen Fällen wird für diese Verbindung das Internet genutzt. Daneben können für diesen Zweck jedoch auch Mietleitungen oder Verbindungen über eine ATM- (Asynchronous Transfer Mode-) oder MPLS- (Multi-Protocol Label Switching-)Plattform geschaltet werden. Aufgabe des Transportnetzes ist die zuverlässige und sichere Datenübertragung zwischen Mobilfunkgerät und Unternehmensnetz sowie die Gewährleistung einer korrekten Abrechnung. Zu den möglichen Gefahren in diesem Bereich zählen (Bild 6):

[4] **Offenes Betriebssystem:** engl. Open Source, eine Software, deren Quellcode frei zugänglich ist.

[5] Siehe hierzu den Beitrag „Mobile Security – Schutzmaßnahmen für Mobilfunkendgeräte“, WissenHeute, 10/2006, S. 557 ff.

- Bedrohung durch Abhören der übertragenen Daten mit den möglichen Folgen: Zugriff auf sensible Anwendungsdaten durch Unbefugte, Verlust der Vertraulichkeit, Verlust der Anonymität.
- Bedrohung durch Datenmanipulation oder Einschleusen von Daten mit den möglichen Folgen: Verlust der Datenintegrität, Verlust der Authentizität.
- Bedrohung durch DoS[6]-Attacken (Denial-of-Service) auf das Unternehmensnetz mit den möglichen Folgen wie eingeschränkte Verfügbarkeit des Unternehmensnetzes und erhöhte Kommunikationskosten.
- Bedrohung durch überhöhte Kosten (Overbilling) auf Grund von unerwünschtem Datenempfang auf der Mobilfunkseite[7].

7 Risikoanalyse Zugang zum Unternehmensnetz

Die Zugangslösung zum Unternehmensnetz ist die Schnittstelle zwischen den externen Zugangsnetzen und den kritischen Ressourcen im gesicherten internen Netz, das im unmittelbaren Einflussbereich des Netzadministrators liegt. Hauptaufgabe dieser Komponente ist der Schutz der internen Netzressourcen vor unbefugten Zugriff, Manipulation, Übernahme oder Zerstörung sowie DoS-Attacken, die deren Verfügbarkeit einschränken. Zu den möglichen Gefahren gehören im Wesentlichen (Bild 7):

- Bedrohung durch Einschleusen von Malware mit den möglichen Folgen: Erhöhte Kommunikationskosten, eingeschränkte Verfügbarkeit, Ausspähung vertraulicher Daten, Datenmanipulation oder Datenverlust.
- Bedrohung durch unbefugten Zugriff mit den möglichen Folgen: Verlust der Vertraulichkeit; Verlust der Anonymität; Verlust der Datenintegrität durch Manipulation.
- Betriebliche Störungen der Netzverfügbarkeit.
- Bedrohung durch DoS-Attacken mit der möglichen Folge einer eingeschränkten Verfügbarkeit der internen Unternehmensressourcen (z. B. Server und Datenbanken).

8 Allgemeine Schutzmaßnahmen

Basierend auf dem grundlegenden Systemmodell und der allgemeinen Risikoanalyse für mobile Datenlösungen lassen sich nachfolgend Schutzmaßnahmen für die Einzelkomponenten ableiten. Welche Maßnahmen in einem konkreten Anwendungsszenario jedoch umgesetzt werden sollten, hängt vom Schutzbedarf der jeweiligen Datenlösung ab.

8.1 Schutzmaßnahmen beim Mobilfunkgerät

Um Mobilfunkgeräte gegen die oben beschriebenen Risiken zu schützen, bieten sich folgende Einzelmaßnahmen an:

- Zugriffssicherung durch Passwort (pre-boot password) mit dem Ziel eines Schutzes vor unbefugtem Zugriff auf Daten und Anwendungen auf dem betreffenden Gerät.
- Datenverschlüsselung auf dem Endgerät und auf externen Speichermedien mit dem Ziel von Schutz vor unbefugtem Zugriff auf sensible Daten.
- Voreingestelltes Benutzerprofil auf dem Mobilfunkgerät durch den Administrator und Einsatz von Remote Device Management mit dem Ziel, dass nur freigegebene Geräte und Software Zugriff auf die Anwendungen bekommen.
- Einsatz von Antiviren-Software mit dem Ziel, das Gerät vor dem Eindringen von Malware zu schützen und die Verbreitung von Malware zu unterbinden.
- Nur gesicherte Netzwerkverbindungen nutzen beispielsweise durch den Einsatz von IP-VPN (Internet Protocol-Virtual Private Network), Deaktivierung von Bluetooth- und Infrarot-Schnittstellen, kein direkter Zugriff auf das Internet mit dem Ziel, Datenintegrität und Datenauthentizität zu gewährleisten.

8.2 Schutzmaßnahmen für das Transportnetz

Die Aufgabe des Transportnetzes ist die zuverlässige und sichere Datenübertragung zwischen Mobilfunkgerät und Unternehmensnetz. Hierzu bieten sich folgende Schutzmaßnahmen an:

Bild 6 Bedrohungen im Transportnetz

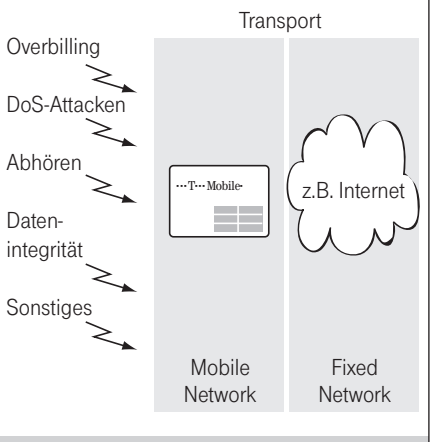
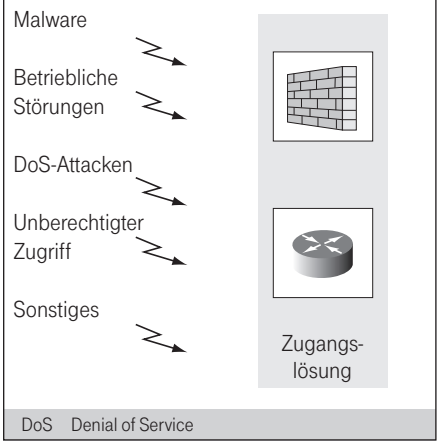


Bild 7 Bedrohungen im Bereich der Zugangslösungen



- Zugangsschutz zum Mobilfunknetz durch SIM-basierte PIN-(Subscriber Identity Module, Personal Identification Number)Abfrage mit dem Ziel, eine unbefugte Nutzung zu verhindern.
- Einsatz einer geschlossenen Benutzergruppe und Authentisierung der teilnehmenden Mobilfunknutzer mit dem Ziel, den unbefugten Zugriff durch Dritte auf Unternehmensressourcen zu unterbinden.
- Verschlüsselung im GPRS-Netz mit dem Ziel, Datenintegrität und Datenauthentizität zu gewährleisten.

[6] **DoS:** Denial of Service ist ein Angriff auf Datenverarbeitungssysteme mit dem Ziel, das angegriffene System durch eine hohe Anzahl von versendeten Daten zu blockieren und für eine normale Nutzung unzugänglich zu machen.

[7] Bei der Datenübertragung mit GPRS oder UMTS sind die übertragenen Datenmengen in Sende- und Empfangsrichtung wichtig für die Abrechnung.

- Sperrung der direkten Datenübertragung zwischen zwei Mobilfunkgeräten im Mobilfunknetz mit dem Ziel, ein Overbilling zu verhindern.
- Einsatz sicherer Übertragungsverfahren im Festnetz wie beispielsweise IPSec (Internet Protocol Security), ATM oder MPLS mit dem Ziel, Datenintegrität und Datenauthentizität zu gewährleisten sowie ein Mithören zu vermeiden.
- Nutzung einer vertrauenswürdigen Datentransportplattform im Festnetz (beispielsweise ATM oder MPLS), um DoS-Attacken oder das Einschleusen von Malware zu unterbinden.
- Redundante Anbindung des Unternehmensnetzes an das Mobilfunknetz mit dem Ziel, die Netzverfügbarkeit zu erhöhen.

8.3 Schutzmaßnahmen beim Zugang zum Unternehmensnetz

Die Aufgabe der Zugangslösung ist der Schutz der internen Netzressourcen vor Angriffen über die externen Zugangsnetze. Hierzu bieten sich folgende Maßnahmen an:

- Einsatz einer VPN-Lösung[8] mit dem Ziel, einen unbefugten Zugriff zu unterbinden und die Vertraulichkeit, Datenintegrität und Authentizität bei der Datenübermittlung über die externen Zugangsnetze zu wahren. Grundsätzlich stehen zwei Realisierungsformen zur Auswahl[9]. Zum einen ein Client-based VPN, bei dem auf der Client-Plattform ein VPN-Client eingesetzt wird, der über das gesamte externe Zugangsnetz bis zur Zugangslösung im Unternehmensnetz einen gesicherten VPN-Tunnel, beispielsweise mit IPSec oder SSL (Secure Socket Layer), aufbaut. Zum anderen besteht die Möglichkeit eines Network-based VPN. Hier wird ein vertrauenswürdiges Zugangsnetz, das die genannten Sicherheitsziele bereits gewährleisten kann, zur Einwahl genutzt. Ein Beispiel hierfür ist „Mobile-IP-VPN“ von T-Mobile.
- Trennung vom Internet mit dem Ziel, das Einschleusen von Malware sowie DoS-Attacken zu vermeiden.
- Sichere Teilnehmerauthentisierung mit Username/Passwort (auch Einmalpasswort).
- Redundante Anschaltung des Unternehmensnetzes an das Mobilfunknetz.

9 Schutzbedarfsanalyse bei M2M (Maschine-zu-Maschine)

Basierend auf dem allgemeinen Systemmodell einer mobilen Datenlösung (s. Bild 4) ergibt sich nachfolgend ein reduziertes Systemmodell für M2M-Lösungen (Bild 8). Diese unterscheiden sich von allgemeinen mobilen Datenlösungen im Wesentlichen durch:

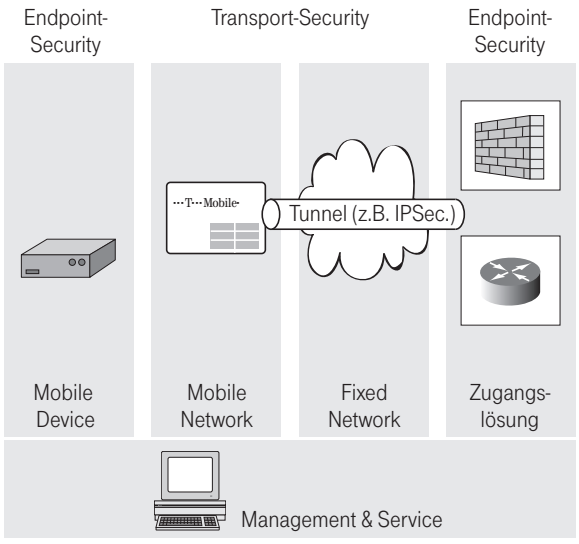
- Endgerät: Bei M2M-Lösungen kommen spezielle Endgeräte für den Festeinbau in Verbindung mit Maschinen und/oder Automaten zum Einsatz, die in der Regel keine eigene Benutzerschnittstelle bieten und nur für bestimmte Anwendungen geeignet sind.
- Feste Kommunikationsbeziehungen: Die Mobilfunkgeräte verbinden sich ausschließlich mit der Leitstelle im Unternehmen.
- Anwendungen: Bei M2M-Lösungen kommen nur wenige, in der Regel nur eine Anwendung zum Einsatz.
- Datenmenge: Bei M2M-Lösungen ist die übertragene Datenmenge pro Mobilfunkgerät in der Regel gering (üblicherweise weniger als 1 MByte pro Monat).

Verfährt man nach dem allgemeinen Sicherheitsgrundsatz, wonach in einem Anwendungsszenario nur das erlaubt werden soll, was unbedingt benötigt wird, und alles andere zu unterbinden ist, so lassen sich für M2M-Lösungen nachfolgende Sicherheitsmaßnahmen ableiten.

9.1 Endgeräte

- Nur Endgeräte ohne direkte Benutzerschnittstelle einsetzen, um unbefugten Zugriff zu unterbinden.
- Nur Endgeräte mit minimal benötigtem Funktionsumfang einsetzen, um eine missbräuchliche Nutzung zu unterbinden.
- Schutz gegen Diebstahl und Vandalismus durch Festeinbau und physikalischen Zugangsschutz (z.B. innerhalb eines Gebäudes).
- Möglichst alle sensiblen Daten sofort über eine gesicherte VPN-Verbindung übertragen. Den Schutz sensibler Daten auf den Endgeräten (falls vorhanden) durch eine Verschlüsselung durchführen.
- Nur VPN-Verbindungen mit geschlossener Benutzergruppe zulassen. Alle anderen Übertragungswege wie Internet, MMS, Bluetooth und IrDa (Infrared Data Association) möglichst unterbinden.

Bild 8 **Komponenten einer M2M-Lösung**



[8] Siehe hierzu den Beitrag „Virtuelle Private Netze – ein Überblick“, WissenHeute, 12/2005, S. 680 ff.

[9] Siehe hierzu „Leitfaden zur mobilen Applikationsentwicklung“, Stefanus Römer, Books on Demand, Februar 2007.

9.2 Transportnetz

Nutzung einer geschlossenen Benutzergruppe im Mobilfunknetz. Die Vorteile sind kein Zugriff von extern und keine Verbindung zum Internet.

9.3 Zugangslösung zur Leitstelle

Sichere Teilnehmerauthentisierung und eingeschränkte Verbindungsmöglichkeiten, beispielsweise nur VPN-Tunnel zulassen. Erhöhte Ausfallsicherheit durch redundante Anschaltung der Leitstelle.

10 Sicherheitslösung „Mobile IP VPN Basic“ von T-Mobile

Die beschriebenen Sicherheitsmaßnahmen in Bezug auf das Transportnetz und die Anschaltung an das Unternehmensnetz für M2M-Lösungen lassen sich mit Hilfe der Zugangslösung Mobile IP VPN von T-Mobile erfüllen[10] (Bild 9). Eine Lösung auf Basis von Mobile IP VPN umfasst folgende Komponenten[11]:

- Privater APN (Access Point Name[12]) mit geschlossener Benutzergruppe
- IPSec-Tunnel über das Internet zum Kunden-Router
- Kunden-Router inkl. Service
- Internet-Anschluss

Zusätzlich bietet Mobile IP VPN die folgenden optionalen Komponenten:

- Deaktivierung des Internet-APN pro SIM-Karte
- Anschaltung des Unternehmensnetzes über eine gesicherte ATM[13]- oder MPLS[14]-Plattform
- Benutzer-Authentisierung (statisches Password oder One Time Password)
- Statische oder dynamische IP-Adresse
- Web-basierte Administrationsoberfläche
- Redundante Netzanschaltung
- SLA (Service Level Agreement)

11 Schlussbetrachtung

Mobile Datenlösungen bieten viele Vorteile, aber auch Risiken. Durch die zunehmende Verbreitung mobiler Anwendungen und auf Grund der steigenden Bedrohungen im Internet nehmen auch hier die Sicherheitsrisiken deutlich zu.

Ein IT-Sicherheitskonzept für mobile Datenlösungen muss alle Komponenten einer mobilen Datenlösung berücksichtigen. Nur punktuelle Lösungen bieten keinen ausreichenden Schutz. Eine VPN-Lösung ist ein wichtiger Bestandteil des Sicherheitskonzeptes, weil eine geschlossene Datenlösung die höchste Sicherheit bietet. *(Ar)*

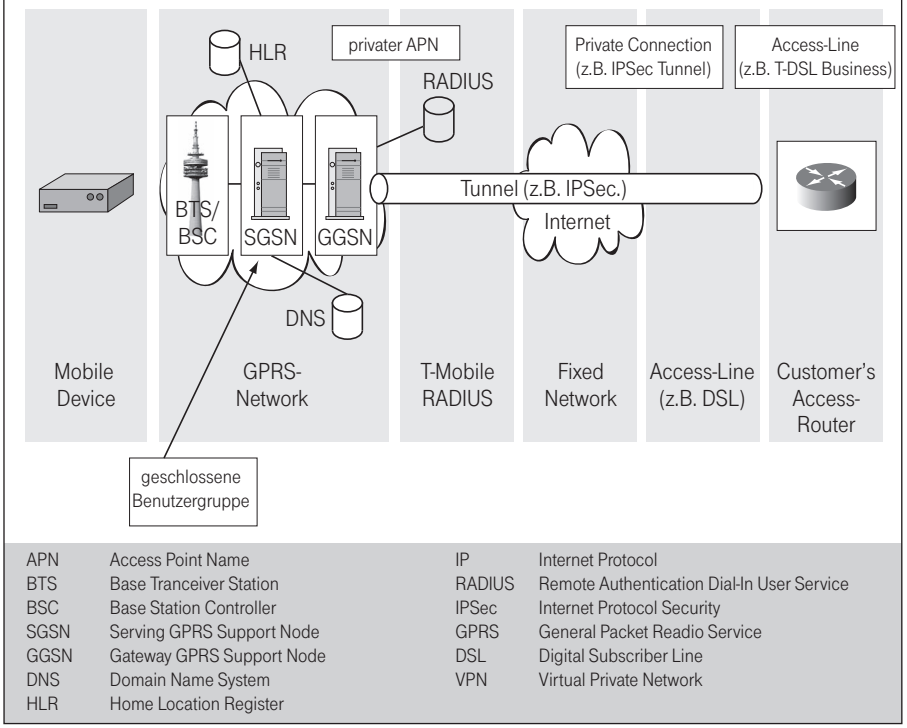
Literaturhinweis

Leitfaden zur mobilen Applikationsentwicklung, Stefanus Römer, Books on Demand, 2007

Weiterführender Internet-Link

www.stefanus-roemer.de

Bild 9 Mobile IP VPN-Basic



APN	Access Point Name	IP	Internet Protocol
BTS	Base Tranceiver Station	RADIUS	Remote Authentication Dial-In User Service
BSC	Base Station Controller	IPSec	Internet Protocol Security
SGSN	Serving GPRS Support Node	GPRS	General Packet Readio Service
GGSN	Gateway GPRS Support Node	DSL	Digital Subscriber Line
DNS	Domain Name System	VPN	Virtual Private Network
HLR	Home Location Register		

Verwendete Abkürzungen

APN	Access Point Name
ATM	Asynchronous Transfer Mode
BSI	Bundesamt für Sicherheit in der Informationstechnik
DoS	Denial of Service
GPRS	General Packet Radio Service
IP	Internet Protocol
IPSec	Internet Protocol Security
IT	Informationstechnik
M2M	Machine-to-Machine
MDA	Mobile Digital Assistant
MMS	Multimedia Messaging Service
MPLS	Multi Protocol Label Switching
PDA	Personal Digital Assistant
PIN	Personal Identification Number
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SMS	Short Message Service
SSL	Secure Socket Layer
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network

[10] Siehe hierzu „Leitfaden zur mobilen Applikationsentwicklung“, Stefanus Römer, Books on Demand, Februar 2007.

[11] Siehe hierzu den Beitrag „Mit GPRS ins Intranet – Das Produkt LAN to LAN GPRS Access“, Unterrichtsblätter Nr. 3/2001, S. 168-174.

[12] Der APN (Access Point Name) ist ein Domain-Name nach RFC 1035 (Request For Comments), der innerhalb der GPRS/UMTS-Netze genutzt wird, um das Zielnetz für eine GPRS-Verbindung zu adressieren. Im Falle des öffentlichen Internet-APN wird die GPRS-Verbindung zum Internet als Zielnetz hergestellt. Bei privaten APNs werden private Unternehmensnetze adressiert.

[13] Asynchronous Transfer Mode (ITU-T I.361- ITU-T I.366) ist ein paket- und verbindungsorientiertes Übertragungsverfahren.

[14] MPLS steht für Multi Protocol Label Switching (RFC 2547) und vereint die Vorteile der schnellen ATM-Vermittlungstechnik mit der Flexibilität von IP-Routing.