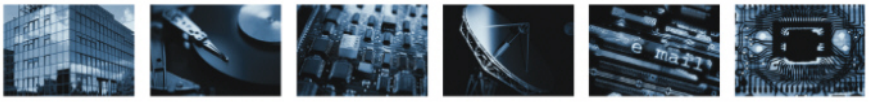
Bundesamt
für Sicherheit in der
Informationstechnik



# Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 228 99 9582-0
E-Mail: mobilfunksicherheit@bsi.bund.de
Internet: http://www.bsi.bund.de

# Inhaltsverzeichnis

# 1. Grundlagen mobiler Dienstnutzung

Mobile persönliche Endgeräte, wie Mobiltelefone oder PDAs, erfreuen sich großer Beliebtheit. Die zahlreich verfügbaren Informations- und Kommunikationsdienste bieten eine große Bandbreite der Nutzung sowohl im privaten, als auch im professionellen beruflichen Einsatz. Mit integrierten Anwendungen wie Terminplanung, elektronischem Notizblock oder E-Mail-Anwendungen leisten sie viel zur Unterstützung des Anwenders. Insbesondere bei Behörden und Unternehmen wächst der Druck, die Produktivität und Effizienz durch Nutzung dieser Geräte zu erhöhen.

Trotz der bereits implementierten Sicherheitsmechanismen der Geräte und Dienste existieren viele Schwachstellen und potentielle Bedrohungen, die beim Einsatz mobiler Endgeräte gezielt beachtet und wirksam abgewehrt werden müssen.

Dieser Text richtet sich sowohl an alle Benutzer mobiler Endgeräte und der entsprechenden Infrastrukturen, als auch an deren Verantwortliche. Dazu werden neben den Techniken auch die möglichen Bedrohungen möglichst verständlich aufgezeigt.

Dieses Kapitel beschreibt die wesentlichen technischen Grundlagen mobiler Endgeräte und Dienste, die für das Verständnis der Bedrohungen gegen diese Systeme und deren entsprechenden Gegenmaßnahmen hilfreich bzw. nötig sind. Zudem werden zur Einordnung beispielhaft Anwendungsszenarios beschrieben. Das Kapitel endet mit einem Ausblick auf zukünftige Entwicklungen.

## 1.1 Technische Grundlagen mobiler Endgeräte

Mobile Endgeräte besitzen neben der komplexen Gerätehardware auch eine Menge an Software, wie das Betriebssystem und die Kommunikations- und Anwendungssoftware. Für die Gesamtsicherheit des Gerätes ist eine Absicherung jedes dieser Teile notwendig.

### 1.1.1 Entwicklung der mobilen Endgeräte

Die Entwicklung der mobilen Endgeräte begann in den achtziger Jahren. Die damaligen Geräte waren spezialisiert (z. B. Organizer) mit geringem Funktionsumfang (in der Regel ohne Kommunikation) und sind heute vom Markt verschwunden. Sie besaßen nicht das breite Einsatzspektrum heutiger Geräte. Mitte bis Ende der neunziger Jahre entwickelten sich die PDAs als persönlicher digitaler Assistent parallel zu den Mobilfunktelefonen, jeweils mit unterschiedlichen Anforderungen, deutlich weiter. Die Verkleinerung der einzelnen Komponenten der mobilen Endgeräte macht es heute möglich, Mobiltelefone und PDAs in einem Gerät zu integrieren. Zudem werden auch moderne Nahbereichsnetze wie Bluetooth oder WLAN unterstützt.

Allerdings sind die mobilen Endgeräte im Unterschied zu normalen Arbeitsplatzrechnern auch heute noch schlecht in herkömmliche betriebliche IT-Infrastrukturen integriert. Der Zugriff und die Synchronisation der Daten der mobilen Endgeräte erfolgen durch spezielle Software. Meist sind die Daten an einen speziellen PC gekoppelt und stehen nicht von überall aus zur Verfügung.

Zudem sind die wenigen vorhandenen Sicherheitsmechanismen der kleinen Begleiter kaum ausreichend, um vertrauliche persönliche oder geschäftskritische Daten zu schützen. Der Verlust eines Gerätes bringt fast immer auch den Verlust der Vertraulichkeit der Daten mit sich.

### 1.1.2 Spezifische Eigenschaften mobiler Endgeräte

Jedes mobile Endgerät stellt heute einen leistungsfähigen Computer dar, dessen Struktur grundsätzlich dem eines herkömmlichen Arbeitsplatzrechners entspricht. Mobile Endgeräte enthalten zudem spezialisierte, für den jeweiligen Einsatzzweck benötigte Hardwarekomponenten. Alle Bestandteile des Systems sind auf niedrigen Stromverbrauch ausgerichtet und besitzen für den mobilen Einsatz spezialisierte Benutzungsschnittstellen. Im Gegensatz zu bekannten PCs ist die Hardware aber nur mit sehr

hohem Aufwand veränderbar. Der Austausch oder die Erweiterung integrierter Komponenten ist nicht möglich. Abbildung 1 zeigt den allgemeinen Aufbau mit wichtigen Komponenten eines mobilen Endgerätes unter einem Hardware-orientierten Blickwinkel, so wie er für die Sicherheitsanalyse nützlich ist.

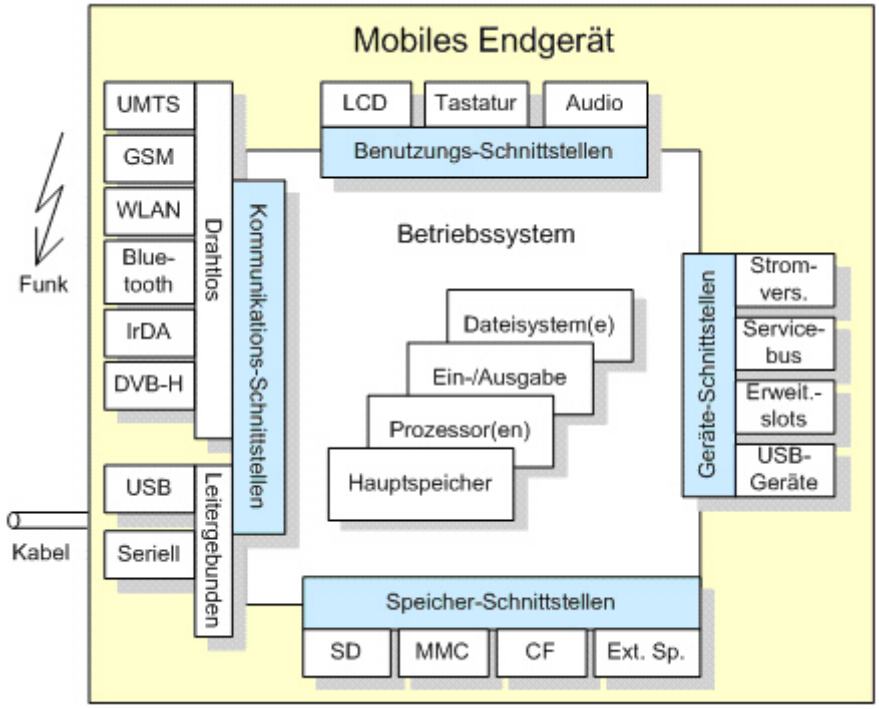



**Abbildung 1: Blockbild eines mobilen Endgerätes**

Der Übergang zwischen den in Hardware realisierten Teilen des Gerätes und den durch Software programmierten Teilen ist fließend. Insbesondere bei der Kommunikationshardware wird mehr und mehr der aufwändigen Hochfrequenzverarbeitung durch Software erledigt bzw. vorbereitet.

Je nach Gerät bzw. Produkt sind die jeweiligen Schnittstellen in unterschiedlicher Qualität vorhanden und können für Angriffe von außen genutzt werden. Die konkreten Sicherheitsbedrohungen gegen mobile Endgeräte hängen deshalb in hohem Maße vom betrachteten Gerät ab.

### Klassen von Endgeräten

Die Ergebnisse der Sicherheitsanalyse in dieser Broschüre zielen auf folgende Klassen mobiler Endgeräte ab: vorrangig Mobiltelefone und Smartphones sowie PDAs, und nachrangig Laptops und Tablet-PCs. Daneben gibt es mobile Endgeräte mit sehr speziellem Einsatzgebiet, wie Spielekonsolen, technische Diagnosegeräte oder Spezialgeräte zur mobilen Datenerfassung. Als mobile Systeme sind ebenfalls moderne Fahrzeuge mit ihrer Informationstechnik anzusehen. Sofern sich die Geräte dieses Spektrums auf das obige Blockbild abbilden lassen und deren Einsatzgebiet nicht zu speziell ist, können die Beiträge in dieser Broschüre auf sie angewendet werden.

Darüber hinaus verfügen auch RFIDs, Chipkarten, USB-Tokens und ähnliche Geräte über Eigenschaften, die mit den oben genannten Klassen Gemeinsamkeiten aufweisen. Allerdings sind sie in der Regel aufgrund fehlender eigener Energieversorgung, fehlender Benutzungsschnittstellen und begrenzter Leistungsfähigkeit nicht als eigenständige Endgeräte anzusehen und werden deshalb in dieser Broschüre nur am Rande behandelt. Für diese Geräte sind nur einige der gezeigten Bedrohungen und Gegenmaßnahmen wirkungsvoll.

### 1.1.3 Betriebssysteme

In mobilen Endgeräten kommen spezielle Betriebssysteme zum Einsatz. Die Konzepte der Betriebssysteme für mobile Endgeräte sind denen der PCs sehr ähnlich. Ihre Umsetzung unterscheidet sich allerdings von den Vertretern stationärer Geräte, da sie spezielle Benutzungsschnittstellen und ein aufwändiges Energiemanagement unterstützen müssen. Üblicherweise werden Kommunikationsverfahren, wie etwa GSM [BSI-GSM], UMTS, Bluetooth und/oder WLAN [BSI-DL], unterstützt.

Daneben werden spezielle Dateisysteme eingesetzt, die den Anforderungen an den Betrieb von Flash-Speichern und dem Starten von Anwendungen ohne Ladevorgang gerecht werden. Das Konzept des virtuellen Speichers wird, wenn überhaupt vorhanden, meist anders umgesetzt, so dass weniger Speicher pro Anwendung verwendet wird.

Bei einigen Mobiltelefonen und bei Spezialgeräten gilt, dass der Hersteller der Hardware auch das Betriebssystem erstellt. Bei den meisten mobilen Endgeräten gilt jedoch, dass der Hardware-Hersteller ein Betriebssystem zukauft und an seine Hardware anpasst. Damit ist in der Regel mehr als ein Hersteller für das Schließen von Sicherheitslücken zuständig, was den Absicherungsprozess zusätzlich erschwert.

#### Wesentliche Konzepte

Allgemein ist das Betriebssystem der Software-Teil eines Gerätes, der zwischen den Hardware-Komponenten und den Anwendungen vermittelt. Das Betriebssystem kontrolliert alle Anwendungen und deren gespeicherte Daten. Als Verwaltungszentrale ist die Sicherheit des Betriebssystems die Grundlage für einen sicheren Betrieb von Benutzeranwendungen. Schwachstellen im Betriebssystem können vom Angreifer derart ausgenutzt werden, dass die Sicherheitsmechanismen der Anwendungen unwirksam werden.

Betriebssysteme besitzen eine Reihe konkreter Aufgaben [TAN02]. Die Mechanismen, die die Sicherheit des Gesamtsystems betreffen, werden im Folgenden kurz angesprochen.

Eine der zentralen Aufgaben eines Betriebssystems ist die **virtuelle Speicherverwaltung**. Sie ist teilweise in Hardware umgesetzt und dient der Zuordnung von Speicherbereichen zu Anwendungen und Diensten. Daneben stellt sie sicher, dass sich mehrere aktive Anwendungen auf einem System nicht gegenseitig beeinflussen können.

Eine fehlerfreie Umsetzung bedeutet, dass Anwendungen ausschließlich zugewiesenen Speicher kontrolliert benutzen können. Bestimmte Mobiltelefone und ältere PDAs besitzen keine virtuelle Speicherverwaltung. Vom Benutzer installierte Programme haben damit die Möglichkeit, Daten anderer Programme zu lesen und zu verändern.

Neben virtueller Speicherverwaltung gibt es andere Speicherschutzkonzepte. Auf mobilen Endgeräten werden insbesondere Java Techniken eingesetzt, die Java Anwendungen gegenseitig absichern, ohne dass virtuelle Speicherschutzkonzepte vorhanden sind. Auf diesen Systemen können deshalb ausschließlich Java Programme nachgeladen werden, ohne dass ansonsten andere Anwendungen beeinflusst werden können.

Damit Benutzerdaten auch nach einem Neustart erhalten bleiben, besitzen Betriebssysteme Mechanismen, persistenten Speicher zu verwalten. Meistens werden diese Speicher durch **Dateisysteme** organisiert und können auch vom Benutzer direkt verwendet werden. Dateisysteme können daneben auch Dateizugriffe kontrollieren und gegebenenfalls Benutzern und Anwendungen den Zugriff verweigern. Neben Benutzerdaten werden in mobilen Endgeräten auch sicherheitsrelevante Gerätekonfigurations- und Systemdaten und kryptografisches Datenmaterial abgelegt. Durch Zugriff auf das Dateisystem können Angreifer deshalb sowohl Benutzerdaten als auch Systemdaten je nach Gerät kompromittieren.

Aktuelle Betriebssysteme für mobile Endgeräte besitzen **kryptografische Verfahren** und die jeweiligen Algorithmen. Diese Verfahren können sowohl von den Anwendungen, als auch von Kommunikationsdiensten genutzt werden. Ob diese Verfahren jedoch einfach zu benutzen sind oder ob sie sich

leicht umgehen lassen, hängt davon ab, wie gut sie in die unterschiedlichen Anwendungen und Dienste integriert sind.

Eine weitere Aufgabe der Betriebssysteme ist es, dem Benutzer einen kontrollierten Zugang zum System und zu den entsprechenden Daten zu ermöglichen. Ob sich derartige **Zugangskontrollen** umgehen lassen, wie fein diese Kontrollen durchzusetzen sind und ob mehrere unterschiedliche Benutzer verwaltet werden können, hängt vom konkreten Betriebssystem ab.

Zudem muss ein Betriebssystem für mobile Endgeräte ein gewisses Maß an **kontrollierbarer Erweiterbarkeit** besitzen. Dies ist sowohl für Gerätehersteller nötig, die ein Betriebssystem für verschiedene Geräte einsetzen, als auch für den Anwender, der zusätzliche Hardware mit dem System nutzen will.

Die Umsetzung aller dieser Konzepte bedeutet zunächst nur, dass sich Dienste und Anwendungen dieser Mechanismen bedienen können. Sind die Anwendungen oder die Dienste fehlerhaft oder werden sie schlichtweg falsch benutzt, kann auch ein sehr gut abgesichertes Betriebsystem nicht vor wirkungsvollen Angriffen schützen.

Aktuelle Betriebssysteme für mobile Endgeräte setzen diese Konzepte unterschiedlich um. Am Beispiel der bekannten Vertreter für mobile Endgeräte erkennt man, dass die genannten Konzepte mittlerweile in gewissem Umfang eingesetzt werden. Wie später noch zu sehen ist, bedeutet das leider aber nicht, dass man damit ein sicheres Gesamtsystem in den Händen hält.

### SymbianOS

SymbianOS, ehemals EPOC, ist für den Betrieb als Einbenutzersystem ausgelegt und setzt ein präemptives Multitasking zur Verwaltung der Rechenzeit ein. Es besitzt eine virtuelle Speicherverwaltung und damit effektiven Speicherschutz zwischen den Prozessen. Neue Versionen von SymbianOS bieten Capability basierten Zugriffsschutz für die Prozesse, die jeden Zugriff der Prozesse auf Daten kontrollieren können. Im Dateisystem besitzen Prozesse eigene private Verzeichnisse, die nur der jeweilige Prozess selbst benutzen kann. SymbianOS enthält sowohl eine Kryptografie-Biblitohek, als auch Mechanismen zum Zertifikatsmanagement. Diese beiden Komponenten werden bei der Softwareinstallation und für abgesicherte Kommunikation verwendet. Zur Erweiterung besitzt das System C++ und Java Programmierschnittstellen. Technische Informationen zu SymbianOS gibt [SYM].

### Windows Mobile

Windows Mobile besitzt Speicherschutz durch virtuelle Speicherverwaltung und präemptives Multitasking. Die integrierten Dateisysteme unterscheiden zwischen Benutzer- und geschützten Systemdateien, wobei letztere nur vom Betriebssystem geändert werden können. Zu den eingebauten können auch Dateisysteme von Drittherstellern eingesetzt werden, die zusätzliche Schutzmaßnahmen bieten können. Windows Mobile enthält Kryptografie- und Zertifikatsmechanismen. Zudem werden unterschiedliche Authentisierungsmechanismen zur Verfügung gestellt. Sowohl betriebssystemnahe Treiber, als auch Anwendungen können mittels komfortabler Entwicklungsumgebungen erstellt werden. Die Programme und jeweiligen APIs unterscheiden sich teilweise von bekannten PC-Betriebssystemen. Weitere technische Informationen findet man unter [MS-GEN] und [MS-API].

### PalmOS

Hatten die ersten Generationen der auf PalmOS basierenden Geräte noch keinen wirkungsvollen Speicherschutz, besitzen heutige Vertreter sowohl einfache virtuelle Speicherverwaltung als auch Multitaskingeigenschaften. Neben Kryptoalgorithmen werden auch Zertifikats- und Authentisierungsmanager integriert. PalmOS nutzt ein eigenes Konzept der Dateisystemorganisation und Speicherung persistenter Daten, das durch Software von Drittanbietern abgesichert werden kann. Es werden nur wenige Hardwareplattformen unterstützt. Weitere Details findet man unter [PALM].

**Linux**

Das Open Source Betriebssystem Linux existiert in unterschiedlichsten Ausprägungen auch für mobile Endgeräte. Technisch unterscheidet es sich nur sehr wenig von den Mechanismen und Schnittstellen gegenüber Linux auf großen Rechnern. Deshalb sind auch viele der anerkannten Linux-Sicherheitseigenschaften in den Ablegern in mobilen Endgeräten nutzbar. Linux bietet ein Speicherverwaltungskonzept und eine Multitasking-Prozessverwaltung. Der Betrieb ist im Gegensatz zu den anderen vorgestellten Betriebssystemen nicht auf einen Benutzer beschränkt, es können dagegen mehrere Vertrauensbereiche für verschiedene Benutzer und Benutzerprofile geschaffen werden. Zudem stehen verschiedene Dateisysteme mit Zugriffsschutz zur Verfügung, Kryptografie wird sowohl vom Betriebsystemkern als auch von Anwendungsbibliotheken angeboten, Authentisierungsmechanismen und Zertifikatverwaltung existieren ebenso. Zur Erweiterbarkeit muss man auf die Verfügbarkeit des Quelltextes und die Möglichkeit und dem Recht zu dessen Änderung hinweisen. Für den professionellen Einsatz bedeutet dies auch, dass man wegen der Quellcodeoffenheit des Systems nicht nur auf Aussagen des Herstellers angewiesen ist, sondern die Sicherheitsmechanismen direkt überprüfen könnte. In der Praxis sind allerdings nur wenige Geräte verfügbar und die Zahl der Anwendungen ist stark eingeschränkt. Einen aktuellen Überblick über Linux-basierte mobile Endgeräte findet man beispielsweise unter [LIN].

**RIM**

Die erste Generation der RIM-Geräte (Research in Motion) basierte auf Intel x86 Prozessoren, ohne den Einsatz (bekannter oder dokumentierter) Speicherschutzmaßnahmen. Heutige Geräte besitzen ein echtzeitfähiges Betriebssystem. Persistenter Speicher wird durch eine einfache Datenbank-ähnliche API den Anwendungen zur Verfügung gestellt. Kryptografische Mechanismen sind integriert, nach zugänglichen Dokumentationen können diese Schnittstellen nur durch Java Anwendungen genutzt werden. Besondere Eigenschaft dieser Geräte ist die zentrale Vergabemöglichkeit von Sicherheitspolicies, die durch die Geräte umgesetzt werden. Dazu zählen beispielsweise Regeln für den Einsatz von Benutzerpasswörtern oder eine Verschlüsselung des Gerätespeichers. Zusätzliche Informationen liefert die Webseite des Herstellers über Programmierschnittstellen [BB-API] als auch über die Sicherheitsarchitektur [BB-SEC].

### 1.1.4 Kommunikationssysteme

Mobile Endgeräte besitzen meist mehrere Kommunikationssysteme, durch die sie Daten mit der Außenwelt austauschen können und damit dem Benutzer unterschiedliche Möglichkeiten zur Kommunikation bieten. Neben GSM und UMTS für die Mobiltelefonie werden auch drahtlose lokale Netze wie WLAN, Bluetooth oder IrDA angeboten. Zusätzlich zu diesen drahtlosen Standards sind stets leitergebundene Kommunikationsverfahren integriert, die für die Datensynchronisation, Softwareinstallation und den Servicebetrieb verwendet werden. Alle diese Kommunikationssysteme lassen sich klassifizieren, wie in Abbildung 2: Kommunikationssysteme zu sehen ist.

Diese Kommunikationssysteme sind in der Regel fest in die mobilen Endgeräte integriert, die zur Steuerung nötige Betriebssoftware dazu ist im Betriebssystem eingebaut. Für WLAN und Bluetooth Kommunikation gilt, dass diese integrierten Sicherheitsmechanismen enthalten. Einerseits ist diese Absicherung teilweise leicht zu umgehen, wie diverse Schwachstellen und Angriffe auf WLAN-Architekturen beweisen. Andererseits nutzen diese Sicherheitsmechanismen diverse kryptografische Verfahren, deren nötiges Schlüsselmaterial unter der Verwaltung des Betriebssystems steht. Der Grad der Sicherheit dieser Kommunikationssysteme hängt deshalb hochgradig von der Sicherheit des Betriebsystems ab.

Anders stellt sich die Situation bei GSM-Systemen dar. Hier werden die Kryptomechanismen und die verwendeten Schlüssel in einer sogenannten SIM-Karte gehalten. Diese wird nur über spezielle Schnittstellen angesprochen und gibt sicherheitskritische Daten nicht nach außen. Trotzdem bedeutet die Kompromittierung des Betriebssystems auch dabei, dass die Kommunikation abgehört und

verfälscht werden kann, da die Daten, die gesendet oder empfangen werden, stets durch die Schnittstellen des Betriebsystems geleitet werden.

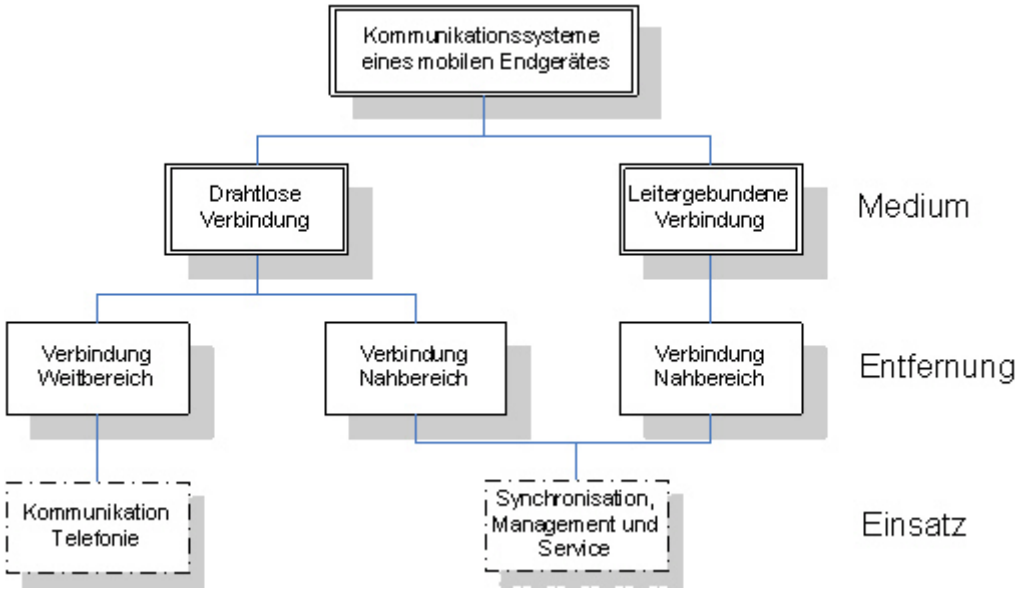



**Abbildung 2: Kommunikationssysteme**

Kommunikationssysteme wie GSM oder UMTS für den Weitbereich besitzen noch eine weitere sicherheitsrelevante Eigenschaft. Sie benötigen im Gegensatz zu WLAN oder Bluetooth eine komplexe Kommunikationsinfrastruktur, die meist von sogenannten Providern zur Verfügung gestellt wird. Dem Dienst des Providers muss der Anwender des mobilen Endgerätes vertrauen, da auf dem Kommunikationsweg Daten sowohl verändert, als auch abgehört werden könnten.

Viele mobile Endgeräte lassen sich zudem über Erweiterungssteckplätze wie CF-Card-Slots oder SDIO-fähige SD-Card-Slots um weitere Funktionen einschließlich zusätzlicher Kommunikationsschnittstellen erweitern.

Zur Datensynchronisation mit anderen Geräten werden meist sowohl leitergebundene, als auch drahtlose Verbindungen angeboten. Auf der Gegenseite, meist ein normaler PC, muss dazu eine spezielle, zum Betriebssystem des mobilen Endgerätes passende Software installiert werden. Damit lassen sich dann die Daten mit dem stationären Rechner abgleichen. Zudem kann auf diesem Weg auch zusätzliche Software auf dem mobilen Endgerät installiert werden.

Neben den für den Endbenutzer wichtigen Kommunikationswegen existieren zudem oft Schnittstellen, die für den Händler und den Service der Provider zur Verfügung stehen. Diese Kommunikationsschnittstellen sollen beispielsweise im Fehlerfall eine Reparatur ohne Öffen des Gerätes ermöglichen. Auch wenn diese Schnittstellen meist nicht öffentlich dokumentiert sind, können Angreifer trotzdem Werkzeuge besitzen, sie zu nutzen.

So wichtig und reizvoll alle diese Kommunikationswege zu den mobilen Endgeräten hin auch sind, diese Wege stehen auch potentiellen Angreifern zur Verfügung. Die Absicherung aller dieser leitergebundenen und drahtlosen Schnittstellen ist ein wesentlicher Schritt zur Erhöhung der Sicherheit mobiler Endgeräte. Zu diesem Thema existieren bereits einige Dokumente des BSI [BSI-DL], [BSI-GSM].

### 1.1.5 Integrierte Sicherheitsmechanismen

Heutige mobile Endgeräte besitzen bereits einige implementierte Sicherheitsmechanismen. Beispielhaft seien folgende genannt:

- Zur **Authentisierung** bieten die Endgeräte Kennwortabfragen oder biometrische Verfahren wie Fingerabdruckleser an.

- Diese Verfahren können beim Neustart des Gerätes, bei der Nutzung bestimmter Anwendungen oder nach einer bestimmten Zeit eine Benutzerauthentisierung erzwingen und die Nutzer damit entweder zur allgemeinen Nutzung des Gerätes oder für bestimmte Funktionalitäten **autorisieren.**
- Die oft in mobilen Endgeräten eingesetzten SIM-Karten stellen durch ihre geschützte Bauart und den eingeschränkten Zugriff eine sichere Möglichkeit zur **vertraulichen** Speicherung persönlicher (z. B. Adressbuch) und kryptographischer (z. B. GSM-Zugangsdaten) Daten dar.

## 1.2 Technische Grundlagen mobiler Dienste und Protokolle

Zusätzlich zu den im Betriebssystem enthaltenen Diensten und Applikationen kann der Benutzer den Funktionsumfang seines mobilen Endgerätes nach seinen Bedürfnissen mit weiteren Applikationen und Diensten von Drittanbietern erweitern, die nachfolgend allgemein als Benutzer-Dienste bezeichnet werden sollen. Aus der Sicht der Nutzer kann generell unterschieden werden zwischen Onboard-Benutzer-Diensten (Ausführung des Dienstes auf dem Endgerät), Online-Benutzer-Diensten (Verbindung zu einem Server erforderlich), browserbasierten Benutzer-Diensten (Internet Browser mit Internetverbindung erforderlich) und (Mobilfunk-) kommunikationsbasierten Benutzer-Diensten (SMS/MMS Kommunikation erforderlich). Diese Benutzer-Dienste unterscheiden sich mithin hinsichtlich ihrer Realisierung auf dem mobilen Endgerät (Client) und der ggf. nötigen Kommunikation mit einem Server. Auch Hardwareerweiterungen können meist nur durch zusätzlich installierte Onboard-Dienste oder Erweiterung der vorhandenen Dienste dem Benutzer zur Verfügung gestellt werden.

### 1.2.1 Mobile Dienstarten und Dienste

Hat man vorrangig die mobilen Endgeräte im Blick, dann werden die Benutzer-Dienste häufig auch als mobile Dienste bezeichnet, da diese Dienste auf einem mobilen Endgerät genutzt werden. Diese mobilen Dienste können in folgende Arten eingeteilt werden:

- Personal Assistant

  Diese Dienste beinhalten Anwendungen zur persönlichen Lebensplanung und –organisation wie z. B. Adressbücher, Kalender, etc.

- Informationsspeicher

  In dieser Kategorie werden Dienste zusammengefasst, die vorwiegend zur abgesicherten und strukturierten Ablage von Informationen genutzt werden wie Office Dokumente, eBooks, oder Passwortmanager, etc.

- Informationsdienste

  Informationsdienste bieten aktuelle Informationen, die von zentralen Infrastrukturen bereitgestellt und aktualisiert werden wie Informationspushdienste über MMS/SMS, Webbrowser, Cell-broadcasts, etc.

- Kommunikationsdienste

  Dienste, die zur Kommunikation von Benutzern untereinander genutzt werden: SMS, MMS, E-Mail, Telefonie, VoIP, Instant Messaging, Push-E-Mail, etc.

- Multimedia

  Dienste, die zur Wiedergabe oder Aufzeichnung multimedialer Inhalte genutzt werden, wie MP3-Spieler, Videoplayer, Fotokamera, Radio, digitales Fernsehen (insbesondere DVB-H), etc.

- Datentransfer/Synchronisation

  Dienste, die zum Austausch oder Abgleich der Daten auf dem mobilen Endgerät mit einem anderen (ggf. mobilen) Endgerät, einem Arbeitsrechner oder einem Server genutzt werden, z. B. SyncML, ActiveSync, Object Push, OBEX, FTP und andere.

- Positionsbasierte Dienste

  Dienste, die geographische Positionsdaten nutzen, wie beispielsweise Navigationsdienste, Flottenmanagement und positionsbasierte Informationsdienste.

- Spiele

  Alle Dienste, die zur interaktiven Unterhaltung des Benutzers dienen.

- Bezahldienste

  Mobile Endgeräte können für verschiedene Formen des bargeldlosen Zahlungsverkehrs genutzt werden, z. B. über Mobilfunkrechnung.

- Spezialanwendungen

  Hierunter fallen alle weiteren Dienste wie beispielsweise Barcode Scanner, Gesundheitsanwendungen, Spezialanwendungen für Außendienstmitarbeiter, etc.

### 1.2.2 Realisierung mobiler Dienste

Die Benutzer-Dienste werden meist als Applikationen direkt auf dem mobilen Endgerät zur Ausführung gebracht (siehe Abbildung 3), greifen dann auf die Betriebssystem-APIs[1] zu und haben somit vollen Zugriff auf die Ressourcen und Funktionen des mobilen Endgeräts.

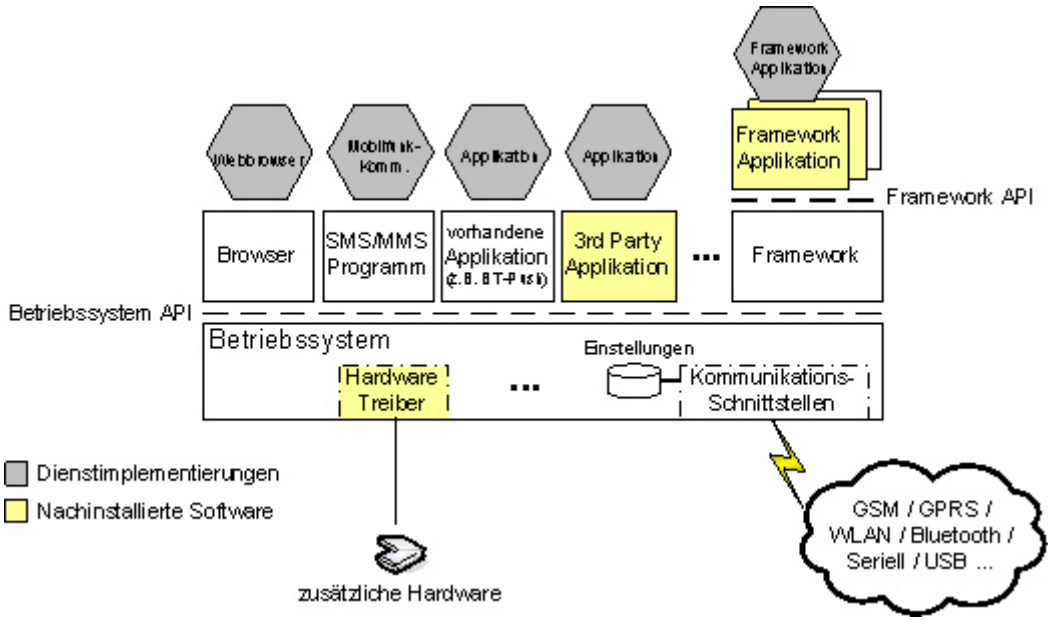



**Abbildung 3: Verschiedene Realisierungen von Benutzer-Diensten**

[1] API: Application Programming Interface

Deshalb sind Angriffe, welche durch eine Applikation ausgeführt werden (Viren, Trojaner, …) besonders schädlich. Durch das Signieren der Applikation wird die Echtheit des Applikations-Herstellers bei der Installation angezeigt und gewährleistet. Häufig werden Applikationen auf mobilen Endgeräten durch Einsatz von Frameworks (bzw. Middleware) realisiert, welche den Applikationsentwicklern eine weitere Abstraktion der Betriebssystem-API anbieten (z. B. NET Framework und Java). Mit der Ausführung in einem Sandbox-Framework wie J2ME können die Zugriffe auf das mobile Endgerät abhängig von den Java-Möglichkeiten (JSR Erweiterungen) und Einstellungen (z. B. Anwendung „darf Internetverbindung herstellen“) kontrolliert und unterbunden werden[2].

Alle Online-Benutzer-Dienste können zur Kommunikation mit dem Dienste Server auf Standard-Kommunikations-Protokolle und deren Sicherheitserweiterungen soweit im Betriebssystem vorhanden zurückgreifen. Darunter zählen unter anderem auch die Kommunikationsprotokolle HTTP und WAP mit deren Sicherheitserweiterungen HTTPS und WTLS zur Datenverschlüsselung.

Bei den (Mobilfunk-) kommunikationsbasierten Diensten greift das Betriebssystem auf die vorhandenen Schnittstellen zur Mobilfunkkommunikation über spezielle Programme und Schnittstellen zu. Dabei, wie auch bei den Online-Benutzer-Diensten, sind die Einstellungen besonders zu überprüfen (z. B. Internet-Verbindungs-Einstellungen, SMSC Einstellungen, etc.), um für die Verbindung nicht falsche Verbindungsendknoten zu adressieren.

Die Präsentation (z. B. über eine GUI) der Benutzer-Dienste erfolgt über betriebssystemabhängige Darstellungsmethoden, welche vom Entwickler über die Betriebssystem-API oder die Framework-API benutzt werden können, und ermöglicht somit freien Gestaltungsraum des Designs der Benutzungsschnittstelle. Die browserbasierten Benutzer-Dienste und (Mobilfunk-) kommunikationsbasierten Benutzer-Dienste werden in der Regel über die im mobilen Endgerät integrierten Webbrowser bzw. SMS/MMS Applikationen benutzt.

### 1.2.3 Integrierte Sicherheitsmechanismen

Mobile Dienste nutzen im Wesentlichen kryptografische Protokolle für folgende Sicherheitsmechanismen:

- Durch die **Authentisierung** wird die Identität des Benutzers gegenüber dem Dienst bzw. dem Dienstleister festgestellt. Für Kommunikationsdienste soll dadurch erreicht werden, dass die Nachricht authentisch ist und vom Absender nicht hinterher abgestritten werden kann.
- Die Kommunikation und die lokalen Daten auf dem mobilen Endgerät werden **verschlüsselt**, damit sollen wertvolle Daten beispielsweise bei Bezahldiensten vor Abhören und unbemerkter Veränderung geschützt werden.

Die zur Umsetzung dieser Verfahren nötigen Mechanismen werden heute von den Betriebssystemen bereitgestellt. Dabei bietet jedes der bekannten Betriebssysteme eine eigene Auswahl an kryptografischen und Authentisierungsverfahren an. Zudem sind die Schnittstellen zwischen den Kryptomechanismen und den Anwendungen bei jedem Betriebssystem unterschiedlich. Das führt bei den mobilen Diensten entweder dazu, dass nur wenige Systeme unterstützt werden können oder der Aufwand bei der Realisierung der mobilen Dienste hoch ist. Zudem besitzen zahlreiche der heutigen verfügbaren mobilen Dienste ganz eigene Implementierungen kryptografischer Algorithmen, was bei den geringen zur Verfügung stehenden Ressourcen der mobilen Endgeräte kontraproduktiv ist.

## 1.3 Zukünftige Entwicklung

Über die weitere Entwicklung mobiler Endgeräte lässt sich natürlich nur spekulieren. Allerdings hat die Entwicklung dieser Geräte bisher dieselben Entwicklungsstufen durchlebt, die man auch beim PC bis zurück zu den Großrechnern früher bereits erlebt hat. Die ersten mit den heutigen Rechnern

[2] J2ME unterstützt keine JNI (Java Native Interface)-Aufrufe ins Betriebssystem

vergleichbaren Computer, die Mainframes, wurden zunächst mit einfachsten Mitteln programmiert, besaßen keinerlei Möglichkeiten zur gleichzeitigen Ausführung von Programmen und ebenso keine Schutzmechanismen zwischen verschiedenen Prozessen. Später kamen virtueller Speicher, Multitasking und persistenter Speicher, wie Festplatten, dazu. Bei den Betriebssystemen wurden der virtuelle Speicher, Interprozesskommunikationsmechanismen und Mehrbenutzermodus später entwickelt, wie in Abbildung 4 zu sehen ist. Nach den Mainframes wurden die Minicomputer, die PCs mit ihren Mikroprozessoren und die Rechner für eingebettete Systeme entwickelt. Diese machten aller dieselben Entwicklungsstufen durch wie die Mainframes Jahre vorher. Diese Zyklen kann man auch bei der Entwicklung von mobilen Endgeräten erkennen. Konzepte wie virtueller Speicher oder Multitasking sind sowohl bei den PDAs und anderen mobilen Endgeräten vorhanden, als auch mittlerweile mit Smartcards möglich geworden. Prinzipiell sind bei den mobilen persönlichen Geräten auch größere Hintergrundspeicher vorhanden, diese allerdings bisher nicht in Form von mechanischen Scheiben der Festplatten, sondern in Form von Flash-Speichern. Allerdings gibt es seit kurzer Zeit Festplatten, die auch den mechanischen Anforderungen beim Einsatz in mobilen Endgeräten gewachsen sind und die jetzt beispielsweise auch in mobilen Endgeräten eingesetzt werden. Insgesamt war die Entwicklung der Betriebssysteme und die der übrigen Software aber getrieben bzw. gebremst durch die zur Verfügung stehende Technologie. Deshalb kann man davon ausgehen, dass die Entwicklung der Betriebssysteme für mobile Endgeräte mit der Entwicklung der Hardware und der Technologie weitergehen wird. Eine wichtige Entwicklung aus dem Bereich stationärer Systeme kann einen hohen Sicherheitsgewinn für mobile Endgeräte bedeuten, sobald sie in diesen Bereich gebracht wird, nämlich die Entwicklungen der Trusted Computing Group (TCG). Diese Erweiterung bestehender Hardware kann die Integrität eines mobilen Endgerätes weitgehend sicherstellen und so etwa bei Verlust und Wiederauffinden des Gerätes nötiges Vertrauen schaffen. Nähere Informationen über Trusted Computing findet man beispielsweise in [BSI-TP].

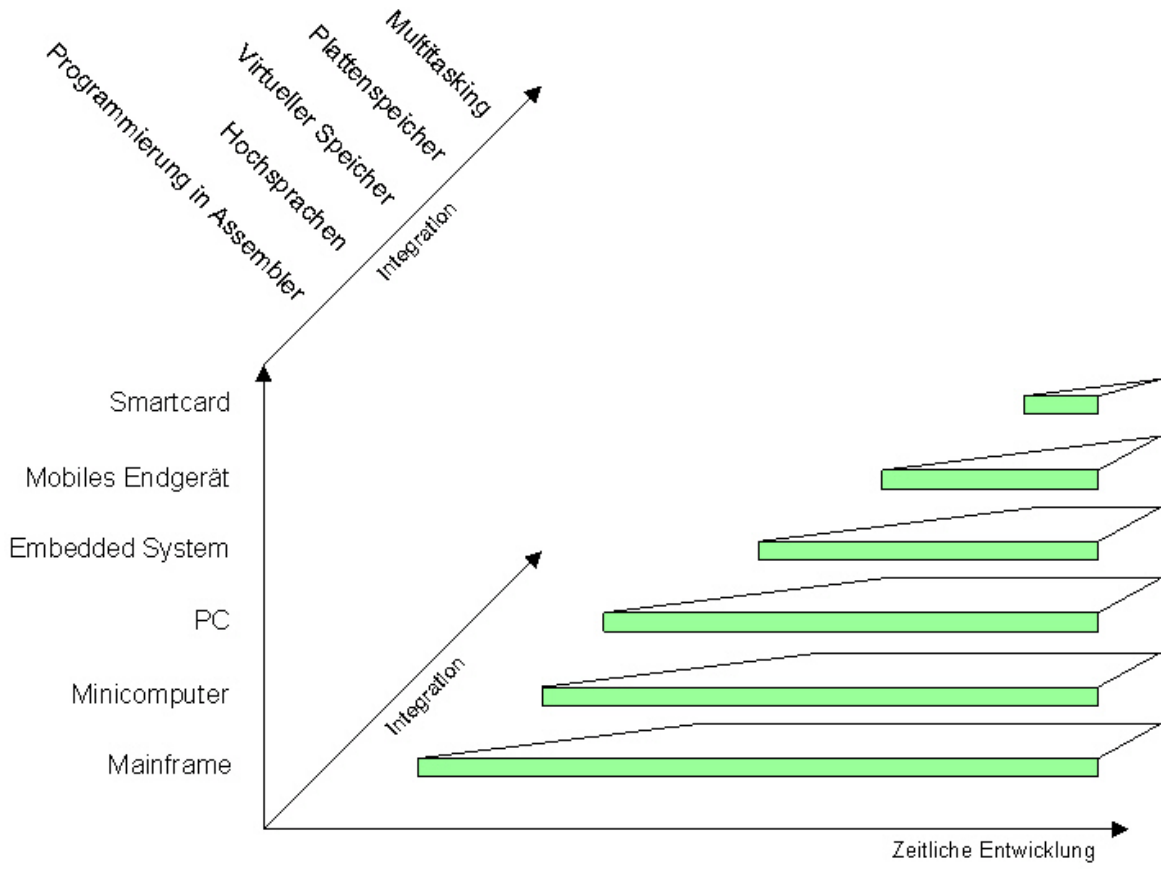



**Abbildung 4: Entwicklung der Integration**

**Entwicklung mobiler Endgeräte**

Die technische Entwicklung ermöglicht sowohl eine zunehmende Integration von Funktionalitäten und Schnittstellen in mobile Endgeräte als auch die Zusammenführung ursprünglich verschiedener Geräteklassen wie beispielsweise Mobiltelefon und PDA in ein einziges Gerät. Darüber hinaus werden die Geräte immer leistungsfähiger und der Grad der Vernetzung wächst sowohl quantitativ durch die Anzahl zur Verfügung stehender Kommunikationskanäle als auch qualitativ durch gesteigerte Übertragungsraten oder andere Übertragungsformen wie Ad Hoc Vernetzung.

Im Kommunikationsbereich werden die Teile, die heute in Hardware realisiert sind, zunehmend in Software realisiert werden. Die verantwortlichen Hersteller sehen darin vor allem die Flexibilität durch einfacheren Austausch der Software, als dies bei Hardwarekomponenten möglich ist. Als Beispiel lässt sich das so genannte Software Defined Radio (SDR) anführen, bei dem die Signalverarbeitung der Kommunikationshardware durch Software erledigt wird. Dieses an sich flexible Verfahren hat den Nachteil, dass auch Angreifer die entsprechende Software verändern und nutzen können, evtl. ohne dass der Nutzer das bemerken kann. Die Firmware aktueller Bluetooth-Chips setzt dieses Vorgehen teilweise bereits um und realisiert das Baseband und den Link Manager.

Eine wichtige Entwicklung wird aber auch in Zukunft darin bestehen, dass die mobilen Endgeräte sehr persönliche Hilfsmittel oder Assistenten für ihre Nutzer sein werden.

**Entwicklung mobiler Dienste**

Im Bereich der Dienste ist eine verstärkte Verbreitung von echten mobilen Diensten festzustellen, die sich, im Gegensatz zu klassischen Anwendungen, die von PCs auf mobile Endgeräte portiert wurden, der spezifischen Eigenschaften und Fähigkeiten der mobilen Endgeräte bedienen.

Hierbei prägen neue Benutzungsparadigmen wie „digital lifestyle“ oder „ubiquitous computing“ die Anforderungen an mobile Dienste. Bedienbarkeit und Kommunikationsfähigkeit spielen hierbei eine hervorgehobene Rolle. Der Wunsch nach aktuellen und ständig verfügbaren Informationen führt zum mobilen Internet und in vielen Fällen zur Verlagerung der Funktionalitäten.

**Entwicklung der Bedrohungslage**

Damit lassen sich zwei Entwicklungen folgern, die für die Entwicklung der Bedrohungslage wesentlich sind:

- Es ist abzusehen, dass ähnliche Angriffe, wie sie heute bei PCs und anderen Rechnern bekannt sind, in Zukunft in deutlich stärkerem Umfang auch bei mobilen Endgeräten auftreten werden. Monokulturen von Software und Hardware können diese Bedrohungslage drastisch verschärfen.
- Der Einsatzbereich eines mobilen Endgerätes reicht vom Arbeitsgerät hin zum persönlichen Lifestyleprodukt und es entstehen neue Anwendungsaspekte, wie Mobilität, langer Batteriebetrieb und neue Kommunikationstechnologien. Im Vergleich zu klassischen Rechnern entstehen durch die Veränderung der Benutzungsparadigmen und wegen neuer Anwendungsszenarien neuartige Bedrohungen.

# 2. Gefährdungen im mobilen Einsatz

Aus der Menge der vielfältigen Bedrohungen auf mobile Endgeräte sind für diese Broschüre im Wesentlichen diejenigen interessant, die die klassischen Schutzziele der Vertraulichkeit (engl. confidentiality), der Integrität (engl. integrity) und der Verfügbarkeit (engl. availability) betreffen.

## 2.1 Überblick und Strukturierung

Bei der Vielzahl der verfügbaren mobilen Endgeräte mit ihren mobilen Diensten und den jeweiligen Anwendungen existieren eine Menge potentieller Gefährdungen gegen diese Systeme. Zur Strukturierung lassen sich diese Bedrohungen wie in Abbildung 5 aufgezeigt einordnen.

Zunächst lässt sich jede potentielle Gefährdung danach unterscheiden, ob der Angreifer im Besitz des Gerätes ist, oder nicht. Hat er physikalischen Zugriff auf das Gerät, so kann er sowohl die darauf enthaltenen Daten stehlen, als auch das Gerät, oder er kann die darauf gespeicherten Daten oder die Software manipulieren. Es kommt hinzu, dass ein von einem Angreifer manipuliertes Gerät dem Besitzer wieder unbemerkt untergeschoben werden kann und dieser den Angriff nicht bemerkt. Der Angreifer muss deshalb nicht für die gesamte Dauer des Angriffs im Besitz des Gerätes sein, es genügen je nach Angriff nur einige Minuten.

Besitzt der Angreifer keinen physikalischen Zugang, so kann er Kommunikationswege nutzen, um das Gerät zu bedrohen und zu kompromittieren. Angriffe über Kommunikationskanäle können aktiv durchgeführt werden, diese beeinflussen den Datenverkehr direkt. Passive Angriffe dagegen werden nur durch Beobachtung und Abhören durchgeführt und sind nur sehr schwer zu entdecken.

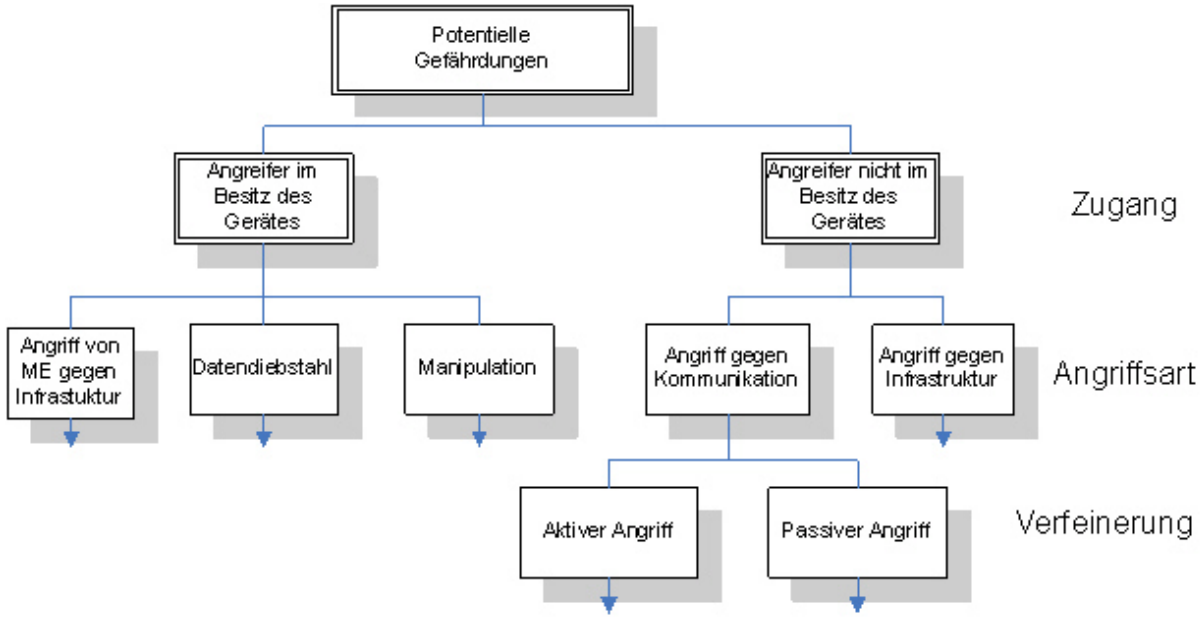
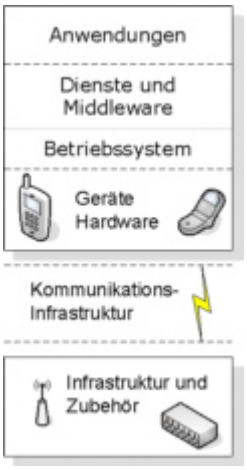



**Abbildung 5: Strukturierung möglicher Gefährdungen**




Neben den Angriffen auf die Kommunikation sind auch Angriffe auf die zusätzliche Infrastruktur möglich, die indirekt Auswirkungen auf die mobilen Endgeräte und deren gespeicherte Daten haben.

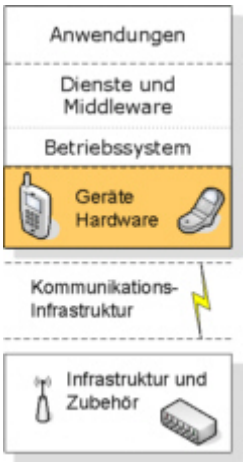
Die mobilen Endgeräte können nicht nur Ziel für Angriffe sein, sie können auch für Angriffe selber genutzt werden. Das mobile System wird damit zum Werkzeug des Angreifers, der dazu nicht zwangsweise auch im Besitz des Gerätes sein muss.

Neben dieser Einordnung der Gefährdungen werden die Komponenten des mobilen Endgeräts und dessen notwendige Infrastruktur nach nebenstehernder Abbildung unterteilt. Diese Unterteilung dient in den folgenden Abschnitten als Richtschnur für das Aufzeigen der Bedrohungspotentiale. Grob wird dabei zwischen Hardware und Software unterschieden. Der Softwareteil befindet sich auf dem mobilen Endgerät und beinhaltet das Betriebssystem und die Anwendungen. Daneben spielen Middleware-Architekturen eine größere Rolle, da sie die Komplexität der eingesetzten Kommunikationsarchitekturen vor den Anwendungen verbergen und so die Anwendungsentwicklung vereinfachen. Der Hardwareteil umfasst das mobile Endgerät und die gesamte zur Kommunikation notwendige Infrastruktur.

## 2.2 Bedrohungspotenziale

Die Absicherung der im mobilen Endgerät vorhandenen Teile, die potentielle Angriffsziele darstellen, ist wesentlich von der Sicherheit der darunter liegenden Komponenten abhängig. Das bedeutet, dass die Sicherheitsmechanismen der Anwendungen nur dann wirken können, wenn die Dienste nicht kompromittiert sind. Diese wiederum können einen abgesicherten Betrieb nur dann gewährleisten, wenn das Betriebssystem und schließlich die Gerätehardware nicht angegriffen worden ist. Umgekehrt bedeutet dies, dass ein erfolgreicher Angriff auf die Gerätehardware immer auch vollen Zugriff auf das Betriebsystem, die Dienste und Anwendungen bedeutet.

### 2.2.1 Angriffsziel: Gerätehardware und Zubehör




**Angreifer im Besitz des mobilen Gerätes**

- Hardware manipulieren und zerstören

  Bringt der Angreifer das Gerät in seinen Besitz, so hat er die volle Kontrolle über die Gerätehardware. Er kann das Gerät abschalten und das Gehäuse öffnen. Im Wesentlichen kann er dann ohne irgendwelche Kontrollen die Hardware manipulieren und zerstören. Der geräteinterne Speicher kann unter Umgehung aller Betriebssystemkontrollen ausgelesen und beschrieben werden. Neben Datendiebstahl können auf diese Weise weitere Anwendungen auf das Gerät gebracht werden. Diese zeichnen beispielsweise später Aktionen des Benutzers auf und geben sie an einen Angreifer weiter oder öffnen dem Angreifer eine Hintertür zum System.

- Gerätemerkmale ausspionieren

  Neben den auf dem Gerät gespeicherten Daten sind auch spezielle Merkmale der Gerätehardware für den Angreifer interessant. Oft werden die mobilen Endgeräte vom Benutzer oder dem Unternehmen durch Seriennummern, Beschriftungen oder Aufkleber identifiziert, die vom Angreifer kopiert und auf ein anderes baugleiches, bereits kompromittiertes Gerät aufgebracht werden. Der Anwender, der das Gerät später wieder erhält, kann das Gerät äußerlich nicht von seinem ehemaligen Gerät unterscheiden. Frühestens nach der Authentisierung könnte er aufgrund unterschiedlicher Gerätekonfiguration den Austausch bemerken. Allerdings ist zu diesem Zeitpunkt sein Passwort bereits eingegeben und dem Angreifer evtl. bekannt.

- Nutzungsspuren analysieren

  Viele Authentisierungsmechanismen basieren auf der Eingabe bestimmter Muster auf einem Touchscreen. Durch wiederholte Eingabe bleiben (physische) Spuren der Muster auf der Eingabefläche, die dem Angreifer Hinweise auf korrekte Muster oder Passworte geben können.

- Manipulation der Geräteausstattung

  Der Angreifer kann Zusatzhardware in das Gerät einbringen, wie etwa zusätzlichen Speicher oder zusätzliche Kommunikationshardware, die den Anwender später bei der Arbeit ausspionieren und die gesammelten Daten protokollieren und versenden.

- Nutzung durch Dritte/Fremde

  Durch die Benutzung eines mobilen Endgerätes durch mehrere Personen können sicherheitsrelevante Probleme entstehen. Heutige Geräte sind nicht für den Mehrbenutzerbetrieb ausgelegt, so dass sich die Nutzer Passwörter und Datenspeicher teilen müssen. Da keine getrennten Vertrauensbereiche auf den Geräten existieren, dürfen Geräteeinstellungen dann nur in Absprache miteinander vorgenommen werden. Die Installation von Software kann schädliche Programme (Spyware etc.) in das System einbringen und schädigt alle Benutzer des Systems.

- Wartungsarbeiten

  Auch bei Wartungs- und Reparaturarbeiten des mobilen Endgerätes außerhalb des eigenen Vertrauensbereiches (z. B. des Unternehmens) entstehen die oben genannten Probleme ebenso. Alle Gerätedaten können in kurzer Zeit verändert und gestohlen werden.

- Diebstahl

  Durch den Diebstahl eines mobilen Endgerätes sind alle Daten auf dem Gerät und in Zusatzspeichern, die nicht durch sehr spezielle Maßnahmen abgesichert wurden, in den Händen des neuen Besitzers.

- Hinterlegung bei Besuch

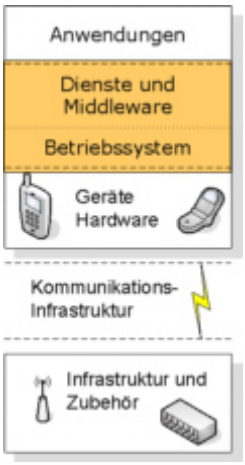
  Durch die Abgabe eines mobilen Endgerätes z. B. an der Pforte eines Unternehmens existieren dieselben Bedrohungspotentiale wie beim Verlust des Gerätes. Allerdings ist abhängig vom (technisch nicht beschreibbaren) Vertrauen das Risiko für einen Angriff wesentlich geringer.

**Angreifer nicht im Besitz des mobilen Gerätes**

Ist das mobile Endgerät nicht im Besitz des Angreifers, so kann er keine direkten Angriffe auf die Hardware durchführen. Denkbare Angriffe, wie etwa das Löschen des Speichers durch Schadsoftware (Malware) setzen einen Angriff auf das Betriebsystem oder die Anwendungen voraus und werden in den folgenden Abschnitten eingeordnet.

### 2.2.2 Angriffsziel: Betriebssystem und Dienste

**Angreifer im Besitz des mobilen Gerätes**




- Systemtest

  Durch konkrete Analysen eines mobilen Endgerätes kann der Angreifer Versionsstände und Art der eingesetzten Software auslesen. Dadurch lassen sich Rückschlüsse auf die Sicherheitspolicy des Unternehmens ziehen und zudem können mit Hilfe von Schwachstellenkatalogen konkrete wirkungsvolle Angriffe gefunden werden. Diese wirken dann nicht nur auf dem einzelnen analysierten Endgerät, sondern vermutlich auf allen Geräten mit gleicher Policy.

- Manipulation/Zerstörung

  Der Angreifer kann das Betriebssystem und alle Dienste des Gerätes beliebig manipulieren. Insbesondere die enthaltenen Sicherheitsmechanismen werden dadurch wirkungslos. Zusätzlich kann so die Funktionalität des Systems beeinträchtigt werden.

- Software-Schädlinge

  Es existieren zahlreiche Varianten von Software-Schädlingen für mobile Endgeräte, die unterschiedlichste Schäden anrichten. Der Angreifer kann sowohl verschiedene Viren, Würmer, und Trojaner in das System einbringen, als auch entsprechende Gegenmaßnahmen aushebeln.

- Ausspionieren des Passworts

  Das Erraten der Benutzerkennwörter kann durch einfaches Ausprobieren geschehen. Da der Angreifer das Gerät stets zurücksetzen kann, kann er das praktisch beliebig oft wiederholen. Zusätzlich kann er mit höherem Aufwand das Passwort im Klartext oder verschlüsselt aus dem Speicher des Gerätes auslesen. Eine weitere Gefahr ist das Einbringen von Spyware in das Betriebssystem, die das Passwort beim nächsten Anmeldeversuch des Benutzers aufzeichnet.

- Umgehung von Autorisationsprüfungen

  Der Angreifer kann mangelhaft implementierte oder unzureichend konfigurierte Zugriffskontrollen ausnutzen, um an gespeicherte Daten zu gelangen. Zudem kann der Angreifer die Daten

manipulieren. Er muss dazu meist nur wenig Systemwissen besitzen und kann den Angriff sofort durchführen.

**Angreifer nicht im Besitz des mobilen Gerätes**

- DoS

  Verschiedene Angriffe erlauben Denial-of-Service-Attacken gegen Systemdienste und Anwendungen. So ist es beispielsweise bei verschiedenen Implementierungen des Bluetooth Stacks auf verschiedenen Mobiltelefonen möglich, durch speziell formatierte Bluetooth Pakete das Gerät zum Absturz zu bringen. Eine wichtige Folge für das Opfer ist, dass es dann keine Anrufe mehr erhält und sich erneut am Gerät anmelden muss.

- Pufferüberlauf

  Über fehlerhafte Netzwerkprotokolle kann ein Angreifer so genannte Pufferüberläufe provozieren. Dabei werden vom Angreifer bewusst unzulässige Eingaben getätigt, die spezielle Seiteneffekte auslösen können. Je nach Endgerät können Überläufe sowohl auf dem Heap (auch Halde genannt) als auch auf dem Stack (auch Keller genannt) ausgenutzt werden.

- Ausführung von nicht vertrauenswürdigem Code

  Da einige mobile Endgeräte keine getrennten Vertrauensbereiche für Systemsoftware, Anwendungen des Benutzers und fremden Code besitzen, birgt das Ausführen von nicht vertrauenswürdigem Code besondere Gefahren. In diesen Systemen besitzt der fremde Code dieselben Rechte wie vertrauenswürdige Programme und kann demnach ebenso auf die Benutzerdaten zugreifen. Als vertrauenswürdig wird beispielsweise der Programmcode des Herstellers bezeichnet, hingegen ist jede Anwendung, die z. B. von unbekannten Seiten aus dem Internet herunter geladen wurde, nicht vertrauenswürdig.

- Umgehen der Authentisierung

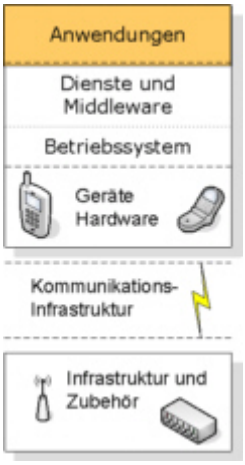
  Kann der Angreifer den Netzwerkverkehr zwischen dem mobilen Endgerät und der Infrastruktur abhören und beeinflussen, so kann er Passworte für Netzwerkdienste und Ressourcen durch Angriffe wie Sniffing, Brute Force, Wörterbuch- und Replay-Attacken herausfinden und umgehen.

- Übernahme bestehender Sessions

  Kommunikationsprotokolle können durch Replay- und Man-in-the-middle-Attacken verletzbar sein, wodurch der Datenaustausch vom Angreifer abgehört und kontrolliert werden kann.

- Kryptografie

  Die kryptografischen Verfahren, die zur Kommunikation eingesetzt werden, können durch Brute Force Attacken oder das Ausnutzen bekannter Schwachstellen in Verschlüsselung und Authentisierung umgangen werden.




### 2.2.3 Angriffsziel: Anwendungen

**Angreifer im Besitz des mobilen Gerätes**

- Umgehung von Authentisierungsprüfungen

  Wenn der Angreifer im Besitz des Gerätes ist, können Authentisierungsmechanismen, die in den Anwendungen durchgeführt werden, ebenso umgangen werden, wie die Prüfungen im Betriebssystem. Das zu vergleichende Schlüsselmaterial befindet sich schließlich im Gerätespeicher, den der Angreifer unter seiner Kontrolle hat.

- Ausnutzung von Programmierfehlern

  Durch die Kenntnis konkreter Programmfehler kann der Angreifer beispielsweise mittels spezieller Eingaben oder Programmparameter Sicherheitsmechanismen von Anwendungen überlisten. Dazu zählen sowohl die Umgehung der Autorisierungsprüfungen innerhalb der Anwendung, als auch das unautorisierte Starten weiterer Kommandos über die Anwendungsgrenzen hinaus.

- Änderung von Logging- und Accountingdaten

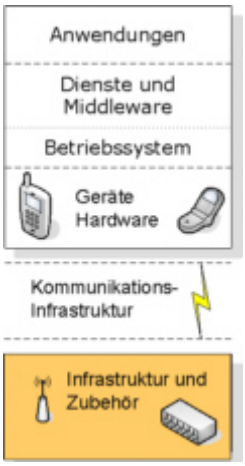
  Protokollierungsdaten, die beispielsweise Angriffsspuren beinhalten, können vom Angreifer geändert oder vernichtet werden. Dadurch wird sowohl der eigentliche Angriff bzw. Angriffsversuch, als auch die Angriffsmethodik verwischt.

**Angreifer nicht im Besitz des mobilen Gerätes**

Hier gelten dieselben potentiellen Bedrohungen, denen auch die Dienste und die Middleware ausgesetzt sind.

### 2.2.4 Angriffsziel: Infrastruktur

**Angreifer im Besitz des mobilen Gerätes**




Ein Sonderfall ist die Benutzung eines mobilen Endgeräts zum Angriff auf Infrastrukturen und Einrichtungen. Ein Angreifer, der im Besitz eines mobilen Gerätes ist, kann dieses als Angriffsmittel missbrauchen. Einige Angriffe lassen sich zudem auch mit fremden, der Umgebung nicht vertrauten Geräten durchführen.

- Einschleusung von Schadsoftware

  Durch mobile Geräte als Träger von Schadsoftware können in manchen Fällen bestehende Sicherheitskonzepte umgangen werden.

- Einsatz manipulierter oder fremder mobiler Geräte

  Durch den Einsatz manipulierter und fremder Geräte in einem vertraulichen Bereich kann ein Angreifer versuchen, Unternehmensressourcen unautorisiert zu verwenden.

- Denial of Service

  Der normale Betrieb kann dadurch gestört werden, dass ein Gerät innerhalb eines geschützten Bereiches als Quellknoten für Angriffe fungiert und damit wirkungsvolle Gegenmaßnahmen erschwert.

- Diebstahl vertraulicher Informationen

  Das in vielen Fällen erhöhte Vertrauensniveau von integrierten Geräten und Benutzern kann missbraucht werden, um Zugang zu Informationen zu erlangen.

- Unerlaubte Dienstnutzung

  Durch physische Kontrolle eines Gerätes lassen sich in vielen Fällen Sicherheitsmechanismen aushebeln, die Service- oder Contentprovider vor einem unbefugten Zugang zu bestimmten Onlinediensten oder vor der Verbreitung geschützter digitaler Inhalte schützen sollen.

- Illegaler Datentransport großer Datenmengen

  Die beiden zuletzt genannten Punkte werden noch verstärkt durch den Typ des eingesetzten Gerätes.
  Aktuelle mobile Endgeräte, insbesondere multimediafähige Geräte wie MP3-Spieler mit Video-

funktionen, besitzen extrem große Datenspeicher (100 GByte). Da diese Geräte über Datenverbindungen mit hohen Bandbreiten (USB bis 480 MBit/s) angeschlossen werden können, ist Datendiebstahl sehr großer Datenmengen möglich.

- Rechtemissbrauch

  Der Benutzer und das mobile Endgerät besitzen innerhalb der Unternehmensinfrastrukturen gewisse Rechte. Gehen diese über die für seine Arbeit notwendigen Rechte hinaus, so kann der Benutzer diese ausnutzen. Beispiele sind der Zugriff auf verschiedene Unternehmensressourcen oder das Benutzen spezieller Infrastruktur. Als Ursachen gelten fehlerhafte Administration und Mängel der Produkte, so dass die Rechte nicht genau genug festgelegt werden können.

**Angreifer nicht im Besitz des mobilen Gerätes**

Durch Angriffe auf die Infrastruktur, die das mobile Endgerät zur Kommunikation und Datensynchronisation benötigt, kann ein Angreifer erheblichen Schaden verursachen.

- Manipulation

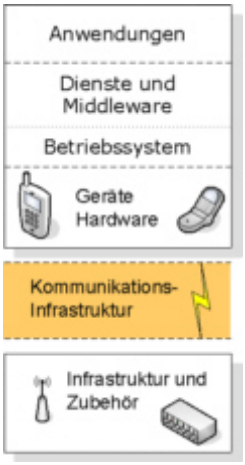
  Es existiert eine Vielzahl unterschiedlichster Angriffe auf Netzwerkkomponenten und Arbeitsplatzsysteme. Alle diese Geräte können für eine funktionierende Infrastruktur eines mobilen Endgerätes notwendig sein. Netzwerkkomponenten ermöglichen eine Verbindung zwischen dem mobilen Endgerät und der Gegenstelle zur Synchronisation. Angreifer können durch einen Angriff sowohl Datenverkehr zwischen den Endgeräten abhören, als auch verändern und vortäuschen. Die reine Beobachtung (passiver Angriff) von Kommunikation zwischen den Geräten stellt für den Angreifer unter Umständen auch schon einen wichtigen Informationsgewinn dar.
  Zudem kann der Angreifer den Arbeitsplatzrechner in seine Kontrolle bringen, der die Daten mit dem mobilen Endgerät synchronisiert. Der Angreifer erhält dadurch sofort den Datenbestand der letzten Synchronisation, ohne dass das mobile Endgerät vorhanden sein muss und außerdem kann er so bösartige Software übertragen lassen.

- Diebstahl

  Durch Diebstahl der Synchronisationsgegenstelle gelangt der Angreifer in den Besitz des Datensatzes der letzten Synchronisation mit dem mobilen Endgerät.

### 2.2.5 Angriffsziel: Kommunikation

**Angreifer nicht im Besitz des mobilen Gerätes**




Aktive Angriffe: Manipulation der Kommunikation

- Angriff bei der Synchronisation

  Zur Synchronisation des mobilen Endgerätes mit einer Arbeitsplatzstation wird Kommunikation über eine Kabelverbindung oder eine Funkschnittstelle aufgebaut. Synchronisation über ein Kabel kann durch kompromittierte Infrastruktur gefährdet sein. Zur Funkübertragung müssen die entsprechenden Funkschnittstellen im mobilen Endgerät eingeschaltet werden. Beispielsweise sind bei Bluetooth-Implementierungen in mobilen Geräten zahlreiche Angriffe bekannt, die je nach Gerät nur eine eingeschaltete Bluetoothschnittstelle voraussetzen [BSI-DL].

- Missbrauch des Servicebusses

  Die meisten mobilen Endgeräte besitzen Mechanismen, durch die der Hersteller Betriebssoftware auf dem Gerät ändern, updaten und installieren kann. Neben Geräten, die dafür spezielle Kabel und Hardware benötigen, gibt es auch Geräte, die diesen Vorgang über das

mitgelieferte Synchronisationskabel erlauben. Ein Angreifer kann durch Kontrolle der Arbeitsplatzstation deshalb während der Synchronisation gezielt auf die Firmware des Gerätes Einfluss nehmen und diese verändern.

- Spoofing Angriffe

  Durch die Vortäuschung falscher Identitäten kann ein Angreifer sich als Quelle für Schadsoftware oder vermeintlich vertrauenswürdige Gegenstelle zur Synchronisation ausgeben.
  Das Verbergen seiner wahren Identität kann ein Angreifer in vertrauenswürdigen Umgebungen dazu ausnutzen, dass er Ressourcen des Unternehmens unautorisiert benutzt.

- Man-in-the-middle

  Über bekannte Man-in-the-middle-Attacken kann sich ein Angreifer in neue bzw. bestehende Kommunikationsverbindungen einschleichen und sich als Kommunikationspartner ausgeben. Dies kann sowohl bei Synchronisationsverbindungen, als auch bei der normalen Dienstnutzung geschehen.

- DoS / Distributed DoS

  Durch Denial-of-Service-Attacken kann ein Angreifer die Dienstnutzung für berechtigte Benutzer verhindern. DoS Angriffe sind je nach Gerät auf verschiedene Netzwerkprotokolle und Kommunikationshardware über Funkverbindungen möglich und können hinterher kaum nachgewiesen werden.

- IP-orientierte Angriffe

  Da die mobilen Endgeräte als Kommunikationsprotokoll oft das TCP/IP Protokoll verwenden, sind viele bekannte Angriffe auf diese Protokollfamilie möglich. Diese Attacken sind auch auf Desktop- und Serversystemen mit anderen Betriebssystemen möglich. Dazu zählen unter anderem Angriffe auf ICMP, ARP (eigentlich nicht klassisch IP), UDP/TCP und die höheren Protokolle wie DNS und HTTP.

- Angriffe basierend auf Schwachstellen der Kommunikationsverfahren

  Auf drahtlose Netzwerke ist eine Reihe von wirkungsvollen Angriffen möglich. Beispielhaft sollen hier nur die relativ schwache WLAN-Sicherheitsarchitektur und Implementierung und die Menge bekannter Bluetooth-Attacken, Angriffe auf OBEX oder schwache PIN genannt werden (siehe [BSI-DL], [BSI-WL]).

Passive Angriffe: Beobachtung der Kommunikation

- Sniffing Angriffe

  Die Aufzeichnung von Kommunikationsbeziehungen erfolgt durch passives Abhören von Verbindungen. Der Kommunikationskanal kann dazu auch stark verschlüsselt sein, solange die Verbindungsdaten (z. B. Quell- und Zieladressangaben) unverschlüsselt sind, ist eine Entschlüsselung der Nutzdaten für diesen Angriff nicht nötig. Alleine die Erkenntnis des Angreifers, wer mit wem kommuniziert, ist bereits ein (teils sehr mächtiger) Angriff.

- Bewegungsprofile aufzeichnen

  Ein mobiles Endgerät mit integrierten aktiven Kommunikationsschnittstellen wie Bluetooth oder WLAN Modulen besitzt für die entsprechenden Protokolle eindeutige Adressen, die durch die Hardware festgelegt sind. Das Gerät, und damit auch der Benutzer, kann so eindeutig identifiziert werden. Bestimmte Konfigurationen der Kommunikationsgeräte erlauben anderen Geräten in Funkreichweite, diese Adressen gezielt abzufragen und zu sammeln. Da die Reichweite dieser Funktechniken zwischen 1 und 100 Meter liegt, kann man in diesem Rahmen Bewegungsprofile aufzeichnen. Zudem kann durchgeführte Kommunikation eindeutig einem Gerät (und damit auch dem Benutzer) zugeordnet werden.

- Gewinn nicht technischer Informationen

  Der Angreifer kann auf verschiedene Arten Informationen über die im Unternehmen eingesetzte Infrastruktur erhalten. Dazu zählen das Benutzen angebotener Dienste, persönliche Gespräche mit Mitarbeitern und die Beobachtung vor Ort. In Schwachstellenkatalogen kann er mit Hilfe dieser gewonnenen Fakten gezielt mögliche Angriffe auf die Infrastruktur suchen, eine Reihe von Angriffen vorbereiten und praktisch gleichzeitig durchführen.

## 2.3 Übergeordnete Bedrohungen

Neben den genannten existieren zusätzliche Bedrohungen, die sich nicht aus dem Architekturbild erkennen lassen, trotzdem aber bekannt und wichtig sind. Diese werden im Folgenden dargestellt.

### 2.3.1 Schadsoftware

Schadsoftware, also Software, die mit dem Ziel entwickelt wurde, Schaden anzurichten, lässt sich in folgende Kategorien einteilen:

- Viren

  Schadsoftware, die sich verbreitet, indem sie Kopien von sich selbst in Programme, Dokumente oder Datenträger schreibt.
  Beispiele sind Dust für die PocketPC Plattform oder Phage für Palm OS.

- Würmer

  Schadsoftware, ähnlich einem Virus, die sich selbst reproduziert und sich durch Ausnutzung der Kommunikationsschnittstellen verbreitet. Es existieren bereits verschiedene Varianten, die sich über MMS oder Bluetooth verbreiten.
  Beispiele sind Cabir oder Commwarrior für Symbian Series 60 Systeme.

- Trojanische Pferde

  Schadsoftware, bestehend aus einem (manchmal nur scheinbar) nützlichen Wirtsprogramm und einem versteckt arbeitenden, bösartigen Teil. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.
  Beispiele sind Cardblock und Pbstealer.A für Symbian Systeme.

- Backdoors

  Eine Backdoor ist ein üblicherweise durch Viren, Würmer oder Trojanische Pferde installiertes Programm, das Dritten einen unbefugten Zugang („Hintertür“) zum Computer verschafft, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen. Backdoors werden oft für Denial-of-Service-Angriffe benutzt.
  Ein Beispiel ist Brador für Windows Mobile 2003.

Schadsoftware ist üblicherweise für eine Betriebssystemvariante oder für einen bestimmten Mobilgerätetyp konzipiert. Zurzeit sind etwas über 100 verschiedene Schädlinge öffentlich bekannt und deren Anzahl steigt weiter. Es sind aber auch Schädlingsversionen denkbar, die auf einem höheren Abstraktionsniveau arbeiten, und systemübergreifend und damit unabhängig vom Betriebssystem und der Gerätehardware funktionieren.

### 2.3.2 Administrationskonzept analysieren und ausnutzen

Durch Falschmeldungen (ein so genannter Hoax) über versuchte Angriffe oder Attacken von Schadsoftware kann ein Angreifer das Vorgehen und die Sicherheitsstrategie der Systemadministration

analysieren und Schwachstellen darin suchen. Dabei ist insbesondere der Zeitraum zwischen bekannt werden und Abwehr der Bedrohungen interessant, aber auch die Prozesse bei der Einführung gezielter Abwehrmaßnahmen. Dabei muss der gemeldete Angriff nicht einmal möglich sein bzw. durchgeführt worden sein.

### 2.3.3 Beeinflussung des Update- und Konfigurationsmanagements

Da ein Großteil der Funktionalitäten mobiler Endgeräte durch Software realisiert wird, ist es der Wunsch von Anwender und Hersteller, sowohl die Firmware, das Betriebssystem, als auch Middleware, Anwendungen und entsprechende Konfigurationen aktualisieren zu können. Dies bedeutet, dass diese Softwareteile auch von Angreifern austauschbar sind. Außerdem ist es notwendig, dass der Benutzer oder die Administratoren der Geräte stets aktuelle, getestete Softwarestände auf den Geräten installieren, um Sicherheitspatches und neue Funktionen der Geräte bereitzustellen. In größeren Umgebungen müssen diese Vorgänge durch technische Lösungen oder durch festgelegte Prozesse unterstützt werden, was wiederum neue Sicherheitsprobleme aufwerfen kann.

### 2.3.4 Geschäftsbeeinflussung durch Negativimage

In einigen Fällen kann ein Angriff schon dann erfolgreich sein, wenn bei Nutzern bestimmter Dienste das Vertrauen in die Betreiber sinkt und diese entweder zu konkurrierenden Anbietern wechseln oder den Dienst nicht mehr in gleichem Maße nutzen. Der eigentliche Angriff muss dazu direkt keinen größeren Schaden verursachen.

### 2.3.5 Keine Trennung zwischen privatem und dienstlichem Einsatz

Im professionellen Umfeld muss zwischen den beiden Vertrauensbereichen privater und geschäftlicher Einsatz unterschieden werden. Der Anwender, der sein privates mobiles Endgerät in das Unternehmen mitbringt und einsetzt, kann auf diese Weise die bestehenden Sicherheitsmechanismen und das Gerätemanagement umgehen und eine Bedrohung darstellen. Zudem vermischt sich der private und geschäftliche Datenbestand aufgrund fehlender Vertrauensbereiche beispielsweise bei der Sicherung im Unternehmen.

Die Benutzung des geschäftlichen Gerätes zu Hause oder im Urlaub kann den Verlust der gespeicherten Unternehmensdaten bedeuten.

# 3. Schutzmaßnahmen

Die Schutzmaßnahmen lassen sich in Kategorien unterteilen, die in den folgenden Abschnitten beschrieben werden.

## 3.1 Prozess der Absicherung

Die Absicherung mobiler Endgeräte kann nur durch die Kombination verschiedener Sicherungsmaßnahmen stattfinden. Diese Maßnahmen finden sich im Lebenszyklus des Endgerätes wieder, der wie folgt eingeteilt wird:

1. Auswahl und Beschaffung der mobilen Endgeräte

   Bei der Auswahl müssen neben den funktionalen Anforderungen der Benutzer verschiedene Punkte beachtet werden. Das Gerät muss sich in die bestehende Unternehmenspolicy einbinden lassen, ohne dass große Änderungen nötig sind. Die integrierten Sicherheitsmechanismen des Gerätes und der Betriebssoftware müssen bei den geforderten Anwendungen entsprechenden Schutz bieten. Auf die Vertrauenswürdigkeit der Lieferanten und Hersteller ist zu achten. Insbesondere sollte die Herstellungskette vertraut sein, da bei modernen mobilen Endgeräten neben dem Hardwarehersteller auch Provider Software auf das Gerät aufbringen können.

2. Installation

   Die Erstinstallation der Geräte erfordert die Kennzeichnung der Geräte, so dass ein wieder gefundenes Gerät möglichst erkannt werden kann. Es ist zu prüfen, welche Anwendungen bereits auf dem Gerät vorinstalliert sind, insbesondere wenn neben dem Hardware- und Betriebssystemhersteller auch Provider Anwendungen installiert haben. Optional muss das Gerät mit zu der Unternehmenspolicy passenden Schutzmechanismen ausgestattet und in eine Verwaltungsinfrastruktur eingebunden werden. Neben der Geräteinstallation müssen auch die Anwender mit der Bedienung und der Funktion der Sicherheitsmechanismen vertraut gemacht werden.

3. Betrieb

   Während des Betriebs ist es nötig, die Software der Geräte mit Sicherheitsupdates zu versorgen. Dazu zählen sowohl die Firmware der Geräte, als auch das Betriebssystem mit seinen Treibern und alle Anwendungen. Das dafür zuständige Gerätemanagement muss außerdem melden, wenn nicht vertrauenswürdige Software auf einem mobilen Endgerät installiert worden ist. Weiterhin sollte der Anwender den Verlust seines mobilen Endgerätes melden, auch wenn er das Gerät kurze Zeit später wieder gefunden hat. Anschließend muss die Integrität des Gerätes von vertrauenswürdiger Stelle sichergestellt werden.

4. Außer Betrieb nehmen

   Nach dem Einsatz eines mobilen Endgerätes muss sichergestellt sein, dass die darauf gespeicherten Daten gelöscht bzw. unbrauchbar gemacht werden. Zudem muss sichergestellt werden, dass das Gerät anschließend keine geschützten Unternehmensressourcen mehr nutzen kann.

Zusätzlich ist es ratsam, Bedrohungs- und Risikoanalysen und Penetrationstests durchzuführen, um konkrete Schwachstellen der Infrastruktur und der eingesetzten Geräte zu finden.

Jede Art der Absicherung kann in eine der folgenden drei Phasen eingeteilt werden.

1. Präventiver Schutz

   Darunter fallen alle Maßnahmen, die im Vorhinein ohne konkreten Angriff zur Erhöhung der Sicherheit eingeführt werden. Dazu zählen z. B. Schulung der Mitarbeiter, eine Unternehmenspolicy, Installation von Verschlüsselungssoftware, etc.

2. Angriffserkennung

   Maßnahmen, die einen stattfindenden Angriff bemerken und melden, wirken als erkennende Maßnahmen. Dazu zählen das Gerätemanagement zur Meldung von Schwachstellen und versuchten Angriffen, die Anzeige verloren gegangener Geräte oder die Analyse von Logfiles.

3. Wiederherstellung und Reparatur eines kompromittierten Systems

   Nach erfolgtem Angriff eines Gerätes müssen ebenfalls Maßnahmen eingeleitet werden. Diese meist organisatorischen Maßnahmen stellen die Wirkung des Angriffs und erfolgte Schäden fest und beseitigen diese. Technische Maßnahmen zur Reaktion werden heute nur vereinzelt eingesetzt.

Jeder Angriff kann analog in die drei Bereiche Angriffsvorbereitung, Durchführung und dem Verwerten des Angriffes unterteilt werden. Eine wirkungsvolle Abwehrstrategie sollte Maßnahmen treffen, die gegen alle drei Angriffsphasen Schutz bietet.

Im Folgenden werden zunächst alle konkreten technischen oder organisatorischen Schutzmaßnahmen erläutert und die Auswahl anschließend an vier konkreten Einsatzszenarios gezeigt. Anschließend wird ein Leitfaden zur Entwicklung einer Sicherheitspolicy beschrieben.

## 3.2 Technische Absicherung mobiler Endgeräte

Kurzbezeichnung (MG)

Im folgenden Abschnitt werden mögliche technische Maßnahmen zur Absicherung der mobilen Endgeräte systematisch aufgezeigt.

### 3.2.1 Maßnahmen gegen potentielle Bedrohungen

Die technischen Schutzmaßnahmen lassen sich analog zu den potentiellen Bedrohungen gliedern, wie in Abbildung 6 dargestellt.

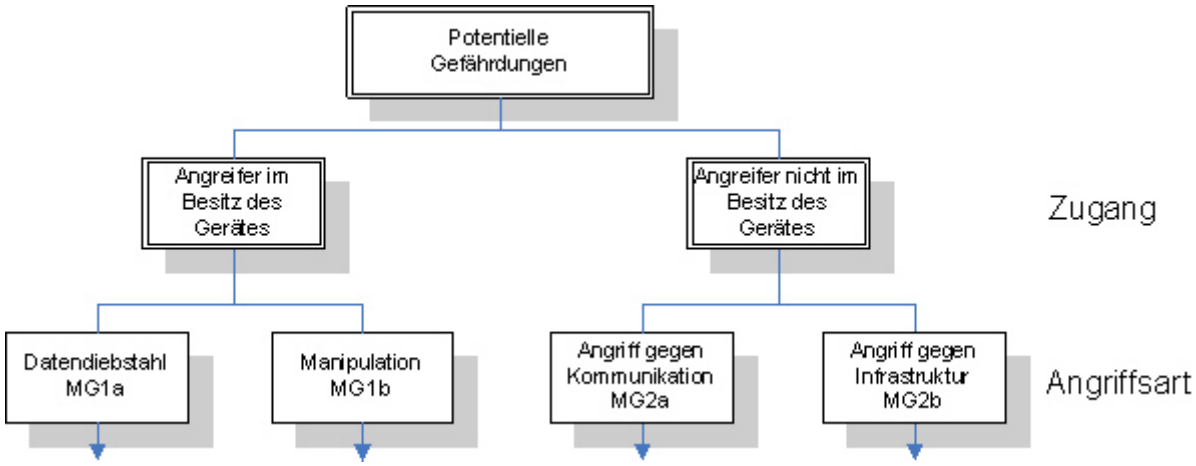



**Abbildung 6: Gegenmaßnahmen**

**Maßnahmen zum Schutz vor Datendiebstahl MG1a**

1. Schutz durch Verschlüsselung

   Durch Verschlüsselungsmechanismen werden die Speicherinhalte des mobilen Endgerätes vor unautorisierten Zugriffen geschützt. Auch der Verlust des Gerätes führt dann nicht unweigerlich zum Verlust der Datenvertraulichkeit. Allerdings muss geprüft werden, in wieweit die Verschlüsselung bei der regulären Benutzung abgeschaltet wird und wie diese Gegenmaßnahme nach gewisser Benutzerinaktivität wieder wirkt.

2. Schutz durch abgesicherten vertraulichen Speicher (SIM)

   Wichtige Daten können in speziellen abgesicherten Speichern abgelegt werden, die sowohl vor unautorisierten Zugriffen, als auch vor physikalischen Angriffen weitgehend geschützt sind. Zu diesen Speichern zählen die SIM Karte eines Mobiltelefons oder eine Chipkarte.

3. Maßnahmen zur Identifikation des persönlichen Endgerätes

   Obwohl es zahlreiche Mechanismen zur Authentisierung des Benutzers gegenüber dem Endgerät gibt, muss umgekehrt der Benutzer dem mobilen Endgerät bei der Authentisierung vertrauen. Es ist wünschenswert, dass Gerätemerkmale zur eindeutigen und möglichst unverfälschbaren Identifikation angebracht werden.

4. Benutzungsspuren entfernen

   Die Benutzungsspuren, die durch die häufige Eingabe des Passwortes oder der PIN auf dem Display an selber Stelle entstehen können, müssen vermieden und entfernt werden.

**Maßnahmen zum Schutz vor Gerätemanipulationen MG1b**

1. Geräteverlust bedeutet Vertrauensverlust

   Mit technischen Mitteln ist dem Verlust des Gerätes nicht beizukommen. Dabei werden nicht nur Vertraulichkeit und Integrität der gespeicherten Daten gefährdet, insbesondere ist ein wieder gefundenes Gerät nicht mehr vertrauenswürdig. Durch aufwändige technische Mittel muss ein kompromittiertes Gerät wieder bereinigt und in den Auslieferungszustand gebracht werden.

2. Schutz durch technische Integration

   Durch eine hohe Integration der Gerätehardware kann eine weitgehend geschützte, auch nach Verlust nicht veränderbare Hardware hergestellt werden. Beispiele dafür sind Chipkarten, die auch nach dem Auffinden (fast) nicht unautorisiert benutzt oder verändert werden können.

**Maßnahmen zum Schutz vor Angriffen auf die Kommunikation MG2a**

Ein wesentliches Mittel die Kommunikation mit mobilen Endgeräten zu schützen, ist eine abgesicherte Ende-zu-Ende-Kommunikation durch kryptografische Maßnahmen. Das Abhören vertraulicher Informationen wird für den Angreifer dadurch erheblich aufwändiger bzw. mit herkömmlichen Mitteln eines Angreifers vollständig verhindert.

1. Kommunikationssicherheit (Ende-zu-Ende-Verschlüsselung)

   Durch den Einsatz von Verschlüsselungstechniken muss die Kommunikation zwischen den Geräten abgesichert werden. Bereits eingeführte Schutzmaßnahmen im Unternehmen, die das Netzwerk betreffen, sollen auch für mobile Endgeräte eingeführt werden.

2. Kommunikationsschnittstellen bei Nichtbenutzung ausschalten

   Da alle Kommunikationsprotokolle potentielle Angriffsziele darstellen, dürfen Kommunikationsschnittstellen nur bei Bedarf vom Benutzer aktiviert werden.

3. Passworte prüfen

   In regelmäßigen Abständen kann geprüft werden, ob die Benutzerpassworte leicht zu erraten sind.

**Maßnahmen zum Schutz vor Angriffen auf die Infrastruktur MG2b**

1. Analyse der Logfiles

   Die regelmäßige Kontrolle der Logfiles soll durch Intrusion Detection Systeme durchgeführt werden.

2. Notwendige Geräteinfrastruktur absichern

   Neben den Schutzmaßnahmen in den mobilen Endgeräten sind auch herkömmliche technische Maßnahmen in der betreffenden IT-Infrastruktur zutreffen.

### 3.2.2 Gegenmaßnahmen durch Einsatz von Softwareprodukten

Kurzbezeichnung (MG3)

Auf dem Markt existiert eine Vielzahl von Softwareprodukten, die einen Teil der genannten Schutzmaßnahmen umsetzen können. Im Wesentlichen werden dazu folgende Funktionalitäten bereitgestellt, um die Sicherheit zu verbessern:

1. Virenschutz

   Diese Softwaregruppe verbessert den Schutz vor Schadsoftware durch aktive Überwachung der Kommunikation, automatisch oder manuell gestarteten Suchroutinen und Schädlingsentfernungsmechanismen. Einige Produkte bieten auch Schutz vor E-Mail und SMS-Spam.

2. Zugangskontrolle für Benutzer

   Die Zugangskontrolle bei mobilen Endgeräten ist bei Auslieferung oftmals nur unzureichend realisiert. Eine Vielzahl von teilweise kostenlosen Programmen bietet hierzu verschiedene Lösungsansätze, angefangen bei normalen Kennwortabfragen über graphische Lösungen bis hin zur Echtzeithandschrifterkennung auf berührungsempfindlichen Bildschirmen.

3. Kommunikationssicherheit

   Um die Kommunikation abzusichern existieren Umsetzungen bekannter Konzepte auf mobile Endgeräte, wie VPN-Lösungen, Browser mit SSL/TLS, SSH-Clients und Firewall-Implementierungen für lokalen Betrieb (so genannte Personal Firewalls).

4. Dateiverschlüsselung (PIN-Manager, E-Mail Verschlüsselung, Speicherkarten, RAM, ...)

   Zum Schutz lokal abgelegter vertraulicher Informationen wie persönlicher Daten, PINs, Kennwörter, etc. werden Verschlüsselungsprogramme eingesetzt, die entweder einzelne Dateien[3] oder ganz Dateisystem(-bereiche) verschlüsseln.
   Oft werden diese Programme mit Zugangskontrollen verknüpft, manche bieten auch die Option, bei mehrfacher Falschauthentisierung die vertraulichen Daten unwiederbringlich zu löschen. Bei normal üblicher Synchronisierung des Gerätes mit einem PC bedeutet dies keinen Datenverlust für den rechtmäßigen Nutzer.

5. Zugriffskontrolle für Hardwareerweiterungen

   Um das Bedrohungspotenzial von Hardwareerweiterungen einzuschränken, sind Betriebssystemerweiterungen oder –änderungen denkbar, die den Zugriff auf die Schnittstellen eines Gerätes wie beispielsweise Erweiterungsslots begrenzen. Konkret finden sich Programme, die SIM-Karten fest an bestimmte Endgeräte binden.

6. Zugriffskontrolle für Softwareerweiterungen

   Ein weiterer Schutzmechanismus ist die Etablierung eines Autorisierungssystems für die Installation von Softwareerweiterungen, wie beispielsweise bei dem JavaCard-Betriebssystem für Chipkarten.

7. Sicherheitsmanagement und Sicherheitspolicies

   Für den Einsatz in Unternehmen und Organisationen können Programme eingesetzt werden, die vorgegebene Sicherheitsrichtlinien auf mobilen Endgeräten durchsetzen. Es existieren hierzu Produkte, die die Umsetzung einfacher Policies und Schlüsselmanagement realisieren.
   Ein weiterer Punkt zum Sicherheitsmanagement, für die Produkte verfügbar sind, ist die zentrale Verwaltung von Sicherheitsprofilen und Benutzern. Manche Produkte sehen auch einen Mehrbenutzerbetrieb für die Geräte vor.

[3] Hierunter fallen auch E-Mail-Verschlüsselungsprogramme

### 3.2.3 Andere technische Maßnahmen

Kurzbezeichnung (MG4)

Andere technische Maßnahmen zur Erhöhung des physikalischen Schutzes der mobilen Endgeräte können sein:

1. Manipulationssichere Hardware, soweit technisch und organisatorisch möglich
2. Abschließbare Gehäuse
3. Diebstahlschutz, wie etwa eine Kette mit Schloss

Diese Schutzmaßnahmen verzögern zwar den erfolgreichen Angriff, kommt der Angreifer aber in den Besitz des Gerätes, können diese ihn nicht aufhalten.

## 3.3 Nutzung abgesicherter Protokolle

Kurzbezeichnung (MP)

Voraussetzung für den sinnvollen Einsatz abgesicherter Protokolle ist der Einsatz starker Passwörter, Schulung der Benutzer auch im Umgang mit Zertifikaten und der sorgfältige Umgang mit vertrauenswürdigem Schlüsselmaterial. Zusätzlich ist bei leitergebundener Kommunikation wichtig, dass die Synchronisation des mobilen Endgerätes nur mit vertrauenswürdigen Gegenstellen durchgeführt und das mobile Endgerät nicht an fremde Geräte angeschlossen wird. Einige dieser Maßnahmen wurden bereits in 3.2 konkret angesprochen, da abgesicherte Protokolle jedoch eine wesentliche Rolle zur Absicherung spielen, werden sie hier nochmals erwähnt.

## 3.4 Organisatorische Maßnahmen

Kurzbezeichnung (MO)

1. Softwareupdate

   Die Software des mobilen Endgerätes, sowie die Synchronisationssoftware auf den Desktops müssen auf dem neuesten Stand gehalten werden. Nur dadurch können entsprechende Sicherheitsprobleme vom Hersteller behoben werden.

2. Verhindern, dass Endgeräte unbeaufsichtigt sind
3. Vertrauliche Umgebungen schaffen

   Bei vertraulichen Besprechungen dürfen nur eigene bzw. geprüfte Geräte zugelassen werden. Je nach Einsatz kann beispielsweise geregelt werden, dass alle mobilen Endgeräte abgeschaltet werden. Dies kann z. B. dadurch durchgesetzt werden, dass alle Akkus eingesammelt werden oder mobile Endgeräte durch Detektoren aufgespürt werden.

4. Protokolle und Logfiles aller Geräte beobachten
5. Speicherkarten als Datenspeicher nutzen

   Wenn es die Gerätehardware und die Anwendungen zulassen, kann es sinnvoll sein, die schützenswerten Daten auf einem entfernbaren Datenträger im mobilen Endgerät abzulegen. Muss das Gerät beispielsweise beim Eingang in ein Unternehmen abgegeben werden, so können zumindest die wichtigen Daten aus dem Gerät entfernt werden.

## 3.5 Anwendungsszenarien

Der Einsatz der mobilen Endgeräte und entsprechender Dienste bringt je nach konkreter Anwendung in Abhängigkeit vom Schutzbedarf verschiedene Anforderungen an die Sicherheit mit sich. Diese ergeben sich vor allem aus den Kenntnissen über die potentiell wirkungsvollen Angriffe und Schwachstellen der Systeme. Sowohl die Gefahren, als auch die notwendigen Gegenmaßnahmen können durch die Betrachtung konkreter Szenarios dargestellt werden. Im Folgenden werden einige charakteristische Einsatzszenarios für mobile Dienste vorgestellt, die dieser Broschüre folgend später für die Umsetzung entsprechender Gegenmaßnahmen verwendet werden können. Die Auswahl erfolgt danach, dass ein möglichst breites Spektrum der Eigenschaften wie Schutzbedarf der Daten, Kommunikationshäufigkeit und Mobilitätsgrad ausgewählt wurde.

**Verschiedene typische Anwendungsszenarios**

***Szenario S1: Außendienstmitarbeiter (geschäftlich)***

Der Außendienstmitarbeiter greift über ein Kundennetzwerk mit seinem mobilen Endgerät auf Daten seines Unternehmens zurück. Dabei kann er zur Kommunikation auch nicht vertrauliche Infrastrukturen wie einen WLAN Access Point des Kunden verwenden. Er nutzt dazu sowohl Informations- als auch Kommunikationsdienste. Hier sind zum einen alle Daten des mobilen Endgerätes schützenswert, zum anderen muss der Außendienstmitarbeiter Sorge tragen, dass die Kommunikationsdaten geschützt werden.

***Szenario S2: Mobiltelefonierer (geschäftlich privat)***

Jemand nutzt sein Mobiltelefon sowohl für private, als auch für dienstliche Zwecke hauptsächlich für die Dienste der Sprachtelefonie, SMS/MMS und E-Mail. Das vom Benutzer geforderte Schutzniveau schwankt ebenso wie der Wert der Daten je nach Einsatz. Dabei sind nicht nur die Nutzdaten schützenswert, sondern auch die anfallenden Signalisierungsdaten und Kontextinformationen, wie z. B. der aktuelle Aufenthaltsort.

***Szenario S3: PDA-Offlinenutzung / Lifestylenutzer (privat)***

Ein Benutzer eines PDAs nutzt das Gerät im Wesentlichen zur Unterhaltung, dazu zählt Musik hören, Spiele, Multimedia Anwendungen und Informationsdienste offline nutzen. Nur für die Installation und Datensynchronisation wird vom mobilen Endgerät über USB oder eine kabellose Bluetooth-Verbindung vernetzt. Auf dem mobilen Endgerät befinden sich vor allem Daten mit langer Lebensdauer, wie etwa Adressbücher, Dokumente und Multimediadaten.

***Szenario S4: mCommerce (privat)***

Ein Anwender eines mobilen Endgerätes nutzt privat mCommerce-Dienste. Im Wesentlichen sind dies Bezahlfunktionalitäten, wie etwa Internetshopping, Bezahlen mit dem Handy oder elektronische (virtuelle) öffentliche Nahverkehrs-Ausweise. Wichtig ist dabei vor allem, dass der Bezahlvorgang vertraulich ist und nachvollziehbar funktioniert und der Kunde nur für erhaltene Leistungen bezahlt.

**Geeignete Schutzmaßnahmen**

Folgende Schutzmaßnahmen werden mindestens für die jeweiligen Einsätze empfohlen. Dabei werden nur die jeweils vordergründigen Gefahren mit den entsprechenden Gegenmaßnahmen aufgezählt. Entsprechende Erläuterungen zu den Gegenmaßnahmen findet man in den vorigen Abschnitten. Die Ziffern am Anfang der Zeilen benennen die jeweiligen Gegenmaßnahmen bezogen auf die obigen Listen dazu.

***Szenario S1: Außendienstmitarbeiter (geschäftlich)***

**MG1a: Schutzmaßnahmen gegen Datendiebstahl**

1,3: Schutz durch Verschlüsselung, Maßnahmen zur Identifikation des persönlichen Endgerätes

**MG1b: Schutzmaßnahmen gegen Gerätemanipulationen**

1,2: Geräteverlust bedeutet Vertrauensverlust, Schutz durch technische Integration

**MG2a: Schutzmaßnahmen gegen Angriffe auf die Kommunikation**

1,2,3: Kommunikationssicherheit, Kommunikationsprotokolle bei Nichtbenutzung ausschalten, Passworte prüfen

**MG2b: Schutzmaßnahmen gegen Angriffe auf die Infrastruktur**

1,2: Analyse der Logfiles, Notwendige Geräteinfrastruktur absichern

**MG3: Schutz durch Einsatz von Softwareprodukten**

1,2,3,4,7: Virenschutz, Zugangskontrolle für Benutzer, Kommunikationssicherheit, Dateiverschlüsselung, Sicherheitsmanagement einführen und nutzen

**MG4 / MP / MO: Andere Maßnahmen, abgesicherte Protokolle und organisatorische Maßnahmen**

1,2,3,4,5: Softwareupdate, ständiges Beaufsichtigen des Endgeräte, vertrauliche Umgebung schaffen, Logfiles analysieren, herausnehmbare Speicherkarten nutzen

***Szenario S2: Mobiltelefonierer (geschäftlich / privat)***

**MG1a: Schutzmaßnahmen gegen Datendiebstahl**

1,2,3: Schutz durch Verschlüsselung, Schutz durch abgesicherten vertraulichen Speicher, Maßnahmen zur Identifikation des persönlichen Endgerätes

**MG1b: Schutzmaßnahmen gegen Gerätemanipulationen**

1,2: Geräteverlust bedeutet Vertrauensverlust, Schutz durch technische Integration

**MG2a: Schutzmaßnahmen gegen Angriffe auf die Kommunikation**

1,2: Kommunikationssicherheit, Kommunikationsprotokolle bei Nichtbenutzung ausschalten

**MG2b: Schutzmaßnahmen gegen Angriffe auf die Infrastruktur**

Es ist für diese Analyse davon auszugehen, dass die Infrastruktur des Mobilfunkbetreibers nicht angegriffen werden kann.

**MG3: Schutz durch Einsatz von Softwareprodukten**

1,2,3,4,6,7: Virenschutz, Zugangskontrolle für Benutzer, Kommunikationssicherheit, Dateiverschlüsselung, Zugriffskontrolle für Softwareerweiterungen, Sicherheitsmanagement einführen und nutzen

**MG4 / MP / MO: Andere Maßnahmen, abgesicherte Protokolle und organisatorische Maßnahmen**

1,2,4,5: Softwareupdate, ständiges Beaufsichtigen des Endgeräte, Logfiles analysieren, herausnehmbare Speicherkarten nutzen

***Szenario S3: PDA-Offlinenutzung / Lifestylenutzer (privat)***

**MG1a: Schutzmaßnahmen gegen Datendiebstahl**

1,3,4: Schutz durch Verschlüsselung, Maßnahmen zur Identifikation des persönlichen Endgerätes, Benutzungsspuren entfernen

**MG2a: Schutzmaßnahmen gegen Angriffe auf die Kommunikation**

2: Kommunikationsprotokolle bei Nichtbenutzung ausschalten

**MG2b: Schutzmaßnahmen gegen Angriffe auf die Infrastruktur**

Es ist für diese Analyse davon auszugehen, dass keine Infrastruktur vorhanden ist.

**MG3: Schutz durch Einsatz von Softwareprodukten**

1,2,3,4,5,6: Virenschutz, Zugangskontrolle für Benutzer, Kommunikationssicherheit, Dateiverschlüsselung, Zugriffskontrolle für Hardwareerweiterungen, Zugriffskontrolle für Softwareerweiterungen

**MG4 / MP / MO: Andere Maßnahmen, abgesicherte Protokolle und organisatorische Maßnahmen**

1,2,5: Softwareupdate, ständiges Beaufsichtigen des Endgeräte, herausnehmbare Speicherkarten nutzen

***Szenario S4: mCommerce (privat)***

**MG1a: Schutzmaßnahmen gegen Datendiebstahl**

1,3: Schutz durch Verschlüsselung, Maßnahmen zur Identifikation des persönlichen Endgerätes

**MG2a: Schutzmaßnahmen gegen Angriffe auf die Kommunikation**

1,2: Kommunikationssicherheit (Ende-zu-Ende-Verschlüsselung), Kommunikationsprotokolle bei Nichtbenutzung ausschalten

**MG2b: Schutzmaßnahmen gegen Angriffe auf die Infrastruktur**

Es ist für diese Analyse davon auszugehen, dass keine Infrastruktur vorhanden ist.

**MG3: Schutz durch Einsatz von Softwareprodukten**

1,2,3,4,5,6: Virenschutz, Zugangskontrolle für Benutzer, Kommunikationssicherheit, Dateiverschlüsselung, Zugriffskontrolle für Hardwareerweiterungen, Zugriffskontrolle für Softwareerweiterungen

**MG4 / MP / MO: Andere Maßnahmen, abgesicherte Protokolle und organisatorische Maßnahmen**

1,2,5: Softwareupdate, ständiges Beaufsichtigen des Endgeräte, herausnehmbare Speicherkarten nutzen

Zwei Anmerkungen zu den charakteristischen Beispielen und Gegenmaßnahmen:

- Insbesondere Angriffe auf die Verfügbarkeit, etwa durch DoS Attacken, können durch die hier vorgestellten Maßnahmen nicht verhindert werden.
- Das Grundschutzhandbuch des BSI [GSHB] liefert zusätzliche Maßnahmen für den mittleren Schutzbedarf, die beispielsweise die physikalische Sicherheit betreffen.

## 3.6 Leitfaden zur Erstellung einer Unternehmenspolicy

Eine Unternehmenspolicy für die IT-Sicherheit ist ein Regelwerk, das beschreibt, was erlaubt ist und was nicht, und das Anforderungen an die Einsatzumgebung stellt.

Für den Einsatz mobiler Endgeräte bedeutet eine Policy im Unternehmen, dass sowohl Unternehmensinfrastrukturen, wie die mobilen Endgeräte und die Benutzer davon direkt betroffen sind. Eine Policy muss genau an die Umgebung angepasst sein, damit sie weder zu strikt ist, noch zu viele Freiheitsgrade lässt.

Der Leitfaden für die Erstellung der Sicherheitspolicy gliedert sich in die Feststellung der Ausgangslage, die Bestimmung der Freiheitsgrade und die Bestimmung der passenden Regeln.

### 3.6.1 Feststellung der Ausgangslage und des Schutzbedarfs

Für die konkrete Umsetzung muss die Ausgangslage des Unternehmens in Bezug auf den Einsatz mobiler Endgeräte festgestellt werden. Diese wird dadurch festgelegt, welche Geräteklasse bzw.

welcher Gerätetyp mobiler Endgeräte vorhanden ist und welche Dienste und mobile Anwendungen bereits eingesetzt werden. Die festgestellte Situation führt dann zu einer Menge von potentiellen Bedrohungen, die durch eine Auswahl genannter Gegenmaßnahmen abgewehrt werden können. Das Erfassen der Ausgangslage zur Erstellung einer Sicherheitspolicy ist in Abbildung 8 dargestellt.

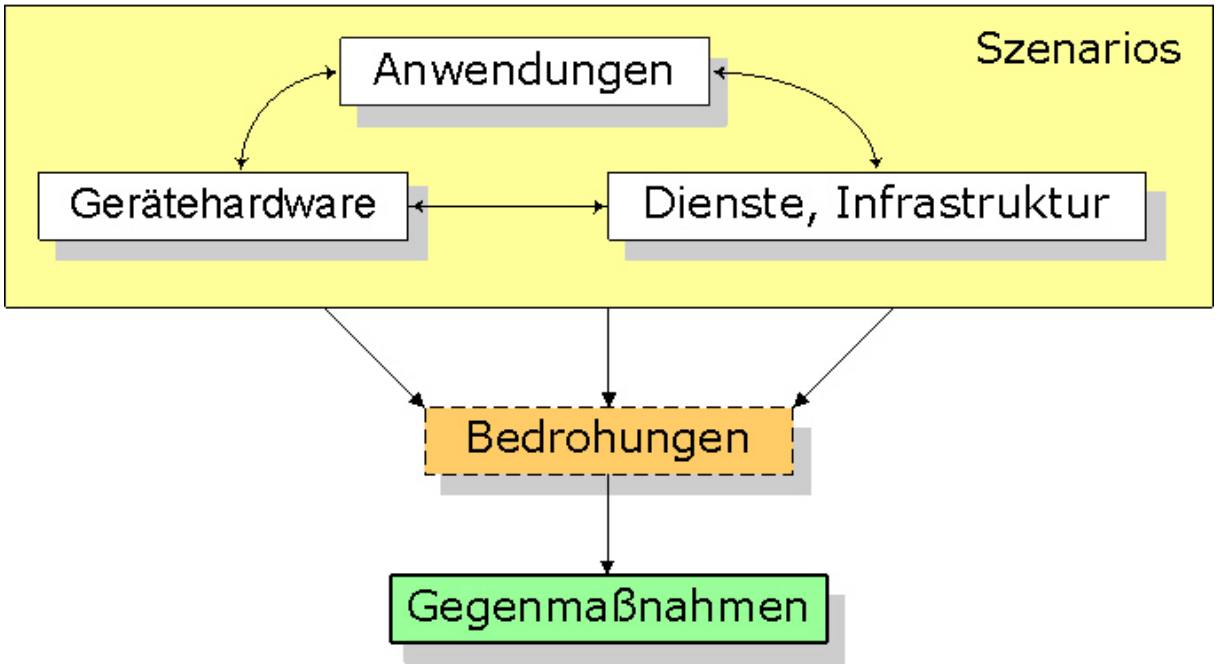



**Abbildung 7: Ausgangslage für Szenarios**

Es entstehen vor allem die drei unterschiedlichen Ausgangpositionen für die Erstellung einer Policy, die sich wie folgt beschreiben lassen:

Fall 1:

Ausgangspunkt: **Gerätehardware ist vorgegeben, Anwendungsszenarios sind bekannt**

Gesucht: *Welche konkreten Dienste können/dürfen von den Anwendern auf welche Weise genutzt werden?*

Fall 2:

Ausgangspunkt: **Dienste sind festgelegt, Anwendungsszenarios sind bekannt**

Gesucht: *Welche Geräteklassen bzw. konkreten Geräte dürfen zum Einsatz kommen?*

Fall 3:

Ausgangspunkt: **Gerätehardware und Dienste und Infrastruktur sind vorgegeben**

Gesucht: *Welche Anwendungen dürfen im Unternehmen erlaubt werden?*

### 3.6.2 Bestimmung der Freiheitsgrade

Durch Festlegen der Ausgangssituation wird klar, welche Freiheitsgrade bei der Einführung der mobilen Dienste bestehen. Beispielsweise sind im Unternehmen bereits mobile Endgeräte im Einsatz und die Anwendungen dafür sind fest vorgegeben. Von der Policy muss dann geregelt sein, wie der Anwender die Dienste nutzen darf.

Bei der Erstellung der Sicherheitspolicy müssen diese Freiheitsgrade des Geräteeinsatzes geregelt werden. Zudem muss beachtet werden, dass die erstellte Policy auch in bestehende Regelwerke integriert werden kann.

### 3.6.3 Bestimmung der passenden Regeln

Die beiden folgenden Listen beschreiben auf hoher Ebene, welche Bereiche von Regeln für den Einsatz der mobilen Endgeräte nötig sein können. Bei der Erstellung der Policy werden daraus sowohl die Punkte zur Regelung der Benutzung, als auch die Anforderungen an die Umgebung und Infrastruktur entwickelt.

**Benutzungsregelung**

- Gerät vor Verlust schützen
- Vorgehen bei Verlust des Gerätes
- Keine Weitergabe des Gerätes an Dritte bzw. Fremde
- Klare Regelung beim Einsatz des mobilen Endgerätes für private Zwecke
- Regelung des Software-Update Prozesses, Zeitfenster für Geräteverfügbarkeit im Netzwerk festlegen
- Passwortpolicy, dazu zählt, dass Passworte nicht auf dem mobilen Endgerät gespeichert werden, dass diese nicht aufgeschrieben werden und die Vergabe starker Passworte
- Regeln über die Art der Daten, die auf dem mobilen Endgerät mitgeführt werden dürfen
- Festlegung der maximalen Speichergröße des mobilen Endgerätes, um massiven Datenklau zu verhindern
- Regeln für Installation neuer/fremder Software auf den mobilen Endgeräten
- Umgang mit Geräteerweiterungen regeln oder verbieten
- Erweiterungsslots prüfen
- Über aktuelle Bedrohungen informieren
- Auf Falschmeldungen über Bedrohungen und Angriffe achten

**Anforderungen an die Infrastruktur**

- Automatische zentralisierte Passwortprüfung
- Zentrale Integrationsprüfungen der mobilen Geräte und der Infrastruktur
- Sicherheitsmaßnahmen der Infrastruktur berücksichtigen
- Benutzer und mobile Endgeräte dürfen nur die für ihre Aufgaben nötigen Rechte innerhalb der Unternehmensinfrastruktur besitzen

Bei der konkreten Erstellung der einzelnen Regeln muss jeder der vier Phasen des Lebenszyklus der Geräte berücksichtigt werden, die Beschaffung, die Installation, der Betrieb und das außer Betrieb nehmen der Geräte. Für diese Phasen können jeweils spezielle Policies nötig sein, andere Policies müssen für bestimmte Phasen umgeschrieben werden.

# 4. Fazit und Ausblick

## 4.1 Zusammenfassung

Es existieren vielfältige Bedrohungen beim Einsatz mobiler Endgeräte. Diese können auch bei normalen Einsatz die Sicherheit der gespeicherten Daten beeinträchtigen. Die Angriffe, die darauf aufbauen, sind teilweise von den stationären Geräten (PC, Workstation und Server) bekannt, teilweise ergeben sich aufgrund der Mobilität und der speziellen Anwendungen neuartige Gefährdungen. Die Geräte mit den darauf gespeicherten Daten sind durch Diebstahl und Verlust besonders gefährdet. Ein Angreifer, der im Besitz des Gerätes ist, kann das mobile Endgerät beliebig manipulieren und die Vertraulichkeit und Integrität der Daten beeinflussen. Deshalb gilt im professionellen Einsatz, dass je

nach Szenario selbst schon das kurzzeitige aus den Augen verlieren des Endgerätes zum Vertrauensverlust führen kann. Dort ist auch die Entwicklung und Umsetzung einer unternehmensweiten Sicherheitspolicy zu empfehlen, die beispielsweise den Einsatz eines persönlichen Endgerätes gleichzeitig für dienstliche und private Zwecke verbietet.

Da die mobilen Endgeräte selbst nur wenige Schutzmaßnahmen bieten, sollten zumindest diese genutzt werden. Sie genügen aber nur bei speziellen Angriffen und reichen nicht gegen die im Alltagseinsatz möglichen Bedrohungen. Nur durch technische und organisatorische Maßnahmen, zusätzliche Soft- oder Hardware und Schulung des Anwenders lässt sich die Anzahl der potentiellen Bedrohungen weiter senken.

## 4.2 Ausblick

Wünschenswert wären mobile Endgeräte, die die Integration aller Sicherheitsmechanismen in einem Gesamtsystem ermöglichen. Solche Systeme würden dann, abgesehen vom Verlust des Gerätes, schon bei der ersten Inbetriebnahme ein hohes Maß an Sicherheit bieten und vom Benutzer oder dem Unternehmen keine zusätzlichen Investitionen oder administrativen Aufwand erfordern.

Mit weiterer Verbreitung der Geräte wird sich entsprechende Schadsoftware (Viren, Würmer und Trojaner) weiter verbreiten. Durch die immer mächtigere Funktionalität der mobilen Endgeräte steigt die Zahl der Schwachstellen in den Systemen. Zusätzlich führen komplexere Anwendungen und Dienste zu mehr potentiellen Bedrohungen, so dass die Zahl der erfolgreichen Angriffe steigen dürfte. Monokulturen gleicher mobiler Endgeräte und Betriebssysteme fördern Angriffe darauf weiterhin, da sich das Verhältnis zwischen Aufwand eines Angriffs und dem erzielbaren Schaden, bzw. die Anzahl der möglichen Angriffsziele, weiter verschiebt.

# 5. Literatur


[GSHB] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutzhandbuch“, http://www.bsi.bund.de/gshb

[BB-SEC] Research in Motion Lim., „BlackBerry Security Overview”, Einstiegspunkt: http://www.blackberry.com/products/enterprisesolution/security/index.shtml

[BB-API] Research in Motion Lim., „Developers”, Einstiegspunkt: http://www.blackberry.com/developers/index.shtml

[BSI-DL] Bundesamt für Sicherheit in der Informationstechnik, „Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte“, Broschüre zum Herunterladen: http://www.bsi.de/literat/doc/drahtloskom/drahtloskom.pdf

[BSI-GSM] Bundesamt für Sicherheit in der Informationstechnik, „GSM-Mobilfunk - Gefährdungen und Sicherheitsmaßnahmen“, Broschüre zum Herunterladen: http://www.bsi.de/literat/doc/gsm/index.htm

[BSI-TP] Bundesamt für Sicherheit in der Informationstechnik, „Trusted Computing“, Online Themen: http://www.bsi.de/sichere_plattformen/trustcomp/index.htm

[LIN] LinuxDevices.com, „The Linux Devices Showcase”, Überblick: http://linuxdevices.com/articles/AT4936596231.html

[MS-API] Microsoft Corp., “Windows Mobile Developer Center”, Einstieg: http://msdn.microsoft.com/mobility/windowsmobile/default.aspx

[MS-GEN] Microsoft Corp., “Mobile Solutions”, Einstieg: http://www.microsoft.com/windowsmobile/default.mspx

[PALM] PalmSource, „Developers”, Einstieg: http://www.palmsource.com/developers/

[SYM] Symbian.com, “Developer – Software development kits”, Einstieg unter: http://www.symbian.com/developer/sdks/index.asp

[TAN02] Tanenbaum, A.S. (2002), „Moderne Betriebssysteme“, Pearson Studium, München.

# 6. Glossar

**- A -**

**ActiveSync**

Ein Produkt der Firma Microsoft um mobile Endgeräte mit Arbeitsrechnern oder Servern zu synchronisieren.

**Angriff**

Angriffe sind unerlaubte und unautorisierte Aktivitäten zum Schaden von Ressourcen, Dateien und Programmen.

**Anwendungsszenario**

Ein Anwendungsszenario ist die Gesamtheit von Einsatzzweck, Umgebungssituation, Benutzertyp, Geräteklasse und Protokollen. Anwendungsszenarios haben das Ziel typische Benutzungssituationen zu beschreiben, um Anwendern die Zuordnung zu Gegenmaßnahmen zu erleichtern.

**API**

Abkürzung für Application Programming Interface; die API beschreibt programmiertechnische Schnittstellen, die von anderen Programmen benutzt werden können.

**ARP**

Abkürzung für Address Resolution Protocol; ARP ist ein Netzwerkprotokoll zur gegenseitigen Auflösung von Hardwareadressen und Internetadressen.

**Authentisierung / Authentifikation**

Nachweis der Zugangsberechtigung durch die Abfrage von Benutzererkennung und Passwort bei Verbindungen zu Servern mit Zugangsbeschränkungen. Die Authentisierung ist das Nachweisen einer Identität, die Authentifizierung deren Überprüfung. Im Englischen wird zwischen den beiden Begriffen nicht unterschieden, das Wort authentication steht für beides.

**Autorisierung**

Die Autorisierung ist die Zuweisung und Überprüfung von Zugriffsrechten auf Daten und Diensten an Systemnutzer. Die Autorisierung erfolgt meist nach einer erfolgreichen Authentifizierung.

**- B -**

**Backdoor**

Eine Backdoor ist ein üblicherweise durch Viren, Würmer oder Trojanische Pferde installiertes Programm, das Dritten einen unbefugten Zugang („Hintertür“) zum Computer verschafft, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen. Backdoors werden oft für Denial-of-Service-Angriffe benutzt.

**Bedrohung**

Eine Bedrohung ist eine mögliche Gefahr für ein System.

**Bluetooth**

Bluetooth ist ein Industriestandard gemäß IEEE 802.15.1 für die drahtlose (Funk-)Vernetzung von Geräten über kurze Distanz.

**Brute-Force-Angriff**

Ein Brute-Force-Angriff stellt einen gewaltsamen Angriff auf einen kryptografischen Algorithmus dar. Das Verfahren probiert systematisch alle möglichen Kombinationen durch, um den Krypto-Algorithmus zu knacken.

**- C -**

**Capability**

Eine Capability ist eine vor fremdem Zugriff geschützte Objektreferenz, die einem Prozess zugeordnet ist und diesem bestimmte Rechte auf Objekte sichert.

**CF**

CompactFlash, Abkürzung CF, ist ein Schnittstellenstandard für Erweiterungskarten kleiner Größe. Diese CF-Karten sind meist digitale Speicherkarten für mobile Endgeräte.

**CF-Card**

Siehe auch CF.

**Chipkarte**

Chipkarten, oft auch als Smartcard oder Integrated Circuit Card (ICC) bezeichnet, sind Plastikkarten mit eingebautem Chip, die eine Hardware-Logik, Speicher oder auch einen Mikroprozessor enthalten.

**- D -**

**Daten**

In der Informatik werden maschinenlesbare und -bearbeitbare Repräsentation von Informationen als Daten bezeichnet.

**DNS**

Das Domain-Name-System wird für die Auflösung von Namen zu Internetadressen benötigt und stellt einen zentralen Dienst des Internets dar.

**DoS Angriff**

Als DoS-Angriff (Denial of Service attack, etwa: „Dienstverweigerungsangriff“) bezeichnet man einen Angriff auf einen Host (Server) mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen. In der Regel geschieht dies durch Überlastung. Erfolgt der Angriff koordiniert von einer größeren Anzahl anderer Systeme aus, so spricht man von einem DDoS (Distributed Denial of Service).

**DVB-H**

Abkürzung für Digital Video Broadcasting for Handhelds, ein Standard zur Übertragung digitaler Videodaten, der speziell auf mobile Endgeräte abgestimmt ist.

**- E -**

**eBook**

Als eBook (von electronic book) werden Bücher in digitaler Form bezeichnet. Dabei ist nicht jede digital gespeicherte Information (beispielsweise Webseiten) automatisch ein eBook. Charakteristisch für ein dBook ist, dass es einerseits der Form eines Buches (beispielsweise durch ein Inhaltsverzeichnis und Seitenangaben) ähnelt, andererseits die Vorteile einer digitalen Speicherung (Suchfunktionen, Metadaten) beinhaltet.

**- F -**

**Flash-Speicher**

Als Flash-Speicher wird eine bestimmte Art von Speicherchips – Flash-EEPROMs - bezeichnet. In Flash-Speichern können Informationen persistent (nichtflüchtig) gespeichert werden.

**Framework**

Ein Framework gibt eine (meist programmtechnisch genutzte) Struktur vor, die Softwareprogramme nutzen und verfeinern können.

**FTP**

FTP - File Transfer Protocol - ist ein Netzwerkprotokoll zur Dateiübertragung über TCP/IP.

**- G -**

**Gegenmaßnahmen**

Maßnahmen zur Reduzierung von Schwachstellen eines Systems oder zum Schutz von Systemen und Informationen gegen Bedrohungen.

**GUI**

Abkürzung für Graphical User Interface; die GUI stellt den Teil der Software dar, der für die grafische Bedienoberfläche verantwortlich ist.

**GSM**

GSM – Global System for Mobile Communications – ist ein digitaler Mobilfunknetz-Standard der zweiten Generation, der hauptsächlich für Telefonie aber auch für leitungsvermittelte und paketvermittelte Datenübertragung sowie Kurzmitteilungen (Short Messages) genutzt wird.

**- H -**

**Heap**

Der Heap (deutsch auch Halde genannt) ist eine Datenstruktur, in der beliebige Daten in beliebiger Reihenfolge gespeichert und wieder entnommen werden können.

**HTTP**

Das Hypertext Transfer Protokoll (HTTP) ist ein Netzwerkprotokoll zur Übertragung von Daten, das von Webbrowsern verstanden wird.

**HTTPS**

Zur Verschlüsselung und Authentisierung kann die HTTP Kommunikation durch das Hypertext Transfer Protokoll Secure abgesichert werden.

**- I -**

**ICMP**

Zur Übertragung von Wege- und Fehlerinformationen im Internet dient das Internet Control Message Protokoll (ICMP), das für den Internetnutzer aber meist verborgen bleibt.

**Information**

Information ist ein potenziell oder tatsächlich vorhandenes nutzbares oder genutztes Muster von Materie und/oder Energieformen, das für einen Betrachter innerhalb eines bestimmten Kontextes relevant ist. Wesentlich für die Information sind die Wiedererkennbarkeit sowie der Neuigkeitsgehalt. Das verwendete Muster verändert den Zustand eines Betrachters – im menschlichen Zusammenhang insbesondere dessen Wissen.

**IrDA**

Die Infrared Data Association – IrDA – beschreibt physische Spezifikationen und Kommunikationsprotokoll-Standards einer Infrarot-Schnittstelle für den Austausch von Daten mittels infrarotem Licht über kurze Strecken.

**- J -**

**J2ME**

Die Java 2 Micro Edition (J2ME) ist eine Java-Implementierung, die speziell auf mobile Endgeräte abgestimmt ist.

**- K -**

**Kompromittierung**

Eine Verletzung der Sicherheitspolitik derart, dass sensitive Informationen unautorisiert enthüllt worden sein können.

**- L -**

**LCD**

Ein LCD-Bildschirm (Liquid Crystal Display) nutzt spezielle Flüssigkristalle zur Darstellung und ist im Gegensatz zum Röhrenbildschirm praktisch emissionsfrei.

**Link Manager**

Eine Komponente eines Bluetooth-fähigen Gerätes, die zum Aufbau und der Konfiguration von logischen Kanälen dient.

**- M -**

**Man-in-the-middle-Angriff**

Bei einem Man-in-the-middle-Angriff steht ein Angreifer entweder physikalisch oder logisch zwischen zwei Kommunikationspartnern und hat dabei mit seinem System komplette Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern und kann die Informationen nach Belieben einsehen und sogar manipulieren.

**mCommerce**

Mobile Commerce ist eine spezielle Ausprägung des Electronic Commerce unter Verwendung drahtloser Kommunikation und mobiler Endgeräte.

**Middleware**

Middleware bezeichnet anwendungsunabhängige Technologien, die Dienstleistungen zur Vermittlung zwischen Anwendungen anbieten, so dass deren Komplexität verborgen wird.

**MMC**

Die Multimedia Card (MMC) ist eine digitale Speicherkarte mit kleineren Ausmaßen als eine CF-Karte.

**MMS**

Der Multimedia Messaging Service (MMS) ist als Nachfolger von SMS (Short Message Service) und EMS (Enhanced Messaging Service) anzusehen und bietet die Möglichkeit mit einem Mobiltelefon multimediale Nachrichten zu anderen mobilen Endgeräten oder zu normalen E-Mail-Adressen zu versenden. MMS wird von 3GPP (Third Generation Partnership Project) und OMA (Open Mobile Alliance) standardisiert.

**Multitasking**

Multitasking bezeichnet die Fähigkeit eines Betriebssystems oder allgemeiner einer Software, mehrere Aufgaben (tasks) (ggf. scheinbar) gleichzeitig auszuführen. In Rechensystemen mit einem Prouessor

werden die verschiedenen Prozesse in so kurzen Abständen immer abwechselnd aktiviert, dass der Eindruck der Gleichzeitigkeit entsteht.

**- O -**

**OBEX**

Das Object Exchange (OBEX) Protokoll ermöglicht den Austausch binärer Objekte zwischen Kommunikationspartnern.

**Object Push**

Übertragung von Datenobjekten, bei dem der sendende Partner die Aktion anstößt.

**Organizer**

Persönlicher Adress-, Termin- und Aufgabenverwalter in Form eines kleinen mobilen Endgerätes, beispielsweise ein PDA.

**- P -**

**PDA**

PDA – Personal Digital Assistant – ist eine Bezeichnung für eine Klasse von mobilen Endgeräten.

**PIN**

Die persönliche Identifikationsnummer (PIN) ist eine Geheimzahl, die zur Authentisierung (meist) gegenüber einer Maschine dient.

**Präemptives Multitasking**

Zeitliche Organisation eines Betriebssystems von parallel ablaufenden Prozessen, die um die vorhandene Rechenzeit konkurrieren. Beim präemptiven Multitasking wird dem Prozess nach Ablauf eines bestimmten Intervalls die Rechenzeit entzogen und ein anderer Prozess kann arbeiten.

**- R -**

**RAM**

Im Arbeitsspeicher (Random Access Memory, RAM) eines Computers werden Programme und Daten abgelegt. Auf seinen Inhalt, der bei Unterbrechung der Stromzufuhr verloren geht, kann in beliebiger Reihenfolge zugegriffen werden.

**Replay-Attacke**

Eine Replay-Attacke nutzt erneutes (nicht-autorisiertes) Einspielen von zuvor aufgezeichneten Datenpaketen in einem Netzwerk – meist nach deren Modifikation – zum Zwecke der Manipulation oder eines Denial-of-Service-Angriffs.

**RFID**

Radio Frequency Identification, in der deutschen Fachliteratur gelegentlich Funkerkennung genannt, ist eine Methode, um Daten auf einem Transponder berührungslos und ohne Sichtkontakt lesen und speichern zu können. Dieser Transponder kann an Objekten angebracht werden, welche dann anhand der darauf gespeicherten Daten automatisch und schnell identifiziert und lokalisiert werden können.

**- S -**

**Schadsoftware (auch Malware):**

Computerprogramme, die oft eine offene oder verdeckte Schadfunktion aufweisen und üblicherweise mit dem Ziel entwickelt werden, Schaden anzurichten. Darunter zählen Viren, Würmer und Trojanische Pferde.

**Schwachstelle (engl. Vulnerability)**

Eine Schwäche eines System oder ein Punkt, an dem ein System anfällig für eine Umgehung, Täuschung oder Modifikation der Sicherheitsfunktionen ist.

**Security Policy**

In einer Security Policy werden Schutzziele und allgemeine Sicherheitsmaßnahmen im Sinne offizieller Vorgaben eines Unternehmens oder einer Behörde formuliert. Detaillierte Sicherheitsmaßnahmen sind in einem umfangreicheren Sicherheitskonzept enthalten.

**SD**

Siehe SDIO

**SDIO - Secure Digital I/O**

SDIO ist eine Erweiterung des SD-Card-Standards um eine funktionelle Erweiterbarkeit von mobilen Endgeräten zu schaffen. Es existieren entsprechende Erweiterungskarten, die Bluetooth, WLAN, GPS Empfänger, uvm. bereitstellen.

**SDR**

Siehe Software Defined Radio

**Sicherheitspolicy**

Eine Sammlung von Gesetzen, Regeln und Praktiken, welche regeln, wie eine Organisation sensitive Informationen verwaltet, schützt und verteilt.

**Sicherheitsrichtlinie**

Eine Menge von Regeln und Empfehlungen, die festlegen, wie ein Unternehmen Sicherheitsmechanismen zum Schutz von sensitiven Daten und Ressourcen einsetzt.-

Anmerkung: Security Policy, Sicherheitspolicy und Sicherheitsrichtlinie werden häufig als Synonyme verwendet.

**SIM-Karte**

Die SIM (Subscriber Identity Module) ist eine kleine Chipkarte, die zur Identifikation des Benutzers bzw. des Gerätes in einem Mobilfunknetz dient.

**Smartcard**

siehe Chipkarte.

**Smartphone**

Smartphone ist eine Bezeichnung für eine Klasse von mobilen Endgeräten, die in vielerlei Hinsicht eine Zusammenführung von PDA und Mobiltelefon ist.

**SMS**

Short Message Service (SMS) ist ein Telekommunikationsdienst zur Übertragung von Textnachrichten.

**SMSC**

Der Short Message Service Center (SMSC) ist in einem Mobilfunknetz die Komponente, die für die Vermittlung von SMS Nachrichten zuständig ist.

**Sniffing**

Eine Angriffsart, bei der Daten aus Kommunikationsverkehr gewonnen werden.

**Software Defined Radio**

Mit dem Terminus Software-Defined-Radio (kurz SDR) beschreibt man die Bestrebung, möglichst die gesamte Signalverarbeitung eines Hochfrequenz-Senders oder -Empfängers mit Hilfe anpassbarer Hardware in Software abzubilden.

**Software Update**

Ein Software-Update bezeichnet die neue Version einer Basissoftware, welche Programmmängel korrigiert oder kleinere Programmverbesserungen enthält.

**Spyware**

Als Spyware bezeichnet man Programme, die Informationen über die Tätigkeiten des Benutzers sammeln und an Dritte weiterleiten. Ihre Verbreitung erfolgt meist durch Trojanische Pferde.

**SSH**

Secure Shell (SSH) ist ein Netzwerkprotokoll zur abgesicherten Verbindung auf einen entfernten (meist Unix-) Rechner.

**SSL/TLS**

Secure Sockets Layer (SSL) und Transport Layer Security (TLS) sind Internetprotokolle zur Absicherung von Kommunikationsverbindungen.

**Stack**

Der Stack (auch Keller genannt) ist eine Datenstruktur, in der nur auf das oberste Element zugegriffen werden kann.

**SyncML**

SyncML (Synchronization Markup Language) ist ein plattformunabhängiger Standard der Open Mobile Alliance (OMA) zur Datensynchronisation.

**- T -**

**Tablet PC**

Ein mobiles Endgerät, dessen Bauform an ein Tablett erinnert und dessen Benutzungsschnittstelle im Wesentlichen aus einem großen berührungssensitiven Bildschirm besteht.

**TCG**

Die Trusted Computing Group (TCG) ist eine internationale Organisation, die einen Standard für eine sowohl durch Software als auch Hardware abgesicherte Computer-Plattform entwickelt.

**TCP**

Siehe TCP/IP

**TCP/IP**

Eine Menge von vielen Protokollen (TCP, UDP usw.), die die Basis für die Kommunikation im Internet darstellen.

**Trojanisches Pferd**

Schadsoftware, bestehend aus einem (manchmal nur scheinbar) nützlichen Wirtsprogramm und einem versteckt arbeitenden, bösartigen Teil. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.

**- U -**

**Ubiquitous Computing**

Der Begriff Ubiquitäre Computertechnik (engl. Ubiquitous Computing) bezeichnet die Allgegenwärtigkeit der Informationsverarbeitung im Alltag von Unternehmen und Kunden.

**UDP**

Siehe TCP/IP

**UMTS**

Universal Mobile Telecommunications System, besser bekannt unter der Abkürzung UMTS, ist ein Mobilfunkstandard der dritten Generation (3G).

**Unternehmenspolicy**

Siehe Sicherheitsrichtlinie

**Update**

Siehe Software Update

**USB**

USB (Universal Serial Bus), weit verbreitete Möglichkeit zum Anschluss von Hardware an Rechensysteme.

**USB-Token**

Eine Hardwarekomponenten, die im Wesentlichen einer Chipkarte entspricht, die über USB mit dem Rechner verbunden wird.

**- V -**

**Virus**

Schadsoftware, die sich verbreitet, indem sie Kopien von sich selbst in Programme, Dokumente oder Datenträger schreibt.

**VoIP**

Voice over IP (VoIP) ist das Telefonieren über ein Computernetzwerk auf der Grundlage des Internetprotokolls (IP).

**VPN**

Ein Virtual Private Network (VPN) stellt eine durch kryptografische Maßnahmen abgesicherte Verbindung über ein öffentliches (meist nicht vertrauenswürdiges) Netzwerk her.

**- W -**

**WAP**

Das Wireless Application Protocol (WAP) stellt Techniken zur Übertragung von Internetdokumenten auf mobile Endgeräte zur Verfügung.

**WLAN**

Wireless LAN bezeichnet ein „drahtloses“ lokales Funknetz, wobei meistens ein Standard der IEEE 802.11-Familie gemeint ist.

**Wörterbuch Attacke**

Als einen Wörterbuchangriff bezeichnet man die Methode der Kryptoanalyse, ein unbekanntes Passwort mit Hilfe einer Passwortliste (im weitesten Sinne eines Wörterbuchs) zu knacken.

**WTLS**

Ein Protokoll zur Absicherung ähnlich dem SSL/TLS Protokoll, das speziell für die Absicherung der WAP-Protokolle entwickelt wurde.

**Wurm**

Schadsoftware, ähnlich einem Virus, verbreitet sich aber direkt über Netzwerke wie das Internet und versucht in andere Computer einzudringen.

**- Z -**

**Zugangskontrolle**

Eine Zugriffskontrolle regelt den Zugriff auf Rechensysteme und sichert diese gegen unberechtigte Benutzer.