Ilmenauer Beiträge zur Wirtschaftsinformatik

Herausgegeben von U. Bankhofer, V. Nissen
D. Stelzer und S. Straßburger

Sebastian Frosch, Daniel Fischer

Maßnahmen zur Sicherung von Datenübertragungen in GSM-/UMTS-Mobilfunknetzen

Arbeitsbericht Nr. 2011-03, September 2011

Technische Universität Ilmenau
Fakultät für Wirtschaftswissenschaften
Institut für Wirtschaftsinformatik

Autor: Sebastian Frosch, Daniel Fischer

Titel: Maßnahmen zur Sicherung von Datenübertragungen in Mobilfunknetzen

Ilmenauer Beiträge zur Wirtschaftsinformatik Nr. 2011-03, Technische Universität Ilmenau, 2011

ISSN 1861-9223

ISBN 978-3-938940-35-8

urn:nbn:de:gbv:ilm1-2011200514

Anschrift: Technische Universität Ilmenau, Fakultät für Wirtschaftswissenschaften, Institut für Wirtschaftsinformatik, PF 100565, D-98684 Ilmenau.
http://www.tu-ilmenau.de/fakww/Ilmenauer_Beitraege.1546.0.html

Gliederung

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

3GPP	3rd Generation Partnership Project
AN	Anonymität
AU	Authentizität
AuC	Authentication Centre
API	Application Programming Interfaces
ARP	Address Resolution Protocol
BSC	Base Station Controller
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSS	Base Station Subsystem
BT	Bluetooth
BTS	Base Transceiver Station
CDMA	Code Division Multiple Access
CN	Core Network
CRM	Customer Relationship Management
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
EDGE	Enhanced Data Rates for GSM Evolution
EIR	Equipment Identity Register
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute
GGSN	Gateway GPRS Support Node

GMSC	Gateway Mobile Switching Center
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HLR	Home Location Register
HSCSD	High Speed Circuit Switched Data
HSDPA	High Speed Downlink Packet Access
HTC	High Tech Computer Corporation
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ID	Identifikationsnummer
IDS	Intrusion-Detection-Software
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
IN	Integrität
IP	Internet Protocol
IrDA	Infrared Data Association
ISO	International Organization for Standardization
IT	Informationstechnik
IV	Informationsverarbeitung
JVM	Java-Virtuelle-Maschine
LAN	Local Area Network
LTE	Long Term Evolution
ME	mobiles Endgerät
MITM	Man-in-the-Middle
MMS	Multimedia Messaging Service

MP3	MPEG-1 Audio Layer 3
MS	mobile Station
MSC	Mobile Switching Center
NOC	Network Operation Center
NSS	Network Subsystem
OM	Organisatorische Sicherheitsmaßnahme
OS	Operating System
OSI	Open Systems Interconnection
OSS	Operation and Support System
OTA	over the air
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
PIM	Personal Information Manager
PIN	Persönliche Identifikationsnummer
RIM	Research in Motion
RNC	Radio Network Controller
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SMS	Short Message Service
SS7	Signalisierungssystem Nr. 7
SSID	Service Set Identity
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
THC	The Hacker's Choice
TM	Technische Sicherheitsmaßnahme

TMSI	Temporary Mobile Subscriber Identity
TMTO	Time Memory Trade-Off
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
VB	Verbindlichkeit
VF	Verfügbarkeit
VT	Vertraulichkeit
VLR	Visitor Location Register
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WLAN	Wireless Local Area Network
WTLS	Wireless Transport Layer Security

Zusammenfassung: GSM-/UMTS-Mobilfunknetze werden im Geschäftsleben nicht nur zur Sprachkommunikation, sondern immer häufiger auch zur Übertragung von Geschäftsdaten eingesetzt. Zur sicheren Gestaltung derartiger mobiler Datenübertragungen erarbeiten wir in diesem Arbeitsbericht einen Maßnahmenkatalog. Zunächst strukturieren wir den Betrachtungsgegenstand „mobile Datenübertragung“ in einem Ebenenmodell. Mit Hilfe einer Bedrohungsanalyse untersuchen wir danach typische Bedrohungen bei der mobilen Datenübertragung und dokumentieren diese in Form von Bedrohungsbäumen. Auf Grundlage einer Literaturrecherche und von uns durchgeführten Expertengesprächen ermitteln wir anschließend mögliche Sicherheitsmaßnahmen. Unser Katalog umfasst 70 technische und organisatorische Maßnahmen.

Schlüsselworte: Mobilfunk, Sicherheit, Bedrohungen, Sicherheitsmaßnahmen, GSM, UMTS

1 Einleitung

1.1 Problemstellung

Mobilfunknetze werden im Unternehmensbereich nicht nur für die Sprachkommunikation genutzt, sondern immer häufiger auch zur Übertragung von Geschäftsdaten. Die zunehmende Ausstattung von Mitarbeitern mit mobilen Endgeräten beschleunigt diesen Trend [IDC09]. Bei der mobilen Datenübertragung im Unternehmensbereich gibt es verschiedene Einsatzfelder, angefangen vom einfachen Abgleich von Kontakt- und Termindaten eines Mitarbeiters bis hin zum Zugriff auf den unternehmensinternen Datenbestand. Weitere Datenübertragungen können sogar mittels mobiler Endgeräte zum Auslösen und Steuern von Unternehmensprozessen genutzt werden, z. B. im Rahmen der mobilen Auftragserfassung für Außendienstmitarbeiter oder zur Aktualisierung von Datensätzen eines CRM-Systems[1] direkt nach einem Kundengespräch. Die Nutzung dieser Dienste vereinfacht die alltägliche Arbeit vieler Mitarbeiter. Jedoch wird die mobile Datenübertragung über Mobilfunknetze oftmals in die Geschäftsprozesse eingebunden, ohne die möglichen Bedrohungen zu kennen, die mit derartigen Übertragungen verbunden sind.

Abb. 1-1 zeigt die an einer Datenübertragung über ein Mobilfunknetz beteiligten Akteure und Systeme. Diese sind: der Nutzer, das mobile Endgerät, das Mobilfunknetz, das Internet[2] und das lokale Unternehmensnetzwerk.

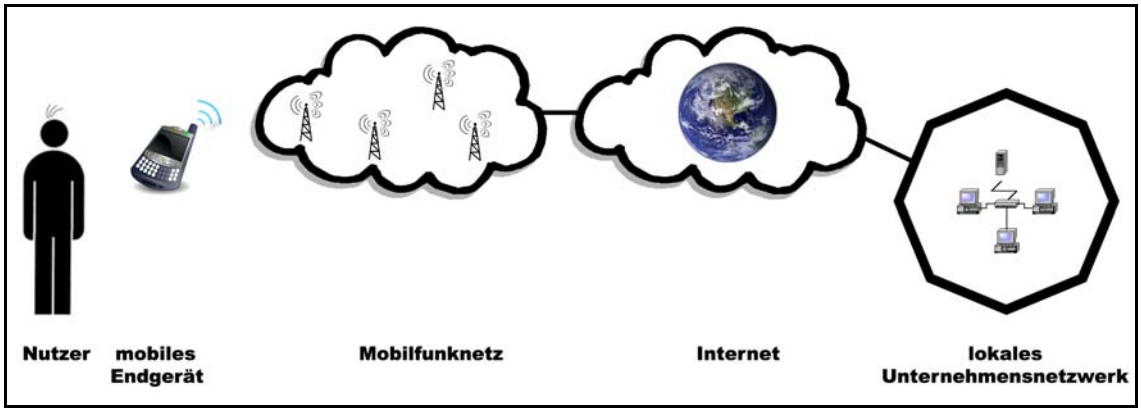

Abb. 1-1: Akteure und Systeme einer Datenübertragung über ein Mobilfunknetz

[1] Customer Relationship Management System sind Datenbankanwendung zur Erfassung von Kundendaten und Interaktionshandlungen mit den Kunden [AbMü09, 278 f.].

[2] Das Internet stellt hier das Transportnetzwerk zwischen Mobilfunknetz und lokalem Netzwerk dar.

Alle diese Akteure und Systeme können Schwachstellen aufweisen. Durch Ausnutzung dieser Schwachstellen können die allgemeinen Sicherheitsziele Integrität, Vertraulichkeit, Authentizität und Verfügbarkeit bedroht werden. Daher stellt sich die Frage: Welche Sicherheitsmaßnahmen sind für die Datenübertragung in Mobilfunknetzen publiziert und wie erhöhen diese das Sicherheitsniveau?

1.2 Zielsetzung

Ziel dieser Arbeit ist es, einen Maßnahmenkatalog zur Sicherung der Datenübertragung über Mobilfunknetze (GSM/UMTS) zu erstellen. Dieser wird aus Nutzersicht erstellt und beinhaltet nur Maßnahmen, die der Nutzer selbstständig ergreifen kann, ohne dabei auf die Unterstützung der Mobilfunknetzbetreiber angewiesen zu sein.

1.3 Methodik

Die Grundlagen zu den Themen IT-Sicherheit, Mobilfunknetze und Bedrohungsanalyse [Ecke08, 170] erarbeiteten wir mit Hilfe einer Literatur- und Internetrecherche. Eine detaillierte Bedrohungsanalyse half uns anschließend typische Bedrohungen bei der Datenübertragung über Mobilfunknetze aufzudecken und in einem Bedrohungskatalog zusammenzustellen. Ausgehend von dem Bedrohungskatalog haben wir durch umfangreiche Literaturanalysen, Internetrecherche, Experteninterviews sowie persönliche Einschätzungen und Tests mögliche Sicherheitsmaßnahmen ermittelt und diese systematisiert in einem Maßnahmenkatalog zusammengefasst. Abschließend stellten wir die ermittelten Bedrohungen und die mögliche Sicherheitsmaßnahmen in Kreuzreferenztabellen [Tern05, 12] dar, um zu verdeutlichen, welche Maßnahmen welchen Bedrohungen entgegenwirken.

1.4 Aufbau

Der vorliegende Arbeitsbericht hat folgenden Aufbau: Im zweiten Abschnitt erörtern wir kurz wesentliche Begriffe zur IT-Sicherheit, zu den Mobilfunknetzen GSM und UMTS sowie zu mobilen Endgeräten. Des Weiteren grenzen wir den Betrachtungsgegenstand der Arbeit durch die Einführung eines Ebenenmodells für die mobile Datenübertragung weiter ein. Im dritten Abschnitt beschreiben wir die Durchführung unserer Bedrohungsanalyse. Anhand von Bedrohungsbäumen [Ecke08, 172 ff.] stellen wir typische Bedrohungen der einzelnen, an der Datenübertragung beteiligten Akteure und Systeme dar. Im vierten Kapitel ermitteln wir Sicherheitsmaßnahmen [FSKr06, 12] (bzw. Gegenmaßnahmen zu den zuvor ermittelten Bedrohungen) und stellen diese in einem Maßnahmenkatalog zusammen.

Zusätzlich ordnen wir in Kreuzreferenztabellen die Sicherheitsmaßnahmen den ermittelten Bedrohungen zu. Im letzten Abschnitt fassen wir unsere Erkenntnisse zusammen, unterziehen diese einer kritischen Würdigung und geben Hinweise für weitere Forschung im Bereich der Sicherheit von mobilen Datenübertragungen.

2 Begriffsbestimmung und Abgrenzung des Betrachtungsgegenstandes

2.1 IT-Sicherheit

2.1.1 Sicherheit

Sicherheit in der Informationsverarbeitung ist ein vielfältig definierter Begriff. Rieger und Witt verstehen unter IT-Sicherheit im Allgemeinen einen Zustand, in dem keine Gefahren und/oder Schwachstellen in einem definierten IT-System[3] vorhanden sind [Rieg05, 23; Witt06, 1]. Da dies aber in der Realität in der Regel nie der Fall ist, stellen andere Autoren bei der Definition eher die Anwendung von Sicherheitsmaßnahmen in der Vordergrund [DBCr01, 15 ff.; Raep01, 8; Stel93, 20ff.]. Das BSI definiert IT-Sicherheit als Zustand „in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind.“ [BSI09, 51]

2.1.2 Schwachstellen und Bedrohungen

Ein IT-System kann verschiedene Schwachstellen aufweisen und ist dadurch anfällig für Bedrohungen [BSI09, 54].

Schwachstellen sind Mängel/Schwächen eine IT-Systems, die das Einwirken von sicherheitsgefährdenden Ereignissen auf dieses System begünstigen [Stel93, 40]. Über eine Schwachstelle können Sicherheitsmaßnahmen eines IT-Systems umgangen, getäuscht oder unautorisiert modifiziert werden [Ecke08, 13 f.; Kapp07, 6].

Eine *Bedrohung* ist ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann [BSI09, 46]. Eine Gefährdung entsteht, wenn eine Bedrohung auf eine Schwachstelle

[3] IT-Systeme sind offene oder geschlossene Systeme, welche dynamischen Entwicklungen unterliegen können und zur Speicherung und Verarbeitung von Informationen dienen [Ecke08, 2].

eines IT-Systems trifft und dies für einen Angriff ausgenutzt werden kann [Sack08]. Ein Verlust der Integrität, der Vertraulichkeit oder der Verfügbarkeit des IT-Systems oder eines Systemteils (sicherheitsrelevante Elemente) wären die Folge [BSI09, 46; Ecke08, 13 ff.; Stel93, 40].

2.1.3 Sicherheitsziele

Sicherheitsziele sind Eigenschaften, „die ein IT-System bereitstellen muss, um den Sicherheitsanforderungen seiner Benutzer zu entsprechen.“ [Raep01, 4] Aus den Anforderungen an die wichtigsten Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit [BSI03, 58] entsteht ein entsprechender Schutzbedarf für ein IT-System. Da Bedrohungen in offenen Netzen immer wieder diesen drei Gesichtspunkten zugeordnet werden können, spricht man bei einer Verletzung dieser Sicherheitsziele von den Grundbedrohungen eines Systems [BSI92, 19]. Darüber hinaus existieren weitere wichtige Sicherheitsziele. Diese sind die Authentifikation von Benutzern, die Kontrolle von Zugriffen, die Verbindlichkeit von Kommunikationsbeziehungen und bei Bedarf auch die Anonymität des Ursprungs von Informationen [Raep01, 8; Schä03, 8].

Vertraulichkeit bedeutet, dass sicherheitsrelevante Elemente (z. B. Daten, Programme und IV-Prozesse) vor unberechtigter Einsicht durch Dritte geschützt sind [BITK03, 63; Raep01, 4; Stel93, 35]. Die Anforderung an die Vertraulichkeit kann sogar dahingehend ausgeweitet werden, dass die bloße Existenz von sicherheitsrelevanten Elementen nicht für Außenstehende erkennbar sein darf [Raep01, 4; Schä03, 8].

Integrität von sicherheitsrelevanten Elementen (Daten, Programme, usw.) bedeutet die Sicherung gegen beabsichtigte oder zufällige Manipulation [FePf00; Sack08; Stel93, 34]. Der Verlust der Integrität kann z. B. durch Übertragungsfehler oder durch bewusst ausgeführte Angriffe verursacht werden, indem ein Angreifer während der Übertragung Informationen ersetzt oder Teile davon modifiziert. Es muss also möglich sein, unbewusste oder beabsichtigte Manipulationen zu erkennen, wofür es wiederum erforderlich ist, den Urheber von Daten eindeutig und nicht manipulierbar zu identifizieren [Raep01, 4; Schä03, 8].

„V*erfügbarkeit* trifft Vorsorge dafür, dass nutzungsberechtigte Personen auf Informationen und Kommunikationsdienste zur rechten Zeit am rechten Ort zugreifen können.“ [Raep01, 4] Durch unbefugte Modifikation von Hardware, Software oder Daten kann ein Verlust der Verfügbarkeit verursacht werden. Ist die Verfügbarkeit von IT-Systemen nicht gegeben, können andere Sicherheitsziele, wie die Integrität oder die Vertraulichkeit ebenfalls ge-

fährdet sein. „Die Anforderungen eines Systems an die Verfügbarkeit sind stark von dessen Einbindung in die operativen Abläufe des Unternehmens abhängig.“ [Raep01, 4] Dabei überschneiden sich beispielsweise Verfügbarkeit und Integrität häufig. Wird ein sicherheitsrelevantes Element zerstört, so ist sowohl die Verfügbarkeit als auch die Integrität verletzt [Stel93, 35].

Authentizität bedeutet das zweifelsfreie Nachweisen der Identität von Daten, Netzen, Systemen oder Personen [BITK03, 15]. Daher müssen Benutzer oder Systeme vor dem Zugriff auf Daten oder Kommunikationsdienste einen eindeutigen Beweis ihrer Identität erbringen. Dieser Nachweis kann durch Besitztum (z. B. SmartCards [Papa06, 260]), Wissen (z. B. einem Kennwort) oder persönliche Merkmale (z. B. einem Fingerabdruck) realisiert werden [BITK03, 48 ff.; Stel93, 43]. Die Authentizität ist außerdem die Voraussetzung für weitere Sicherheitsziele wie Integrität und Vertraulichkeit [Ecke08, 429].

Die V*erbindlichkeit* von Kommunikationsbeziehungen soll es unmöglich machen, die Nutzung oder den Empfang eines sicherheitsrelevanten Elementes abzustreiten [Stel93, 39]. Im Bereich der elektronischen Kommunikation muss ein vergleichbares Sicherheitsniveau geschaffen werden, wie bei der Verwendung des Mediums Papier, bei dem der Inhalt eines Dokumentes untrennbar mit einer Unterschrift verbunden ist [Raep01, 5].

Anonymität schützt, z. B. aus Gründen des Datenschutzes, eine Person davor, ihre Identität preiszugeben [Raep01, 6]. Anonymität muss vor allem dort gewährleistet werden, wo personenbezogene Daten in Verbindung mit vorausgegangenen Authentifikationsverfahren erhoben werden. Die beteiligten Akteure müssen sich demnach gegenseitig authentisieren, wobei ihre eingegebenen Daten vor dem Zugriff unbefugter Dritter geschützt werden müssen.

2.1.4 Sicherheitsmaßnahmen

Sicherheitsmaßnahmen[4] sind Methoden und Werkzeuge, die dazu geeignet sind, identifizierte Schwachstellen (Sicherheitslücken) zu reduzieren und somit den Anforderungen an die Sicherheit eines Systems gerecht zu werden [Raep01, 22; Schn04, 269]. Grundsätzlich stehen dabei folgende Arten von Maßnahmen zur Auswahl [BSI92, 73; Hump04, 15; Raep01, 23; Schn04, 269 f.]:

[4] Zu dem Begriff Sicherheitsmaßnahme existieren in der Literatur verschiedene Synonyme, wie z. B. Sicherungsmaßnahme [Witt06, 5], Schutzmechanismus [Bran05, 8 ff.], Gegenmaßnahme [Ecke08, 49 ff.] usw. Im Folgenden verwenden wir einheitlich den Begriff Sicherheitsmaßnahme.

- präventive Maßnahmen, die Gefahren bereits im Vorfeld zu vermeiden helfen,
- überwachende Maßnahmen, die Angriffe bei ihrem Eintritt erkennen und abzuwehren versuchen, sowie
- reaktive Maßnahmen, die nach Eintritt der Bedrohung die Schadensfolgen verringern.

Dabei ist es wichtig, sich nicht nur auf eine Art von Maßnahmen (Schutz, Erkennung oder Reaktion) zu verlassen. Es ist wichtig, eine gute Kombination aus allen zur Verfügung stehenden Maßnahmen zu nutzen, denn was wäre zum Beispiel eine Erkennungsmaßnahme ohne eine reaktive Maßnahme [Schn04, 269 f.]?

Existieren mehrere Alternativen zur Minderung einer Bedrohung, so ist die Entscheidung für oder gegen eine bestimmte Sicherheitsmaßnahme von verschiedenen Faktoren abhängig [Raep01, 23]:

- Schutzwirkung der Maßnahme,
- Kosten für die Beschaffung, Einführung und den Betrieb der Maßnahme,
- Höhe des verbleibenden Restrisikos nach Anwendung der Sicherheitsmaßnahme,
- Zusammenwirken mit anderen Maßnahmen,
- Benutzerfreundlichkeit der Maßnahme.

Die Schutzwirkung muss immer im Verhältnis zum Wert des geschützten Elementes stehen, da mit dem Einsatz stärkerer Sicherheitsmaßnahmen gewöhnlich auch die Kosten steigen. Ist mit der Einführung der Maßnahme das verbleibende Restrisiko immer noch zu hoch, dann sollte über andere oder ergänzende Alternativen nachgedacht werden. Dabei sind die bereits vorgeschlagenen Sicherheitsmaßnahmen in die Planung mit einzubeziehen, da sie selbst sicherheitsrelevante und damit schutzwürdige Elemente darstellen können [Stel93, 42].

2.2 Mobilfunknetze

2.2.1 Global System for Mobile Communications

Das Global System for Mobile Communications (GSM) ist ein leitungsvermitteltes Übertragungssystem, welches für die Sprachkommunikation von mobilen Teilnehmern entwickelt wurde [Detk97; Ster06]. GSM unterstützt aber nicht nur die Sprachkommunikation,

sondern auch die Datenkommunikation. 1989 übernahm das European Telecommunications Standards Institute (ETSI) die Verantwortung für die Standardisierung von GSM[5]. 1991 begann die kommerzielle Nutzung der GSM-Netze [Detk97, 22 ff.; Ster06, 7 ff.]. Es ist der weltweit am weitesten verbreitete Mobilfunkstandard, auf dessen Grundlage in über 130 Ländern Mobilfunknetze betrieben werden. Heute sind vor allem vier Frequenzbänder für eine weltweite GSM-Kommunikation entscheidend: 850 MHz, 900 MHz, 1800 MHz und 1900 MHz [Saut08, 30]. Abb. 2-3 zeigt den Aufbau eines GSM-Mobilfunknetzes.

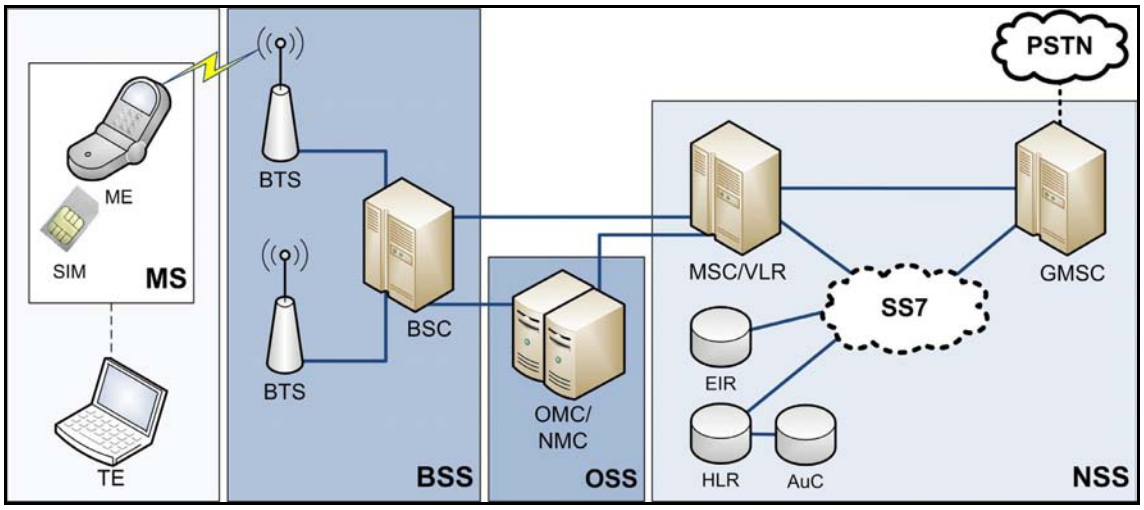

Abb. 2-1: Aufbau eines GSM-Netzes ohne GPRS [BSI08a, 9]

Die *mobile Station (MS)*, die im allgemeinen Sprachgebrauch als mobiles Endgerät oder Mobiltelefon bezeichnet wird, ermöglicht einen ortsunabhängigen Zugriff auf die im GSM-Netz angebotenen Dienste [BSI08a, 9 ff.; Detk97, 39 ff.; Fede99, 37 ff.; Saut08, 12 ff.]. Die mobile Station besteht aus dem Subscriber Identity Module (kurz: SIM-Karte) und aus der Hardware zum Senden und Empfangen von Sprache und Daten. Die *SIM-Karte* enthält den geheimen Schlüssel (K_i) und Informationen zur Identifikation des Nutzers[6]. Aus K_i wird der Verschlüsselungsschlüssel (K_c) generiert, welcher für die Verschlüsselung der gesendeten Daten benötigt wird.

Das *Base Station Subsystem (BSS)* ist das eigentliche Funknetz [BSI08a, 9 ff.; Detk97, 39 ff.]. Es besteht aus den Base Transceiver Stations (BTS), den so genannten Funkantennen, welche über die Luftschnittstelle (Air Interface) die Verbindung zur mobilen Station und

[5] Für die Standardisierung ist mittlerweile das 3rd Generation Partnership Project (3GGP) zuständig. Dokumentationen und Spezifikationen befinden sich unter http://www.3gpp.org.

[6] Die Identifikation des Nutzers erfolgt über die International Mobile Subscriber Identity (IMSI). Anhand der IMSI ist ein Teilnehmer international eindeutig identifizierbar.

zum Base Station Controller (BSC) herstellen. Der Base Station Controller ist die Funkkanal-Vermittlungseinrichtung innerhalb des BSS und übernimmt die Prozesssteuerung der BTS. Das BSC ist wiederum über das Abis-Interface mit den BTS verbunden [Saut08, 42]. Zur Übertragung der Signalisierungs- und Inhaltsdaten wird im GSM-Netz der Algorithmus A5 verwendet. Vom A5 Algorithmus existieren vier Varianten [BSI08a, 20]:

- A5/0 ist eine Variante ohne jegliche Verschlüsselung, die nachträglich implementiert wurde, da in einigen Staaten die Verschlüsselung verboten ist.
- A5/1 ist eine Stromchiffre, dessen Algorithmus nicht offen gelegt wurde, durch Reverseengineering aber nachgestellt wurde und mittlerweile anfällig für Angriffe ist.
- A5/2 ist ebenfalls eine Stromchiffre, allerdings eine abgeschwächte Version des A5/1 Algorithmus, die extrem anfällig für Angriffe ist.
- A5/3 ist eine Blockchiffre, die auch unter dem Name „Misty“ bekannt ist. Dieser ist identisch zu dem als „Kasumi“ bekannten Algorithmus, der in UMTS-Netzen zum Einsatz kommt. Die Spezifikationen von A5/3 wurden von Anfang an offen gelegt, was die Identifikation und Schließung von Schwachstellen vereinfacht.

Das *Operation and Support System (OSS)* koppelt das BSS und das NSS und stellt Funktionalitäten zur Konfiguration sämtlicher GSM-Netzkomponenten sowie zur Gesprächsüberwachung bereit [BSI08a, 9 ff.; Detk97, 39 ff.; Fede99, 37 ff.].

Das *Network Switching Subsystem (NSS)* übernimmt die Vermittlung von Verbindungen innerhalb des Netzes und auch in andere Netze [BSI08a, 9 ff.; Detk97, 39 ff.; Fede99, 37 ff.; Saut08, 12 ff.]. Zentrales Element ist das Mobile Switching Center (MSC). Alle Verbindungen werden immer über ein MSC geleitet und kontrolliert, auch der Handover[7] zwischen den verschiedenen BSC wird durch das MSC durchgeführt. Im Visitor Location Register (VLR) werden alle Teilnehmer, die sich im Bereich des MSC aufhalten, temporäre verwaltet (Besucherdatenbank). Es enthält Kopien der im Home Location Register (HLR) gespeicherten Teilnehmerdaten, um die Signalisierung zwischen MSC und HLR zu reduzieren. Das HLR ist die Teilnehmerdatenbank. In ihr werden alle für die Identifikation der Teilnehmer notwendigen Daten und die für die Teilnehmer freigeschalteten Dienste ge-

[7] Handover bezeichnet die Übergabe einer sich bewegenden mobilen Station von einer zur anderen Funkzelle ohne einen Verbindungsabbruch [Jung02, 3-270].

speichert. Das Authentication Centre (AuC) enthält neben den Algorithmen zur Authentifizierung der Teilnehmer auch die geheimen Schlüssel (K_i) der Teilnehmer. Auf jeder SIM-Karte befindet sich einer dieser Schlüssel als Kopie. Das Equipment Identity Register (EIR) enthält eine Gerätedatenbank, welche die mobilen Stationen und die zugehörigen Nutzungsbedingungen registriert. Das Gateway-MSC (GMSC) übernimmt die Vermittlung von Verbindungen aus dem internen Netz in externe Netze, wie z. B. das Festnetz. Das Signalisierungssystem Nr. 7 (SS7) ist für den Signalisierungskanal zuständig. Auf diesem Kanal werden Verbindungsaufbau- und -abbau-Informationen übertragen.

Da GSM vor allem für die Sprachkommunikation entwickelt wurde, entstanden in Bezug auf die Datenkommunikation schnell große Defizite [AKHa03, 10 f.; Saut08, 87 f.]. Vor allem die geringe maximale Datenübertragungsrate von 9,6 kbit/s[8] (bzw. 14,4 kbit/s mit Circuit Switched Data) erwies sich als Hemmnis. Als Ergänzung des GSM-Standards wurde daher *High Speed Circuit Switched Data (HSCSD)* eingeführt. Dieses leitungsvermittelte Datenübertragungsverfahren ermöglicht durch Bündelung mehrere Kanäle Übertragungsrate von bis zu 57,6 kbit/s. Jedoch konnte auch HSCSD den Ansprüchen an ein steigendes Datenübertragungsvolumen nicht lange gerecht werden. Somit wurde die nächste GSM-Erweiterung implementiert, *General Packet Radio Services (GPRS)*. GPRS nutzt erstmals eine paketvermittelte Datenübertragung innerhalb des GSM-Netzes. Dies ermöglicht nicht nur eine höhere Datenübertragungsrate von maximal 171 kbit/s, sondern auch eine effektivere Nutzung der begrenzten Ressourcen der Luftschnittstelle. Um die Übertragungsgeschwindigkeit nochmals zu steigern, wurde eine weitere Ausbaustufe unter dem Namen *Enhanced Data Rates for GSM Evolution (EDGE)*[9] eingeführt. Mit EDGE wurde die maximale Datenübertragungsrate auf 474 kbit/s angehoben. Für die Ausbaustufen GPRS und EDGE sind allerdings aufwendige Erweiterungen an der Infrastruktur des Mobilfunknetzes erforderlich.

2.2.2 Universal Mobile Telecommunications System

Das Universal Mobile Telecommunications System (UMTS) ist nach GPRS eine weitere Entwicklungsstufe mobiler Telekommunikationsnetze [BSI08a, 35 ff.; Saut08, 149 ff.]. UMTS wurde auf Basis von GSM entwickelt. Es vereint die Eigenschaften eines leitungs-

[8] Die in diesem Abschnitt aufgeführten Datenraten entsprechen den theoretisch maximalen Datenraten. Die in der Praxis erzielten Datenraten liegen meist weit unter diesen theoretischen Datenraten.

[9] Enhanced Data Rates for GSM Evolution wird auch als EGPRS bezeichnet, normalerweise wird aber die Abkürzung EDGE verwendet.

vermittelten Sprachnetzes mit denen eines paketvermittelten Datennetzes. Abb. 2-2 zeigt den Aufbau eines UMTS-Mobilfunknetzes, die in weiten Teilen dem Aufbau eines GSM-Netzes sehr ähnlich ist. Die größten Unterschiede liegen eher in bestimmten Konzepten, weniger in zusätzlichen Hardwareelementen des UMTS-Netzes.

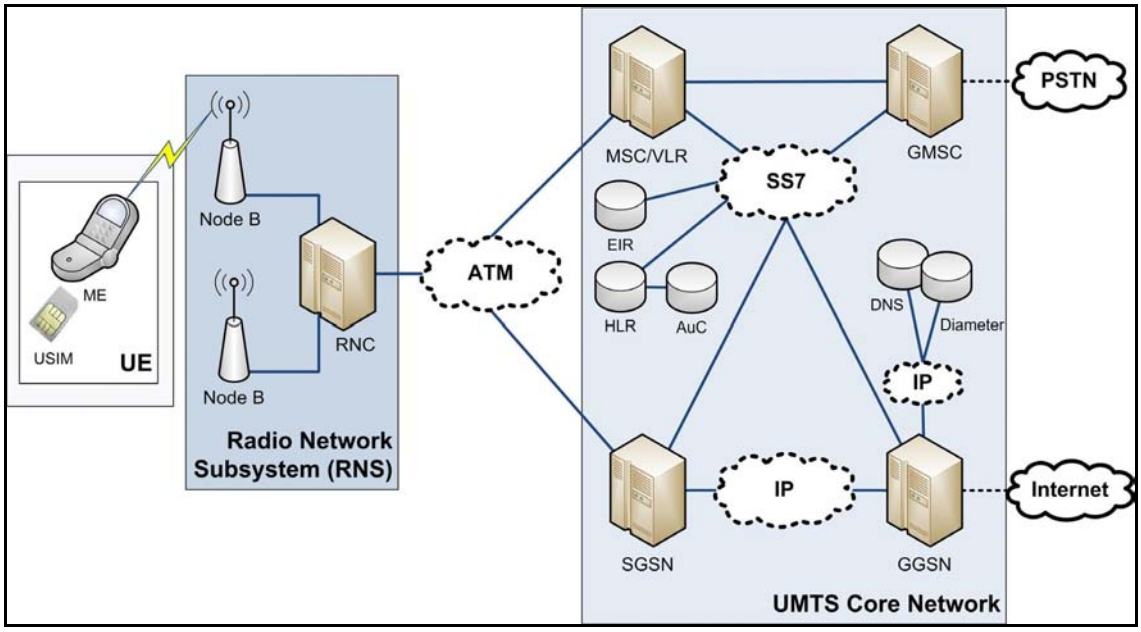

Abb. 2-2: Aufbau eines UMTS-Netzes [BSI08a, 35]

Das UMTS-Netz lässt sich in drei Teilbereiche untergliedern, das User Equipment (UE), das Radio Network Subsystem (RNS) und das UMTS Core Network [BSI08a, 35 ff.; Saut08, 149 ff.].

Beim *User Equipment (UE)* handelt es sich um die Einheit aus Mobile Equipment (ME) und dem Universal Subscriber Identity Module (USIM), welches der mobilen Station und der SIM-Karte im GSM-Netz entspricht.

Der *Radio Network Controller (RNC)* übernimmt im Radio Network Subsystem im Wesentlichen die gleichen Aufgaben wie der BSC im Base Station Subsystem des GSM-Netzes. Im UMTS-Mobilfunknetz wird zur Verschlüsselung der Datenübertragung zwischen dem mobile Equipment und dem Node B (Basisstation) der Algorithmus A5/3[10] verwendet, der auch unter der Bezeichnung „Kasumi“[11] bekannt ist.

Im *Core Network (CN)* gibt es im Vergleich zu GSM die zusätzlichen Komponenten SGSN und GGSN. Der Serving GPRS Support Node (SGSN) übernimmt für den paket-

[10] Siehe dazu Abschnitt 2.2.1.
[11] Kasumi stammt aus dem Japanischen und bedeutet verschleiern.

vermittelten Teil des UMTS-Netzes ähnliche Aufgaben wie das MSC für den leitungsvermittelten Bereich und stellt eine IP-basierte Schnittstelle zum GGSN bereit. Das Gateway GPRS Support Node (GGSN) ist für den Übergang in andere Paketnetze, wie z. B. das Internet zuständig. Hauptelemente des GGSN sind IP-Router, welche die Verkehrslenkung und die Weiterleitung von IP-Paketen übernehmen.

Weitere Unterschiede zum GSM-Netz ergaben sich durch die Einführung neuer Konzepte [BSI08a, 35 ff.; Saut08, 149 ff.]. Eine der gravierendsten Änderungen stellt das verwendete Multiplexverfahren Code Division Multiple Access (CDMA) dar. Dieses ermöglicht gegenüber dem Multiplexverfahren von GSM eine wesentlich höhere Datenübertragungsrate, da mehrere Teilnehmer die volle Bandbreite der Übertragungskanäle nutzen können. Weiterhin wird bei paketvermittelten Übertragungen ein dedizierter Kanal zwischen Teilnehmer und Netz vergeben. Dieser wird auch dann für eine bestimmte Zeit aufrechterhalten, wenn keine Daten gesendet werden. Dies macht eine ständige Neuzuweisung unnötig und vermeidet lange Verzögerungszeiten bei Datenübertragungen. Die Vergabe eines solchen dedizierten Kanals bringt auch für den Zellwechsel Vorteile. Wurde der Handover im GSM-Netz von der mobilen Station durchgeführt und sorgte somit für eine Unterbrechung von einer bis drei Sekunden, so wird im UMTS-Netz der Handover vom Netz unterbrechungsfrei durchgeführt. Außerdem wurde eine gegenseitige Authentifizierung zwischen dem UE und dem Mobilfunknetz eingeführt [Ecke08, 809 ff.]. Bei UMTS muss sich nicht nur der Teilnehmer bzw. das UE gegenüber dem Mobilfunknetz, sondern auch das Mobilfunknetz gegenüber dem Teilnehmer authentisieren. Dies geschieht mittels eines symmetrischen Challenge-Response-Verfahrens, bei dem zwischen UE und Mobilfunknetz Authentifizierungs-Vektoren ausgetauscht werden.

2.3 Mobile Endgeräte

2.3.1 Kategorien mobiler Endgeräte

„Mit mobilen Endgeräten ist es […] Benutzern möglich, Dienste über drahtlose Netze oder lokal verfügbare mobile Anwendungen zu nutzen.“ [BSI10] Diese Endgeräte besitzen eine eigene Stromversorgung, in der Regel einen Akkumulator, und können kabellos zu einem Netz Verbindung aufnehmen [BSI06, 5 ff.; Ruck06, 2 ff.]. Mobile Endgeräte unterscheiden sich in ihrer Größe und Leistungsfähigkeit. Dabei übernehmen sie mitunter komplette Auf-

gaben eines PC-Systems[12] oder aber sie sind auf spezielle Aufgaben, wie die Telefonie, beschränkt. Mobile Endgeräte lassen sich daher in verschiedene Geräteklassen einteilen, z. B. Mobiltelefone, Personal Digital Assistants (PDAs), Smartphones, Laptops und Tablet-PCs [BSI06, 6; Ruck06, 2 ff.; WaPi02, 50 ff.; Wiec02, 405]. Oftmals ist der Übergang zwischen den einzelnen Geräteklassen fließend, jedoch stellt jedes mobile Endgerät heute einen (leistungsfähigen) Computer dar, dessen Struktur grundsätzlich dem eines herkömmlichen PC-Systems ähnlich ist. In Abb. 2-3 sind die wichtigsten Hardwarekomponenten eines mobilen Endgerätes dargestellt.

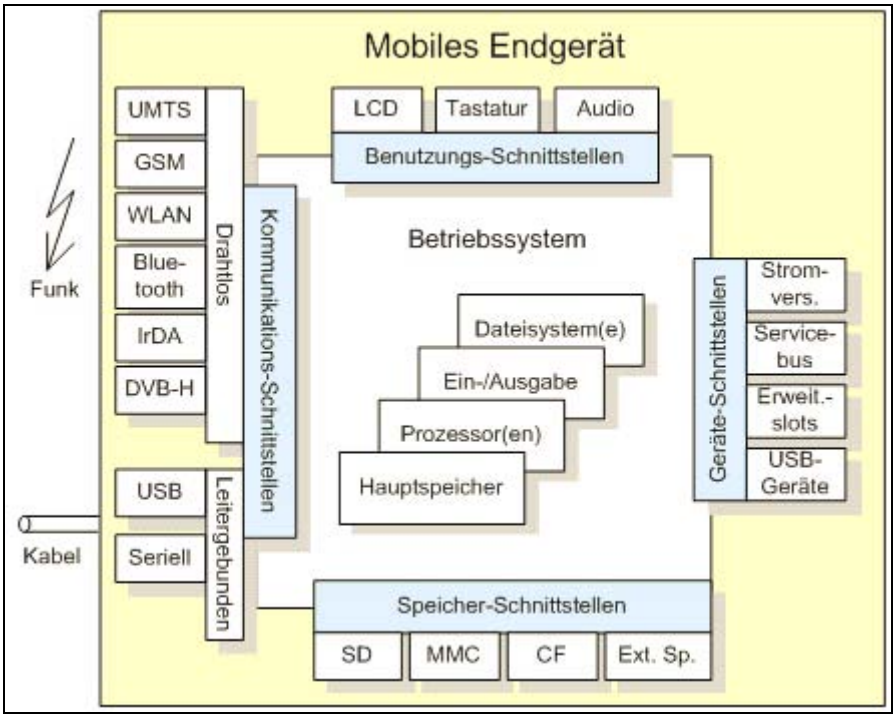

Abb. 2-3: Blockbild eines mobilen Endgerätes [BSI06, 6]

Der Übergang der als Hardware realisierten Teile des Endgerätes und der durch Software realisierten Teile ist fließend. Insbesondere im Kommunikationsbereich wird immer mehr der aufwendigen Hochfrequenzverarbeitung durch Software übernommen oder durch sie vorbereitet.

Laptops bzw. Notebooks sind tragbare PC-Systeme, welche lediglich in ihrer Größe reduziert wurden und auf geringen Stromverbrauch hin optimiert wurden [Wiec02, 406 f.]. Die Leistungsfähigkeit heutiger Laptops steht denen von Desktop-PCs nicht nach. Auch die verwendeten Komponenten, wie z. B. Prozessor, Grafikkarte und Festplatten sind denen

[12] In dieser Arbeit verstehen wir den Begriff PC-System stellvertretend für Desktop-PCs, Laptops und Notebooks.

der Desktop-PCs sehr ähnlich. Mit einer PCMCIA-UMTS-Datenkarte ausgerüstet oder mit einem Mobiltelefon als Modem verbunden, ist es Laptops beispielsweise möglich, von jedem Ort aus über ein Mobilfunknetz Verbindung mit dem Internet aufzunehmen.

Tablet-PCs sind laptopähnliche Geräte, welche statt mit Tastatur und Maus mit berührungsempfindlichen Bildschirmen ausgestattet sind, sich sonst jedoch kaum von einem Laptop unterscheiden [BSI06, 5 ff.].

Persönliche digitale Assistenten (PDA) wurden Anfang der 90er Jahre als „kleiner Computer“ entwickelt, der zunächst nur zum Termin- und Aufgabenverwaltung eingesetzt wurden [Ruck06, 3 f.; WaPi02, 52 ff.; Wiec02, 413 f.]. Dies beinhaltet Aufgaben bzw. Applikationen wie Kalender, Kontakte, Notizen und Nachrichtenverwaltung. Dabei ist das Bedienkonzept von Maus und Tastatur durch ein berührungsempfindliches Display und die Eingabe per Stift ersetzt. Ein weiteres Merkmal dieser Geräte ist das Eingeben von Texten per Schreiben auf dem Display, welches den Umgang mit diesen „kleinen Computern“ wesentlich erleichtern sollte. Waren PDAs zu Anfang ihrer Entwicklung mit geringer Rechenleistung ausgestattet, so steht ein heutiger PDA einem Laptop nur noch in wenigen Punkten nach. Aktuelle PDAs sind mit vielen Kommunikations- und Erweiterungsschnittstellen ausgerüstet. Bluetooth, Wireless LAN sowie diverse Erweiterungssteckplätze für Speicherkarten oder funktionserweiternde Steckkarten gehören zur Standardausstattung aktueller PDAs.

Mobiltelefone, deren flächendeckender Einsatz Anfang der 90er Jahre mit der Einführung von GSM begann, wurden mit der Zeit immer kleiner, leistungsfähiger und kostengünstiger [BSI06, 5 ff.; Ruck06, 4 f.; WaPi02, 52 ff.; Wiec02, 407 ff.]. Zu Beginn der Entwicklung konnte mit einem Mobiltelefon lediglich telefoniert werden, 1993 kam die Möglichkeit des Versandes von Textnachrichten[13] hinzu. Die neuesten Entwicklungen gehen dahin, aus Mobiltelefonen Multimediageräte zu machen, die mit vielen zusätzlichen Anwendungsmöglichkeiten, wie z. B. Digitalkamera, Videoplayer und MP3-Player ausgerüstet sind.

Smartphones stellen den fließenden Übergang zwischen PDAs und Mobiltelefonen dar [Ruck06, 4 f.; WaPi02, 52 ff.; Wiec02, 417]. Hier wird die Hauptfunktion des Mobiltelefons, das Telefonieren und Versenden von Textnachrichten, mit den Funktionen des PDAs

[13] Auch als SMS (Short Message Service) oder Kurzmitteilungen bezeichnet.

in einem Gerät verschmolzen. Ein Smartphone kann wie ein Mobiltelefon benutzt werden und bietet zusätzlich die Möglichkeit, Personal Information Manager Daten (PIM-Daten) zu verwalten, E-Mails zu versenden, einen Internetzugang zu nutzen oder zusätzliche Anwendungssoftware zu installieren. Auch bei diesen Geräten gehören GSM, UMTS, Wireless LAN, Bluetooth und Erweiterungssteckplätze zur Grundausstattung.

Trotz ihrer Ähnlichkeit unterscheiden sich alle Geräteklassen in der Qualität ihrer vorhandenen Komponenten und Schnittstellen [WaPi02, 53 ff.]. Konkrete Schwachstellen hängen daher stark von der betrachteten Geräteklasse bzw. vom betrachteten Gerät ab. Im weiteren Verlauf der Arbeit beschränken wir uns im Wesentlichen auf Mobiltelefone und Smartphones. Den Begriff „mobiles Endgerät“ verwenden wir als Synonym für Mobiltelefon bzw. Smartphone.

2.3.2 Betriebssysteme mobiler Endgeräte

Für mobile Endgeräte haben sich in den letzten Jahren eine ganze Reihe unterschiedlicher Betriebssysteme etabliert. Zu den bekanntesten Betriebssysteme gehören Apple iOS, BlackBerry, Linux, Palm OS, Symbian OS und Windows Mobile [Gart10]. In dieser Arbeit konzentrieren wir uns auf die Betriebssysteme BlackBerry, Symbian OS und Windows Mobile.

BlackBerry ist ein proprietäres Smartphone Betriebssystem der kanadischen Firma „Research in Motion“ (RIM). Es konnte sich erfolgreich in Nordamerika durchsetzen und wird seit 2003 auch in Europa angeboten [Wieh04, 74]. Es ist ein echtzeitfähiges Betriebssystem mit integrierten kryptografischen Mechanismen und der zentralen Vergabemöglichkeit von Sicherheitspolicies[14], welche durch das Gerät umgesetzt wird [BSI06, 9]. Hauptaugenmerk des BlackBerry-Betriebssystems in Verbindung mit der BlackBerry-Infrastruktur [Fox05, 647 f.] liegt auf den verschlüsselten Ende-zu-Ende E-Mail- und Intranetservices. Für zusätzliche Anwendungssoftware stehen Java-Programmierschnittstellen zur Verfügung.

Symbian OS ist ein offenes lizenzierbares Betriebssystem für Smartphones, welches für Sprach- und Datenanwendungen optimiert wurde [BSI06, 8; Wieh04, 74]. Es ist als Einzelbenutzersystem ausgelegt und nutzt preemptives Multitasking. Aktuelle Versionen von

[14] Sicherheitspolicies stellen ein Regelwerk dar, mit deren Hilfe genau definiert wird, was z. B. auf einem Endgerät einer bestimmten Benutzergruppe erlaubt ist und was nicht [BSI06, 33].

Symbian OS beinhalten Capability[15] basierten Zugriffsschutz für die Application Programming Interfaces (API), wodurch alle Zugriffe von Prozessen auf Daten und APIs kontrolliert werden. Außerdem enthält das System eine Kryptografiebibliothek und Mechanismen für ein Zertifikatsmanagement. Zusätzliche Anwendungssoftware lässt sich über Java- und C++-Programmierschnittstellen realisieren.

Windows Mobile ist das Betriebssystem von Microsoft für PDAs und Smartphones. Bezüglich der Benutzeroberfläche ist es stark an Windows für PC-Systeme angelehnt [Alby08, 109 f.]. Im Betriebssystem integriert sind angepasste Versionen der typischen Microsoft Office Anwendungen. Das System ist mit Speicherschutztechniken ausgestattet und verwendet preemptives Multitasking [BSI06, 8]. Das integrierte Dateisystem unterscheidet zwischen Benutzer- und geschützten Systemdateien, kann aber auch durch Dateisysteme anderer Hersteller, die zusätzliche Sicherheitsmaßnahmen unterstützen, ergänzt werden. Außerdem stehen Kryptografie- und Authentisierungsmechanismen zur Verfügung. Seit der Version Windows Mobile 2005 können die Rechte eines Benutzers durch Security Roles[16] beschränkt bzw. definiert werden [Enz07]. Security Policies (z. B. Security Policy 4102 - „erlaube -“ oder „verbiete die Ausführung unsignierter Anwendungen“[17]) regeln zusätzlich die Sicherheitseinstellungen des mobilen Endgerätes. Anwendungssoftware wird unter anderem in C# und C/C++ geschrieben und kann mittels Zertifikaten unterschiedliche Ausführungsrechte (normal, privilegiert) erhalten.

2.4 Abgrenzung des Betrachtungsgegenstandes

Der Betrachtungsgegenstand in dieser Arbeit ist die Datenübertragung von einem mobilen Endgerät über ein Mobilfunknetz und das Internet in ein lokales Unternehmensnetzwerk (vgl. Abb. 1-1). Für die systematische Untersuchung einer derartigen Datenübertragung haben wir zunächst ein Strukturierungsmodell entwickelt.

In Anlehnung an das Modell der Sicherheit in der Informationsverarbeitung von Stelzer [Stel93, 26 ff.] unterscheiden wir hierzu einerseits folgende Betrachtungsebenen: Infrastrukturebene, technische Ebene (mit Hard- und Software) sowie organisatorische und Nutzer-Ebene. Andererseits differenzieren wir anhand der Systeme, die an der Daten-

15 Capabilitys sind Berechtigungen. Diese Berechtigungen sind in entsprechende Klassen eingeteilt und erlauben den Zugriff von Programmen auf bestimmte API [Enz07, Abschnitt 2.2].

16 Vgl. zur Auflistung der zur Verfügung stehenden Security Roles [Micr10a].

17 Vgl. zur Auflistung der zur Verfügung stehenden Security Policies [Micr10b].

übertragung beteiligt sind: mobiles Endgerät, Mobilfunknetz (GSM/UMTS), Internet und lokales Unternehmensnetzwerk.[18] Das anhand dieser beiden Kriterien entstehende Modell für die Strukturierung einer mobilen Datenübertragung ist in Abb. 2-4 dargestellt.

			Systeme einer mobilen Datenübertragung		
			mobiles Endgerät	**Mobilfunknetz (GSM/UMTS)**	**Internet**	**lokale Netzwerke**
Betrachtungsebenen	**Organisatorische und Nutzer-Ebene**		Verhalten des Nutzers (z. B. (un)beabsichtigte Fehlhandlungen, Unkenntnis über Sicherheitsrisiken, Verlust)	Verhalten des Nutzers (z. B. (un)beabsichtigte Fehlhandlungen, Unkenntnis über Sicherheitsrisiken)	Verhalten des Nutzers (z. B. (un)beabsichtigte Fehlhandlungen, Unkenntnis über Sicherheitsrisiken)	Verhalten des Nutzers (z. B. (un)beabsichtigte Fehlhandlungen, Unkenntnis über Sicherheitsrisiken)
			organisatorische Regelungen (z. B. Regelungen über die Nutzung von mobilen Endgeräten, Schulungen in Sicherheitsbelangen)	org. Regelungen (z. B. Regelungen über den Umgang mit sicherheitsrelevanten Elementen, Schulungen in Sicherheitsbelangen)		org. Regelungen (z. B. Regelungen über den Umgang mit sicherheitsrelevanten Elementen, Schulungen in Sicherheitsbelangen)
	technische Ebene	**Software**	Anwendungen (z. B. Browser, E-Mailprogramme, ERP-Clients, CRM-Clients)	Verschlüsselungsalgorithmen (z. B. A5, A8)	Anwendungen (z. B. DHCP-Server, DNS-Server, Proxy-Server)	Anwendungen (z. B. Browser, ERP-Systeme, E-Mailprogramme)
			Betriebssysteme (z. B. Symbian OS, Windows Mobile, BlackBerry, Mac OS)	Betriebssystem und Software zum Betreiben der Systeme eines Mobilfunknetzes	Server-Betriebssysteme (z. B. Windows, Linux)	Betriebssysteme (z. B. Windows, Linux, Mac)
		Hardware	(reine) PDA (z. B. HTC, Hewlett-Packard, Asus)	Infrastruktur des Mobilfunknetzes (z. B. Mobilfunksendesystem (BSS), Vermittlungssystem (NSS oder CSS))	Hardwareinfrastruktur (z. B. Server)	Hardwareinfrastruktur (z. B. Arbeitsplatzrechner, Server)
			(reine) Mobiltelefone (z. B. Nokia, Samsung, Motorola)		Kommunikationsinfrastruktur (z. B. Gateways, Router)	Kommunikationsinfrastruktur (z. B. Router, Switch, Firewall)
			Smartphones (z. B. Nokia, HTC, RIM, Sony, Samsung)			
			Mobilfunkkarten für tragbare PCs (z. B. PCMCIA-Datenkarten, UMTS-USB-Stick)			
	Infrastrukturebene		Kommunikationsschnittstellen mobiler Endgeräte (z. B. GSM, UMTS, WLAN, Bluetooth, IrDA)	Übertragungsdienste und -protokolle (z. B. GPRS, HSDPA, SMS, WAP)	Kommunikationsprotokolle (z. B. TCP/IP)	Kommunikationsprotokolle (z. B. TCP/IP)

Legende: Bereiche/Elemente, die in dieser Arbeit im Mittelpunkt stehen

Abb. 2-4: Ebenenmodell zur Strukturierung des Betrachtungsgegenstandes[19]

Hinsichtlich der im Modell unterschiedenen Bereiche haben wir für die weiteren Untersuchungen folgende Eingrenzungen vorgenommen:

- Als *mobile Endgeräte* sind Smartphones, deren Kommunikationsschnittstellen, Betriebssysteme und Anwendungen exemplarisch zu untersuchen. Bei den Betriebssysteme konzentrieren wir uns auf BlackBerry, Symbian OS und Windows Mobile (vgl. hierzu auch Abschnitt 2.3.2).
- Das Nutzerverhalten und die organisatorischen Regelungen sind Gegenstand unserer Betrachtungen. Es werden Bedrohungen berücksichtigt, die durch unbewusstes oder absichtlich nachlässiges Handeln des Nutzers entstehen.
- In Bezug auf das *Mobilfunknetz* beschränken wir uns auf eine allgemeine Betrachtung der Mobilfunkstandards GSM und UMTS, da sie die technische Basis für da-

[18] Für eine ausführlichere Beschreibung der Systeme vgl. Abschnitt 3.2.

[19] Alle farblich hervorgehobenen Bereiche sind Gegenstand der weiteren Betrachtungen.

rauf aufbauende Übertragungsdienste und -protokolle darstellen. Des Weiteren untersuchen wir Mobilfunk- und Datendienste.

- Das *Internet* als Transportnetz zwischen Mobilfunknetz und lokalem Unternehmensnetzwerk ist größtenteils nicht Gegenstand der weiteren Diskussionen, da hierzu bereits umfassende Untersuchungen zu Sicherheitsbedrohungen und Sicherheitsmaßnahmen existieren, vgl. z. B. [FRRö00; Raep01].
- Im *lokalen Unternehmensnetzwerk* werden wir nur Sicherheitsbedrohungen und -maßnahmen betrachten, die für die direkte Anbindung von mobilen Endgeräten in das Netzwerk von Relevanz sind. Zu allen weiteren (regulären) Sicherheitsaspekten in lokalen Unternehmensnetzwerken existiert bereits eine Vielzahl von Publikationen, so dass wir diese im Folgenden nicht weiter betrachtet werden, vgl. z. B. [Alex06; Hunt98].

Entsprechend der getroffenen Eingrenzungen haben wir die von uns betrachteten Bereiche bzw. Elemente einer mobilen Datenübertragung in Abb. 2-4 farblich hervorgehoben. Alle weiteren Bereiche bzw. Elemente stehen nicht im Fokus dieser Arbeit.

3 Bedrohungsanalyse

3.1 Vorgehensweise

Eine *Bedrohungsanalyse* ermöglicht die systematisch Ermittlung relevanter organisatorischer, technischer und benutzerbedingter Bedrohungen, die zu Schäden an IT-Systemen (oder Systemteilen) führen können [BSI92, 52; Ecke08, 170 f.; Schn99]. Hierzu ist es zunächst notwendig, die bedrohten Elemente der IT-Systeme zu erfassen und diese gegebenenfalls in Teilelemente zu detaillieren, falls Bedrohungen nur auf diese Teilelemente einwirken. Eine Bewertung der Elemente und Bedrohungen findet nicht statt.

Die möglichst vollständige Ermittlung der Bedrohungen eines IT-Systems stellt eine schwierige Aufgabe dar [Schn04, 279] und erfordert fundierte Kenntnisse über Sicherheitsprobleme und Schwachstellen der zu betrachtenden IT-Systeme. *Bedrohungsbäume*[20] helfen relevante Bedrohungen systematisch zu ermitteln und darzustellen [Ecke08, 172 f.;

[20] Bedrohungsbäume werden häufig auch als Angriffsbäume bezeichnet [Schn99; Schn04, 309 f.].

Schn04, 309 f.]. Die Bedrohungen werden hierzu in einer Baumstruktur abgebildet, wobei jede Bedrohung als Wurzelknoten definiert wird, der wiederum in diverse Bedrohungsteilziele untergliedert ist [Schn99; Wurs04, 79 ff.]. Diese werden auch als Blattknoten bezeichnet. Der Baum wird rückwärts, vom eigentlichen (Haupt-)Bedrohungsziel zu den Teilzielen, Ebene für Ebene aufgebaut. Müssen mehrere Teilziele gemeinsam erfüllt werden, um ein Bedrohungsziel zu erreichen, wird dies mit Hilfe einer UND-Verbindung abgebildet. ODER-Verbindungen werden bei alternativen Zwischenzielen verwendet. Bedrohungsbäume werden zur Gewährleistung der Übersichtlichkeit meist grafisch aufbereitet [Wurs04, 82]. Werden diese zu komplex, können sie in Bedrohungsteilbäume nach Teilzielen untergliedert werden. In Abb. 3-1 haben wir die in der Arbeit verwendete grafische Darstellung an einem Beispiel exemplarisch dargestellt. Nicht weitere gekennzeichnete Verbindungen stellen ODER-Verbindungen dar, lediglich UND-Verbindungen werden gesondert beschriftet.

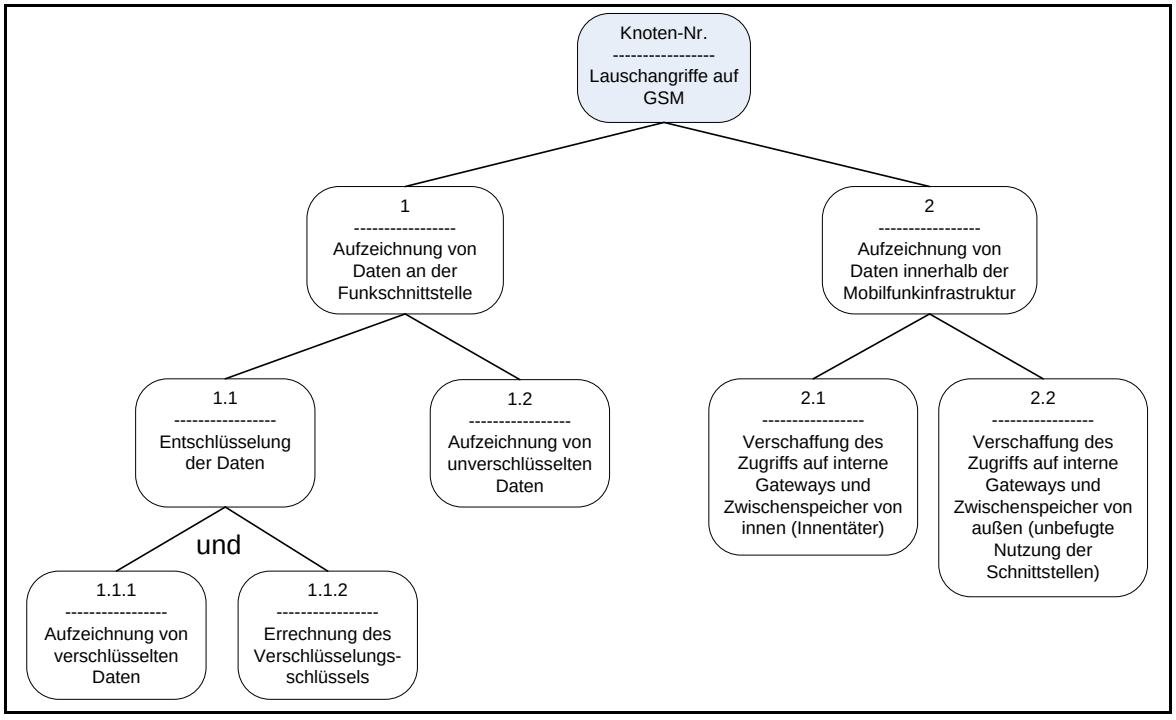

Abb. 3-1: Bedrohungsbaum (grafisch)

Für die Darstellung komplexer Bedrohungsbäume wird auch oft eine textuelle Beschreibungsform verwendet [Ecke08, 176 f.; Schn04, 315 f.]. Hierbei werden die ODER- und UND-Teilbäume mit Hilfe von Texteinrückungen dargestellt. Beginnend mit der Wurzel des Baumes, dem Hauptbedrohungsziel, werden alle direkten Nachfolger der Wurzel auf einer Beschreibungsebene aufgelistet. Alle weiteren Ebenen werden durch erneutes Einrü-

cken des Textes gekennzeichnet. In Abb. 3-2 ist der exemplarische Bedrohungsbaum aus Abb. 3-1 in der textuellen Form abgebildet.

Ziel: Lauschangriffe auf GSM
- **Subziel 1:** Aufzeichnung von Daten an der Funkschnittstelle (ODER)
  - Subziel 1.1: Entschlüsselung der Daten (ODER)
    - Subziel 1.1.1: Aufzeichnung von verschlüsselten Daten (UND)
    - Subziel 1.1.2: Errechnen des Verschlüssungsschlüssels
  - Subziel 1.2: Aufzeichnung von unverschlüsselten Daten (ODER)
- **Subziel 2:** Aufzeichnung von Daten innerhalb der Mobilfunkinfrastruktur (ODER)
  - Subziel 2.1: Verschaffung des Zugriffs auf interne Gateways und Zwischenspeicher von innen (Innentäter)
  - Subziel 2.2: Verschaffung des Zugriffs auf interne Gateways und Zwischenspeicher von außen (unbefugte Nutzung von Schnittstellen)

Abb. 3-2: Bedrohungsbaum (textuell)

3.2 Ermittlung der sicherheitsrelevanten Elemente

Wie in den Abschnitten 1.1 und 2.4 bereits dargestellt, sind an einer mobilen Datenübertragung mehrere Systeme sowie die Nutzer dieser Systeme beteiligt. Zur Ermittlung der sicherheitsrelevanten Elemente ist es notwendig, die beteiligten Systeme detaillierter zu betrachten:

- Das mobile Endgerät, welches den Start- oder Endpunkt einer mobilen Datenübertragung darstellt, ist eines der sicherheitsrelevanten Elemente. Dieses untergliedern wir zusätzlich in Hardware- und Softwareelemente.
- In einem Mobilfunknetz (GSM/UMTS) gibt es verschiedene Elemente (z. B. Funkstrecke, Basisstationen, Mobile Switching Center, Gateway-MSC, Gateway GPRS Support Node), die wir als sicherheitsrelevante Elemente betrachten.
- Das Internet als Transportweg zwischen dem Mobilfunknetz und dem lokalen Unternehmensnetzwerk besteht aus Servern, Routern, Gateways und Kabelverbindungen, die durch Ausnutzung von Schwachstellen zu Angriffspunkten werden können und somit sicherheitsrelevante Elemente darstellen.
- In lokale Unternehmensnetzwerke betrachten wir Arbeitsstationen, Servern, Routern und Kabelverbindungen als sicherheitsrelevante Elemente.

- Der Nutzer muss für eine Betrachtung der Bedrohungen einer mobilen Datenübertragung mit seinem Handeln berücksichtigt werden, da auch durch sein wissentliches oder unwissentliches Fehlverhalten Bedrohungen entstehen können.

3.3 Ermittlung von Bedrohungen

Bei der mobilen Datenübertragung existieren viele Bedrohungen und Schwachstellen, die durch Angriffe[21] gezielt ausgenutzt werden und zu einer Verletzung der Sicherheit führen können [BSI06, 17 ff.; BSI08a, 21 ff., 33 ff., 43 ff.]. Die dadurch entstehenden Gefährdungen können zum Verlust von Vertraulichkeit, Integrität und Verfügbarkeit führen.[22]

Angriffe lassen sich in zwei Hauptkategorien unterteilen: unbeabsichtigte[23] und beabsichtigte. Im Folgenden konzentrieren wir uns auf beabsichtigte Angriffe. Bei diesen werden wiederum aktive und passive Angriffe unterschieden [BSI92, 317; Ecke08, 17; Schn04, 106; Schw05, 4]. Passive Angriffe[24] dienen der unbefugten Informationsbeschaffung und bedrohen die Vertraulichkeit, nicht aber die Verfügbarkeit oder die Integrität. Aktive Angriffe[25] hingegen sind auf Veränderung, Zerstörung oder Blockierung von Informationen und Ressourcen ausgerichtet und bedrohen die Vertraulichkeit, Integrität und/oder Verfügbarkeit.

Im folgenden Abschnitt haben wir die möglichen Bedrohungen einer mobilen Datenübertragung anhand bekannter, gut dokumentierter Angriffe im mobilen Bereich zusammengestellt.[26] Aufgeführt werden auch Bedrohungen, die nicht direkt zur Gefährdung einer mobilen Datenübertragung führen, aber z. B. zu deren Vorbereitung dienen. Kategorisiert haben wir die Bedrohungen anhand der in Tab. 3-1 dargestellten Angriffskategorien und -typen.

---

21 Angriffe sind Aktionen/Vorgänge, deren Folge oder Ziel eine Verletzung der Sicherheit ist. Personen, die derartige Aktionen/Vorgänge durchführen, werden als Angreifer bezeichnet. Sie verfolgen ein bestimmtes, meist illegales Ziel. Angreifer lassen sich in verschiedene Angreifer-Typen einteilen [BSI09, 45; Ecke08, 19 ff.; Schn04, 39 f.].

22 Vgl. zu primären und sekundären Konsequenzen sicherheitsgefährdender Ereignisse und Beeinträchtigungen von Sicherheitszielen z. B. [Stel93, 34 ff.].

23 Unbeabsichtigte (zufällige) Angriffe sind vom Angreifer nicht gewollt. Sie werden zwar von ihm ausgelöst, jedoch unbewusst, zum Beispiel: ein defektes elektrisches Gerät wird zum Störsender. Witt bezeichnet derartige Angriffe auch als zufällige Ereignisse oder unbeabsichtigte Fehler [Witt96, 67 f.].

24 Typische passive Angriffe sind z. B. das Auffangen elektromagnetischer Abstrahlungen bzw. Übertragungen, das Abhören von Leitungen und die Verkehrsflussanalyse [Ecke08, 18; Schw05, 4].

25 Typische aktive Angriffe sind z. B. das funktionale Stören von Systemen oder Systemteilen (z. B. DoS-Attacken) und das Einfügen, Löschen oder Modifizieren von Inhalten einer Datenübertragung [Ecke08, 18; Schw05, 4].

26 Durch zukünftige Entwicklungen sind weitere Arten und Motivationen von Angriffen denkbar, vor allem weil die Nutzung und Akzeptanz von mobilen Endgeräten sowohl im privaten als auch im unternehmerischen Bereich ansteigt.

Angriffskategorie	Angriffstyp
Passiv	Erkundungsangriffe Lauschangriffe
Aktiv	Verfügbarkeitsangriffe Manipulationsangriffe weitere Angriffe

Tab. 3-1: Angriffskategorisierung/-typen

Bei *Erkundungsangriffen* (engl. sniffing, snooping, footprinting, gathering) versuchen Angreifer, die Datenkommunikation in einem Netzwerk mitzuhören, aufzuzeichnen und anschließend gezielt auszuwerten [KrWe07, 393; SACO06, 12 ff.; Zieg08, 5]. Dadurch können Informationen über das Netzwerk selbst (z. B. Anzahl und Art der Endgeräte, verwendete IP-Bereiche, verwendete Verschlüsselung) und seine Teilnehmer (z. B. Verhalten, Interessen, Gewohnheiten) gewonnen werden. Erkundungsangriffe dienen häufig zur Vorbereitung weiterer Angriffe.

Lauschangriffe (engl. eavesdropping) zielen darauf ab, die gesendeten (unverschlüsselten) Daten (z. B. Inhaltsdaten, Passwörter) innerhalb eines Netzwerkes unbemerkt für eine spätere unbefugte Nutzung aufzuzeichnen [Eren07, 105 f.; Wang09, 3].

Durch *Verfügbarkeitsangriffe* (engl. denial-of-service attack) soll die Nutzung bestimmter Ressourcen und Dienste eines Netzwerkes eingeschränkt bzw. verhindern werden. Mittels Störquellen (z. B. einem Störsender) oder durch eine Überflutung mit Anfragen werden Ressourcen oder Dienste eines Netzwerkes so überlastet, dass sie für befugte Nutzer nicht mehr zur Verfügung stehen [Ecke08, 111; KrWe07, 29].

Mit *Manipulationsangriffen* können mehrere Ziele verfolgt werden. Z. B. kann ein Angreifer versuchen, eine falsche Identität vorzutäuschen (engl. masquerading), um unbefugten Zugang zu Daten zu erlangen oder um einen Kommunikationspartner zu täuschen [Schä03, 8]. Das Intrigieren (engl. tampering) kann ein weiteres Ziel sein. Hierbei werden Nachrichten bei ihrer Übertragung unbemerkt verändert. Wiederholen und Verzögern (engl. replay and delay) sind ebenfalls Ziele von Manipulationsangriffen. Dabei wird die Sendung der Nachricht wiederholt durchgeführt oder eine Nachricht abgefangen und unverändert, aber verzögert weitergesendet.

3.3.1 Bedrohungen für Global System for Mobile Communications (GSM)

3.3.1.1 Erkundungsangriffe

Durch Erkundungsangriffe ist es einem Angreifer möglich, Informationen über GSM-Teilnehmer bzw. deren mobile Endgeräte zu sammeln. Hierzu zählen vor allem die Identifikation des mobilen Endgerätes anhand der IMSI-Nummer bzw. IMEI-Nummer und die Bestimmung des Aufenthaltsortes des Endgerätes.

Ein Mobilfunkbetreiber kann aus der technischen Gegebenheit heraus, dass der Standort (die Funkzelle, in der sich ein mobiles Endgerät aufhält) eines mobilen Endgerätes dem Mobilfunknetz jederzeit bekannt sein muss, um die ein- und ausgehenden Verbindungen des mobilen Endgerätes zu realisieren, in Erfahrung bringen, wo sich das mobile Endgerät aufhält. Innentäter[27] können so den Aufenthaltsort eines bestimmten Teilnehmers in Erfahrung bringen.

Mobiltelefonortung ist ebenfalls über bestimmte Dienste im Internet[28] für jedermann möglich [NETZW09]. Es muss lediglich die Telefonnummer bekannt sein. Um der Möglichkeit der Ortung zuzustimmen, versenden die Anbieter meistens eine SMS, die die Zustimmung zur Ortung einholt, jedoch sind die Betreiber dazu gesetzlich nicht verpflichtet [BSI08a, 27]. Ist kein Anbieter auffindbar, der die Ortung auch ohne vorherige Zustimmung des Mobilfunknutzers vornimmt, so muss es einem Angreifer lediglich gelingen, das mobile Endgerät kurzzeitig in seinen Besitz zu bringen, um die Rückfrage zu bestätigen. Danach ist es möglich, zu ermitteln, in welcher Funkzelle sich das mobile Endgerät aufhält.

Ein bekanntes Hilfsmittel für Erkundungsangriffe ist der IMSI-Catcher [Fox02, 213]. Der IMSI-Catcher ist in der Lage, sich als GSM-Basisstation auszugeben [BSI08a, 21], da sich im GSM-Standard lediglich das mobile Endgerät bzw. die SIM-Karte gegenüber dem Mobilfunknetz authentisieren muss. Eine Authentisierung des Mobilfunknetzes gegenüber dem mobilen Endgerät ist nicht vorgesehen. Da ein mobiles Endgerät sich immer mit der Basisstation verbindet, welche die beste Verbindungsqualität ermöglicht, verbinden sich in unmittelbarer Nähe befindliche mobile Endgeräte mit dem IMSI-Catcher. Dieser ist dann in der Lage, IMSI-Nummern und IMEI-Nummern der mit ihm verbundenen Endgeräte

---

[27] Innentäter sind Personen, welche in einem Unternehmen oder in einer Behörde arbeiten und aufgrund ihrer Position/Stellung besondere Rechte besitzen und damit leichteren Zugriff z. B. auf sicherheitskritische Daten haben. Diese besonderen Rechten bzw. Zugangsmöglichkeiten können sie für Angriffe nutzen.

[28] Ein Internet-Anbieter zur Ortung von mobilen Endgeräten ist z. B. http://www.handy-ortung.org.

auszulesen. Der Aufenthaltsort eines mobilen Endgerätes kann vom Mobilfunkprovider lediglich auf die Funkzelle, in der sich das mobile Endgerät aktuell befindet, genau bestimmt werden. Eine wesentlich genauere Standortbestimmung ist hingegen mit Hilfe des IMSI-Catchers möglich, da dieser aufgrund seiner geringeren Sendeleistung [Fox02, 213] den Aufenthaltsort besser eingrenzen kann.[29]

3.3.1.2 Lauschangriffe

Daten, welche mittels Funktechnik übertragen werden, sind grundsätzlich der Gefahr ausgesetzt, dass sie relativ leicht von unbefugten Dritten aufgezeichnet werden können. Da zumindest ein Teil der GSM-Kommunikation über die so genannte Funkschnittstelle realisiert wird, ist dies für GSM eine Quelle für Bedrohungen. Die über die GSM-Funkschnittstelle übertragenen Daten sind zwar verschlüsselt, jedoch können Fehler in den Verschlüsselungsalgorithmen oder deren Implementierung[30] dafür sorgen, dass die Verschlüsselung gebrochen wird und somit die verschlüsselten Daten entschlüsselt werden.

Eine solche Möglichkeit zeigte die Hackergruppe THC[31] mit einem Time-Memory-Trade-Off-Angriff (TMTO-Angriff [Oech03, 1]) auf den Verschlüsselungsalgorithmus A5/1 [Rütt07]. Dazu ist es lediglich notwendig, das erste verschlüsselte Datenpaket einer Verbindung aufzuzeichnen. Analysen des GSM-Verbindungsaufbaus ergaben, dass der Inhalt des ersten verschlüsselten Datenpaketes fast vollständig vorhersehbar ist und immer aus vornehmlich nutzlosen, konstanten Füllbits besteht. Anschließend konnte der Schlüssel zur Verbindungsverschlüsselung errechnet werden, um somit die aufgezeichneten verschlüsselten Daten zu entschlüsseln.

Die Aufzeichnung von Verbindungen ist auch mittels eines IMSI-Catchers möglich, wenn dieser zuvor das mobile Endgerät dazu veranlasst hat, die Verschlüsselung der Verbindungsdaten zu deaktivieren[32].

---

29 In den Bedrohungsbäumen unterscheiden wir daher zwischen „Ermittlung des ME-Standortes (Zellortung)“ und „Ermittlung des ME- Standortes (Signalstärke)“. Bei der erst genannten Bezeichnung handelt es sich um die Ortung mittels des Mobilfunkproviders und bei der zweit genannten Bezeichnung um die Ortung mittels des IMSI-Catchers.

30 GSM-Mobilfunknetzbetreiber sind nicht gezwungen, eine bestimmte Implementierung des Verschlüsselungsalgorithmus A5 zu verwenden. Sie sind lediglich dazu angehalten, eine geeignete Implementierung zu wählen. Es können daher je nach Betreiber unterschiedliche Schwachstellen auftreten [BSI08a, 23].

31 The Hacker's Choice ist eine nicht kommerziell orientierte Gruppe von internationalen IT-Spezialisten, die sich IT-Sicherheit befassen [THC11].

32 Zur Deaktivierung der Verschlüsselung vgl. Abschnitt 3.3.1.4.

Des Weiteren ist es denkbar, dass unbefugte Dritte als so genannte Innentäter an vertrauliche Daten gelangen. Die im GSM-Netz übertragenen Daten werden vom mobilen Endgerät nur auf dem Weg bis zur nächsten Basisstation verschlüsselt [Ecke08, 798]. Die empfangende Basisstation entschlüsselt diese und leitet sie zur weiteren Bearbeitung an das Network Subsystem weiter. In der Mobilfunkinfrastruktur liegen die Daten ab dem BTS unverschlüsselt vor und könnten von einem Innentäter mit entsprechenden Zugangsmöglichkeiten aufgezeichnet werden.

Eine weitere Möglichkeit zur unbefugten Aufzeichnung der gesendeten Daten stellen die für Ermittlungsbehörden geschaffenen Schnittstellen zur Verbindungsüberwachung dar. Mobilfunkbetreiber sind gesetzlich verpflichtet, den Behörden derartige Überwachungsmöglichkeiten zur Verfügung zu stellen.[33] Eine solche Schnittstelle wurde 1999 im Zuge der Aktualisierungen des GSM-Standards durch die Standardisierungsinitiative 3rd Generation Partnership Project (3GPP) geschaffen [BSI08a, 22]. Da eine derartige Schnittstelle existiert, ist es denkbar, dass sich unter bestimmten Bedingungen auch unbefugte Dritte darauf Zugriff verschaffen können. Ein solcher Fall wurde zum Beispiel in Griechenland bekannt [Fisc08].

3.3.1.3 Verfügbarkeitsangriffe

Es gibt verschiedene Möglichkeiten, das Zustandekommen einer Verbindung zu verhindern oder eine Verbindung abbrechen zu lassen. Eine Möglichkeit der Blockierung bietet der IMSI-Catcher, welcher durch seine technische Beschränkung immer nur eine Verbindung eines mobilen Endgerätes weiterleitet, sämtliche anderen „gefangenen“ mobilen Endgeräte blockiert. Auch ist es denkbar, dass das vermeintlich weitergeleitete „gefangene“ mobile Endgerät an der Kommunikation gehindert wird [Fox02, 214].

Mittels eines Störsenders (GSM-Jammer) ist es ebenso möglich, in begrenzter Reichweite[34] den GSM-Funk zu stören, so dass keine Verbindungen aufgebaut werden können [neue09, SESP11]. Dazu ist es allerdings notwendig, dass der Angreifer den Aufenthaltsort des zu blockierenden mobilen Endgerätes kennt.

Mobilfunkbetreiber können Anschlüsse ihrer Kunden sperren, wenn diese z. B. ihre Rechnung nicht bezahlt haben oder das mobile Endgerät bzw. die SIM-Karte als verloren/ge-

[33] Vgl. dazu §§ 100a, 100b Strafprozessordnung [StPO11].

[34] Je nach Modell ist die Reichweite dieser Sender von wenigen Metern bis etwa einem Kilometer möglich, vgl. hierzu z. B. [SESP11].

stohlen gemeldet wurde. Dann ist es mit der gesperrten SIM-Karte nicht mehr möglich, eine Verbindung aufzubauen. Auch dieser Mechanismen könnte sich ein unbefugter Dritter bemächtigen und somit eine Kommunikation verhindern.

3.3.1.4 Manipulationsangriffe

Da sich im GSM-Standard lediglich das mobile Endgerät gegenüber dem Netz authentisieren muss, nicht aber das Netz gegenüber dem Endgerät [BSI08a, 19], sind Bedrohungen durch Maskierungsangriffe bzw. so genannte Man-in-the-Middle-Angriffe [Schn04, 106] denkbar. Es ist, wie bereits in Abschnitt 3.3.1.1 beschrieben, möglich, ein Gerät wie den IMSI-Catcher so zu maskieren, dass dieser eine GSM-Basisstation imitiert [Fox02, 214]. Der IMSI-Catcher ist dann in der Lage, mittels spezieller Kommandos, die sonst dem Mobilfunknetz vorbehalten sind, die Verschlüsselung der Kommunikation zu deaktivieren und Verbindungen aufzuzeichnen.

Die Vortäuschung einer vermeintlich vertrauenswürdigen Identität ist auch durch das Klonen von SIM-Karten möglich [BSI08a, 24; WeLu99, 3]. Ein Angreifer kann so die Identität eines anderen Mobilfunkteilnehmers annehmen und andere zur Übermittlung von sensiblen Daten verleiten. Für einen solchen Angriff ist allerdings der physische Zugriff auf die zu klonende SIM-Karte und die Kenntnis der PIN der SIM-Karte notwendig. Dieser Angriff ist außerdem nur mit SIM-Karten möglich, die vor 2001 ausgegeben wurden [Back07; BSI08a, 24].[35]

3.3.2 Bedrohungen für General Packet Radio Service (GPRS)

Grundsätzlich gelten für GPRS ähnliche Bedrohungen wie für GSM[36], da GPRS ein Teil des GSM-Netzwerkes ist [BSI08a, 33]. GPRS ermöglicht den Teilnehmern permanent, mit einer eigenen IP-Adresse online zu sein. Dadurch kommen verstärkt Angriffe aus dem Internet zu den bereits aufgeführten Bedrohungen hinzu [Ecke08, 806].

---

[35] Das Klonen von SIM-Karten ist nur mit SIM-Karten möglich, die den COMP128-Algorithmus in der Version 1 verwenden. Diese erste Version wurde mittlerweile durch die Nachfolgeversionen 2 bzw. 3 abgelöst. Bei den Nachfolgeversionen ist es nicht mehr möglich, den geheimen Schlüssel Ki auszulesen und die SIM-Karte zu klonen. Der COMP128-Algorithmus Version 1 wurde 2001 abgelöst. SIM-Karten, die nach diesem Zeitraum ausgegeben wurden, sind daher nicht mehr gefährdet [Back07; RaEf08, 151].

[36] Der im Abschnitt 3.3.1.2 aufgeführte Time-Memory-Trade-Off-Angriff zur Brechung des Verschlüsselungsalgorithmus A5/1 ist für GPRS nicht anwendbar, da GPRS den Verschlüsselungsalgorithmus A5/3 verwendet, der auch in UMTS-Netzen Verwendung findet und als (noch) sicher gilt.

3.3.2.1 Manipulationssangriffe

Zu denen über das Internet ausgeführten Angriffen zählt z. B. die Übermittlung von Schadsoftware[37]. Schadsoftware kann als Anhang von E-Mails an das mobile Endgerät übermittelt werden oder innerhalb einer manipulierten Webseite als aktiver Inhalt verborgen sein.

Denkbar sind weitere, bereits aus dem PC-System-Bereich bekannte, Bedrohungen durch die Nutzung des Internets (z. B. Pharming[38], Browser-Hijacking[39], Link-Manipulation[40]).

3.3.2.2 Sonstige Angriffe

Da GPRS IP-basiert ist, können auch Schwachstellen der Internetprotokolle (z. B. UDP/TCP, DNS, HTTP, ICMP, ARP usw.) für Manipulations-, Verfügbarkeits- oder Lauschangriffe genutzt werden.

3.3.3 Bedrohungen für Universal Mobile Telecommunications System (UMTS)

3.3.3.1 Erkundungsangriffe

Bedrohungen durch Erkundungsangriffe sind für UMTS in ähnlicher Weise wie bei GSM denkbar. Der UMTS-Standard muss eine Kompatibilität zu GSM aufweisen, um im Falle einer zu geringen Netzabdeckung durch UMTS eine Verbindung über GSM zu ermöglichen [BGTe04, 130; BSI08a, 44]. Hierdurch wird der Einsatz eines IMSI-Catchers wieder möglich, obwohl gerade diese Schwachstelle von GSM, die fehlende gegenseitige Authentisierung, im UMTS-Netz durch eine gegenseitige Authentisierung behoben werden sollte. Die Erkundung der in der Nähe befindlichen mobilen Endgeräte ist ohne Kenntnis der IMSI-Nummer und vorher beschaffter Authentisierungsinformationen jedoch nicht mehr möglich. Liegen diese aber vor, sind eine ungefähre Ortsbestimmung des mobilen Endgerätes und das Auslesen der IMEI-Nummer weiterhin realisierbar [MeWe04, 95].

---

37 Schadsoftware (engl. Maleware) ist jegliche Art von Software, die dazu geeignet ist, die Sicherheit von Systemen und Daten zu beeinträchtigen. Beispiele dafür sind: Viren, Trojaner, Würmer, Key-Logger [BSI08a, 126].

38 Als Pharming wird der Versuch bezeichnet, Internetnutzer auf eine manipulierte Webseite zu locken [Kapp07, 270 ff.]

39 Als Browser-Hijacking wird eine Technik bezeichnet, die die Einstellungen des Webbrowsers manipuliert oder den Nutzer am Besuch von bestimmten Webseiten hindert [Wang09, 24].

40 Bei der Link-Manipulation wird das eigentliche Ziel eines Links verschleiert. Der Link zeigt demNutzer ein Ziel, z. B. http://www.hausbank.de, das eigentliche Ziel ist aber www.hacker.de. Dies kann auf verschiedene Arten geschehen, z. B. mittels HTML-E-Mails, in denen es möglich ist, mittels HTML-Formatierungen einen Link einzugeben und ihn mit Hilfe von Anzeigetext anders erscheinen zulassen.

3.3.3.2 Lauschangriffe

Die Nutzung eines IMSI-Catchers bzw. allgemein das Durchführen einer Man-in-the-Middle-Attacke wurde durch das neue Authentisierungsverfahren im UMTS-Standard [Ecke08, 809 ff.] zwar erschwert, kann einen solchen Angriff aber nicht verhindern. Meyer und Wetzel dokumentieren, wie sich ein solcher Angriff mit Hilfe eines IMSI-Catchers weiterhin durchführen lässt [MeWe04].

Des Weiteren sind die in Abschnitt 3.3.1.2 erwähnten Angriffe durch Innentäter und die unbefugte Nutzung der Schnittstellen für Ermittlungsbehörden auch bei UMTS denkbar, sofern keine Ende-zu-Ende-Verschlüsselungsanwendungen durch die Provider eingesetzt werden.

3.3.3.3 Verfügbarkeitsangriffe

UMTS-Verbindungen lassen sich mit den in Abschnitt 3.3.1.3 beschriebenen Methoden ebenfalls verhindern bzw. unterbrechen. Die in diesem Abschnitt erwähnten GSM-Jammer gibt es in ähnlicher Funktionsweise für UMTS bzw. als Multifunktionsgeräte [SESP11].

3.3.3.4 Manipulationsangriffe

Bedrohungen durch Abschalten der Verbindungsverschlüsselung sind auch im UMTS-Netz gegenwärtig. Wie beispielsweise ein IMSI-Catcher auch bei UMTS-Endgeräten eingesetzt werden kann, haben Meyer und Wetzel gezeigt [MeWe04, 94].

Die Datendienste im UMTS-Netz bauen hauptsächlich auf dem Datendienst GPRS auf, der auch in den GSM-Netzen für die Datenübertragung zur Verfügung steht [BGTe04, 157]. Die in Abschnitt 3.3.2.1 und 3.3.2.2 erwähnten Bedrohungen durch die Internetnutzung sowie die Bedrohungen durch Schwachstellen in den Internetprotokollen können daher auch für UMTS-Datendienste Bedrohungen darstellen.

3.3.4 Bedrohungen für allgemeine Mobilfunk- und Datendienste

3.3.4.1 Kurzmitteilungen (SMS)

Kurzmitteilungen werden auf dem Signalisierungskanal, der normalerweise für den Rufaufbau genutzt wird, übertragen und unterliegen dabei den gleichen Verschlüsselungsmethoden wie die Signalisierungs- und Sprachdaten [BSI08a, 65 ff.]. Allerdings sind auch sie nicht mit einer Ende-zu-Ende-Verschlüsselung geschützt, sondern liegen innerhalb des

Network Subsystems unverschlüsselt vor. Innentäter und auch sich von außen Zugriff verschaffende Angreifer könnten auf die Inhalte der Kurzmitteilungen zugreifen.

Mittels spezieller SMS-Nachrichten ist es möglich, Einstellungen und Konfigurationen auf dem mobilen Endgerät anzupassen, teils sogar ohne dass der Nutzer davon etwas bemerkt [BSI08a, 66]. Mittels spezieller Control-SMS lässt sich bspw. die SSL-Verschlüsselung des WLAN abschalten, um anschließend den Datenverkehr abzuhören [Stei09].

3.3.4.2 Multimedia-Mitteilungen (MMS)

Multimedia-Mitteilungen[41] können für verschiedene Angriffe missbraucht werden [BSI08a, 85]. Richtet ein Angreifer einen eigenen MMS-Proxy-Server ein und hat zuvor mittels OTA-Provisioning (siehe Abschnitt 3.3.5.1.4) die MMS Konfiguration des mobilen Endgerätes manipuliert, so kann er mittels einer MMS, die auf seinen eigenen MMS-Proxy-Server verweist, das mobile Endgerät auf diesen Server zugreifen lassen und beliebige Inhalte an das mobile Endgerät übergeben. Da es Nutzern nicht ohne weiteres möglich ist, zu erkennen, welche aktiven Inhalte in einer Multimedia-Mitteilung enthalten sind, kann sich in einer solchen Mitteilung Schadsoftware befinden, die beim Öffnen der Mitteilung ausgeführt wird.

3.3.4.3 Wireless Application Protocol (WAP) und Internet-Dienste

Internetdienste mit WAP 1.x gewährleisten keine Ende-zu-Ende-Verschlüsselung [BSI08a, 95]. Das in WAP 1.x verwendete Protokoll, Wireless Transport Layer Security (WTLS), gewährleistet nur eine Verschlüsselung bis zum WAP-Gateway des Mobilfunkbetreibers. Erlangt ein Angreifer Zugriff auf diese Gateways, so kann er gesendete Daten aufzeichnen.

Mittels WAP-Push-Nachricht kann der Nutzer dazu veranlasst werden, eine mit aktiven Inhalten präparierte Webseite aufzurufen, die darin enthaltenen Inhalte werden automatisch ausgeführt. Somit wird das mobile Endgerät kompromittiert [BSI08a, 80; Stei09].

Für die effizientere Nutzung verschiedener Internetdienste (z. B. Surfen und E-Mail) wird oftmals Anwendungssoftware angeboten, die für die entsprechenden Dienste keine direkte Verbindung aufbaut, sondern über Proxy-Server die Dienste zur Verfügung stellt [BSI08a, 87 f.]. Dabei könnten Inhalte einer angeforderten Webseite komprimiert werden, bevor die Weiterleitung an das mobile Endgerät erfolgt. Diese Art des Verbindungsaufbaus bietet

[41] Zu den technischen Hintergründen von Multimedia-Mitteilungen vgl. [BSI08a, 83 ff.].

außerdem keine Möglichkeit einer Ende-zu-Ende-Verschlüsselung, da der Proxy-Server aus jeder Verbindungsrichtung den Endpunkt der Verschlüsselung darstellt. Des Weiteren ist es denkbar, dass sich unbefugte Dritte Zugriff auf den Proxy-Server verschaffen und so die gesendeten Daten aufzeichnen können. Auch die Manipulation von Anwendungssoftware, die eine Verbindung über einen Proxy-Server aufbaut, kann für einen Angriff genutzt werden.[42]

Bewegt sich der Nutzer im Internet, so sind hier Bedrohungen durch verschiedene Manipulationstechniken denkbar. Der Nutzer kann durch gefälschte Zertifikate oder gefälschte Status- und Adressanzeigen im Browser dazu verleitet werden, manipulierte Webseiten aufzurufen, die sich oft als originale Seiten (z. B. Bankwebseiten) tarnen.[43] Gibt der Nutzer dann Zugangsdaten auf dieser Webseite ein, werden diese an unbefugte Dritte weitergeleitet. Auch können verborgene Inhalte innerhalb der Webseite nachgeladen werden. Somit wird das mobile Endgerät kompromittiert, um spätere Datenübertragungen abzuhören oder zu manipulieren. Weitere Bedrohungen, welche aus dem PC-System-Bereich bekannt sind, sind bei der Nutzung des Internets denkbar. Diese werden wir hier allerdings nicht im Detail aufzeigen, da bereits eine Vielzahl von Literatur existiert, die sich mit diesem Thema beschäftigt.[44]

Werden Server, PC-Systeme sowie die dazu notwendigen Softwarekomponenten für eine mobile Synchronisation von Kontakt-, Kalenderdaten, E-Mails und Dateien verwendet, können Angreifer durch Ausnutzung von Sicherheitslücken in diesen Komponenten die darüber versendeten Daten ausspähen oder manipulieren.[45] Verfügbarkeitsangriffe auf diese Komponenten sind ebenfalls zur Verhinderung der Kommunikation denkbar. Erlangt ein Angreifer Zugriff auf einen solchen Synchronisationsserver, so kann er sich eine firmeninterne Identität erschleichen und somit Nutzer dazu verleiten, sensible Informationen und Daten an den Angreifer weiterzuleiten [BSI08a, 94]. Zusätzlich zu einem Synchronisationsserver kann ein Network Operation Center (NOC) betrieben werden [BSI08a, 91]. Dieses leitet die zu übermittelnden Daten, angepasst an die mobilen Endgeräte und an die zur Verfügung stehenden Übertragungswege, an das mobile Endgerät weiter.

---

42 Zur näheren Erläuterung siehe Abschnitt 3.3.5.1.4.

43 Diese Techniken werden als Pharming oder Phishings bezeichnet [Kapp07, 270 ff.].

44 Exemplarisch seien hier [Jano07; Raep01] genannt.

45 In Abschnitt 3.3.5.1.4 gehen wir auf diesen Aspekt noch detaillierter ein.

3.3.5 Bedrohungen für mobile Endgeräte

In diesem Abschnitt werden die Bedrohungen nach den Angriffstypen und zusätzlich hinsichtlich des Angriffsortes (der Angreifer ist im Besitz des mobilen Endgerätes bzw. er ist nicht im Besitz des mobilen Endgerätes) unterschieden.

3.3.5.1 Angreifer ist nicht im Besitz des mobilen Endgerätes

3.3.5.1.1 Erkundungsangriffe

Mobile Endgeräte besitzen oft mehrere Schnittstellen für die drahtlose Kommunikation, neben GSM/UMTS z. B. für WLAN, Bluetooth oder IrDA[46]. Diese können teilweise aus großer räumlicher Distanz mit verschiedenen Hilfsmitteln hinsichtlich der verwendeten bzw. nicht verwendeten Sicherheitsmaßnahmen untersucht werden. Zu nennen sind hier vor allem WLAN-Sniffer[47] und Bluetooth-Sniffer [Bach07a]. Weiterhin sind bestimmte Hilfsmittel z. B. dazu in der Lage, aus mitgelesenen Datenpaketen während einer Bluetooth-Kopplung die Kopplungs-PIN mittels einer Brute-Force-Attacke [Erte07, 24 f.] zu erraten, um daraus wiederum den Link-Key[48] zu errechnen [Bach05; Detk06, 175; ShWo05]. Damit ist es einem Angreifer möglich, Zugriff auf ein mobiles Endgerät zu erlangen.

3.3.5.1.2 Lauschangriffe

Die drahtlosen Schnittstellen von mobilen Endgeräten können von Angreifern für Lauschangriffe genutzt werden, insbesondere wenn sie permanent und ohne aktivierte Sicherheitsmaßnahmen betrieben werden. Angreifer nutzen hierfür Sicherheitslücken in den drahtlosen Schnittstellen aus, um Zugang zum mobilen Endgerät und dessen Datenkommunikation zu erlangen.[49]

Weitere Lauschangriffe sind bei der Nutzung von Hot Spots möglich. Ein entsprechend maskiertes Gerät (z. B. ein Laptop) kann einen seriösen öffentlichen Hot Spot vortäuschen und mit entsprechenden Mitteln den über ihn laufenden Datenverkehr aufzeichnen.

---

46 IrDA ist eine Infrarot-Schnittstelle zur Datenübertragung zwischen zwei (mobilen) Endgeräten.

47 WLAN-Sniffer analysieren den WLAN-Datenverkehr, um Informationen über das Netzwerk oder über bestimmte Endgeräte zu erlangen. Ein Beispiel eines solchen Sniffers ist Kismet [Kism11].

48 Link-Key ist ein Schlüssel, den die Geräte abspeichern, um ihn für die Verbindungsverschlüsselung und die gegenseitige Authentisierung zu nutzen.

49 Es gibt immer wieder Meldungen über fehlerhafte Bluetooth Protokolle. Vgl. dazu z. B. [Bach09].

In einigen Ländern ist das Verschlüsseln von gesendeten Daten verboten. Die entsprechenden Strafverfolgungsbehörden dieser Länder können daher auch mit Herstellern zusammenarbeiten, um Möglichkeiten zu schaffen, alle gesendeten Daten zu überwachen. Hält man sich in einem solchen Land auf, kann es sein, dass man ebenfalls von derartigen Maßnahmen betroffen ist [Webe08].

3.3.5.1.3 Verfügbarkeitsangriffe

Mobile Endgeräte lassen sich zum Absturz bringen, indem mittels provozierter Pufferüberläufe Angriffe auf fehlerhafte WLAN-Komponenten, Bluetooth-Komponenten, Netzwerkprotokolle oder Anwendungssoftware durchgeführt werden [Bach07b; BSI06, 20]. Die Folgen eines solchen Angriffes sind Unerreichbarkeit oder der Abbruch einer Datenübertragung.

Sind System- oder Anwendungssoftware fehlerhaft, so können speziell präparierte Daten diese zum Absturz bringen [Bach07b; Hemp09]. Auch manipulierte Anwendungssoftware kann das mobile Endgerät zeitweilig, ganz oder teilweise unbrauchbar machen [O'Co07, 17].

3.3.5.1.4 Manipulationsangriffe

Bei mobilen Endgeräten kann die Betriebssystem- und Anwendungssoftware auf verschiedenen Wegen manipuliert werden. Häufig erfolgt dies mit Hilfe von Schadsoftware[50].

Eine Manipulation des Betriebssystems eines mobilen Endgerätes ist z. B. bei Updateprozeduren über die Firmware-Over-The-Air-Schnittstelle möglich [BSI08a, 124]. Hierbei kann als Update getarnte Schadsoftware auf das mobile Endgerät übertragen werden [Ahle09].

Manipulierte Anwendungssoftware für ein mobiles Endgerät kann für Angreifer Hintertüren öffnen, um Zugriff auf das Gerät zu erlangen oder um vertrauliche Informationen an Dritte weiterzuleiten. Browser könnten z. B. derart manipuliert werden, dass sie die gesendeten Daten über einen feindlichen Proxy-Server umleiten, der sämtlichen Datenverkehr aufzeichnet und ggf. verändert. Auch als harmloses Spiel getarnte Schadsoftware kann vertrauliche Informationen weiterleiten [O'Co07, 19].

---

[50] Schadsoftware im Allgemeinen stellt eine immer stärker werdende Bedrohung für mobile Endgeräte und deren Inhalte dar [Grie08]. Ein Beispiel ist der Wurm mit der Bezeichnung 'Yxes' für Symbian S60 3rd Edition Geräte [Augu09].

Mobile Endgeräte werden oft mit PC-Systemen oder speziellen Synchronisations-Servern abgeglichen, um Kontakt-, Kalenderdatenbanken, E-Mails oder Dateien miteinander zu synchronisieren.[51] Dazu ist meist eine Synchronisationssoftware notwendig. Ist das für die Synchronisation verwendete PC-System oder der Server von einem Angreifer manipuliert oder weist die Synchronisationssoftware Sicherheitslücken auf[52], welche von einem Angreifer ausgenutzt werden, kann sich ein Angreifer darüber Zugriff auf das mobile Endgerät verschaffen bzw. die gesendeten und empfangenen Daten manipulieren.

Wird das mobile Endgerät mit einem PC-System verbunden, das nicht vertrauenswürdig ist, besteht ebenfalls die Gefahr der Manipulation des mobilen Endgerätes, da das PC-System präpariert sein kann, um bspw. Schadsoftware auf das mobile Endgerät zu übertragen.[53]

Manipulationen von auf dem mobilen Endgerät befindlichen Konfigurationsdaten sind über die Over-The-Air-Schnittstelle möglich. Over-The-Air-Provisioning (OTA) [Gemp09] ist eine Schnittstelle, die es Mobilfunkprovidern erlaubt,[54] Konfigurationsdaten (E-Mail-Konfigurationen, WAP-Konfigurationen, Konfigurationen für Datenverbindungen mittels GPRS etc.) eines mobilen Endgerätes ohne Zutun des Nutzers anzupassen oder Applikationen einzuspielen [BSI08a, 123 f.]. Über diese Schnittstelle ist es möglich, mit Hilfe einer speziellen SMS die Zugangsdaten für Datenverbindungen mobiler Endgeräte so zu manipulieren, dass die Datenverbindungen auf einen frei gewählten Server umgeleitet werden, um dort aufgezeichnet und manipuliert werden zu können [Ries09].

Eine weitere Bedrohung stellt die Manipulation von Menüpunkten des mobilen Endgerätes dar.[55] Mittels SIM-Toolkit können vom Mobilfunkprovider kleine Applikationen an die SIM-Karte gesendet werden [Saut08, 77]. Diese Applikationen können auf Benutzereingaben reagieren oder auch Menüpunkte in die Menüstruktur des mobilen Endgerätes einbinden. Verschafft sich ein Angreifer Zugriff auf die SIM-Toolkit-Schnittstelle, so kann er in

---

51 Für Symbian OS steht die 'PCSuite' zur Verfügung, bei Windows Mobile 'Active Sync' und bei BlackBerry die 'BlackBerry Desktop-Software'. Zusätzlich gibt es bei BlackBerry den Enterprise Server für Unternehmen. Windows Mobile Geräte lassen sich mit diversen Exchange Servern synchronisieren.

52 Dokumentierte Beispiele für Sicherheitslücken in Synchronisationssoftware traten z. B. bei der BlackBerry Desktop-Software [Tech08] und im BlackBerry Enterprise Server [Tech09] auf.

53 Vgl. für die notwendige Nutzerinteraktion bei diesem Angriff Abschnitt 3.3.6.

54 Obwohl Over-The-Air-Provisioning ein Dienst ist, den das Mobilfunknetz zur Verfügung stellt, wurde diese Bedrohung den Bedrohungen der mobilen Endgeräte zugeordnet, da die mobilen Endgeräte oftmals den Nutzern keine Möglichkeit bieten, die Durchführung dieser Veränderungen abzulehnen.

55 Die Bedrohungen durch SIM-Toolkit sind den mobilen Endgeräten zugeordnet, da die SIM-Karte und das mobile Endgerät in der Literatur immer als zusammengehörige Einheit dargestellt wird.

die Software des mobilen Endgerätes eingreifen und manipulierte Menüeinträge ablegen. In Verbindung mit bereits auf dem Telefon befindlicher Schadsoftware kann so die oftmals benötigte Mithilfe des Benutzers beim Ausführen von Schadsoftware leicht erreicht werden. Auch können schon auf dem mobilen Endgerät befindliche manipulierte Firmwarekomponenten aktiviert werden.

3.3.5.2 Angreifer ist im Besitz des mobilen Endgerätes

Werden mobile Endgeräte „aus der Hand“ gegeben, z. B. für Wartungsarbeiten, zur Abgabe im Empfangsbereich beim Besuch eines fremden Unternehmens zur Wahrung des Firmengeheimnisses oder durch Diebstahl, sind folgende weitere Bedrohungen denkbar:

3.3.5.2.1 Erkundungsangriffe

Mobile Endgeräte eines Unternehmens oder einer Behörde können gewisse äußerliche Merkmale aufweisen (bspw. Gerätekennzeichnungen, Inventarnummern etc.), die sie als unternehmens- bzw. behördenzugehörig erscheinen lassen. Solche Merkmale können ausspioniert werden, um manipulierte Endgeräte äußerlich so zu verändern, dass sie als unternehmens- bzw. behördenzugehörig angesehen werden [BSI06, 17].

Zugangsdaten bzw. Passwörter lassen sich über verschiedene Wege erkunden: über den Nutzer selbst (siehe Abschnitt 3.3.6), durch Erraten der Zugangsdaten sowie über Wörterbuch-, Brute-Force-, Known-Plaintext-, Known-Chiphertext-Angriffe [Ecke08, 333 f., 453]. Auch Passwortdateien, in denen Hashwerte des Passwortes abgelegt werden, lassen sich mittlerweile über Webseiten auf das Klartext-Passwort zurückrechnen bzw. per Wörterbuchtabellen in Erfahrung bringen.[56]

Geräte mit berührungsempfindlichen Displays weisen oftmals Gebrauchsspuren auf, die auf Passwörter zur Anmeldung am Gerät schließen lassen (bspw. Kratzspuren durch häufige PIN- oder Passworteingabe beim Einschalten des Gerätes) [BSI06, 17].

Im Besitz von Angreifern befindliche mobile Endgeräte können hinsichtlich der eingesetzten Betriebssysteme, der Anwendungssoftware und der Sicherheitsmaßnahmen (z. B. Sicherheitssoftware, Sicherheitspolicies) analysiert werden [BSI06, 17]. Dies kann das Finden von Angriffspunkten erleichtern.

[56] Als Beispiel einer solchen Webseite sei auf http://md5cracker.org verwiesen.

3.3.5.2.2 Lauschangriffe

Ist ein Angreifer im Besitz eines mobilen Endgerätes, kann er vielfältige Informationen aus dem internen Telefonspeicher oder von Speicherkarten auslesen, wenn der Zugriff auf diese unzureichend gesichert ist. Hierbei können nicht nur sensible Unternehmensdaten ausgelesen werden, sondern auch Passwörter oder Konfigurationsdaten (z. B. gültige IP-Bereiche etc.). Das Entfernen von Log-Dateien ist ebenso denkbar [BSI06, 21].

Es besteht die Möglichkeit des Erlangens von sensiblen Daten, wenn mobile Endgeräte die nicht für den Mehrbenutzerbetrieb ausgelegt sind, von mehreren Personen genutzt werden [BSI06, 17]. Wird ein Gerät beim Nutzerwechsel zurückgesetzt, wird oft der Speicher des mobilen Gerätes nicht sicher gelöscht. Daten, die vor der Löschung auf dem Gerät gespeichert waren, können dann ggf. leicht wiederhergestellt werden. Unbefugte erhalten dadurch relativ leicht Zugriff auf sensible Daten.

3.3.5.2.3 Verfügbarkeitsangriffe

Das mobile Endgerät kann zur Verhinderung einer Datenkommunikation gezielt entwendet werden. Ein Diebstahl kann aber auch zum Zwecke der Manipulation erfolgen und anschließend wieder zurückgegeben werden (vgl. folgenden Abschnitt).

3.3.5.2.4 Manipulationsangriffe

Ein Gerät kann bereits beim Hersteller manipuliert werden, aber auch bei den in Abschnitt 3.3.5.2 erwähnten Gelegenheiten, sind folgende Manipulationen denkbar:

- Installation zusätzlicher Speicher- und Kommunikationshardware zur Protokollierung der Eingaben und von gesendeten/gespeicherten Daten
- Manipulation des Betriebssystems/ der Firmware und der Anwendungssoftware
- Ausnutzung der Software-Schwachstellen (Betriebssystem-, Anwendungssoftware)
- Deaktivierung der Sicherheitsmaßnahmen und Authentisierungsmechanismen
- Installation von Schadsoftware

Anschließend wird das manipulierte mobile Endgerät dem Nutzer zurückgegeben. Dieser verwendet es unter Umständen ohne vorherige, intensive Prüfung auf Manipulationen durch einen Techniker bzw. Administrator. Durch die (fahrlässige) Weiterverwendung können dann z. B. Informationen über Zugangsdaten an unbefugte Dritte übermittelt werden.

Eine weitere Bedrohung besteht in der Verwendung von zurückgegebenen, gefälschten mobilen Endgeräten. Ist eine Manipulation des ursprünglich entwendeten Endgerätes nicht möglich, ist es ebenfalls denkbar, dass das entwendete mobile Endgerät geklont wird. Hierbei wird das einzuschleusende mobile Endgerät sowohl äußerlich als auch von der Softwarekonfiguration her so gestaltet, dass der Nutzer, dem es später zurückgegeben wird, keinen Unterschied zum ursprünglichen Gerät bemerkt und es weiter verwendet.

3.3.5.3 Mögliche Bedrohungen für Symbian Operating System

Sicherheitsmaßnahmen von Symbian OS basieren hauptsächlich auf Capabilities[57] und auf der Signierung von Anwendungssoftware [EnWe08; Enz07]. Sicherheitsrelevante APIs sind immer mit einer Capability verknüpft. Eine Anwendungssoftware bzw. ein Prozess kann nur dann auf diese APIs zugreifen, wenn er die Rechte an der entsprechenden Capability hat. Möchte eine Anwendungssoftware bspw. auf die Kurznachrichten des mobilen Endgerätes zugreifen, benötigt diese die Rechte an der ReadUserData-Capability[58]. Die Zugriffsrechte werden anhand der Signierung mit unterschiedlichen Zertifikaten festgelegt. Die Signierung kann mit einem selbst erstellten Zertifikat geschehen, jedoch hat dabei die Anwendungssoftware lediglich die Zugriffsrechte auf die User-Capabilities. Nur wenn Anwendungssoftware von der offiziellen Signierungsinstanz „SymbianSigned“ beglaubigt wurde, kann diese mittels eines Zertifikats erweiterte Zugriffsrechte, so genannte Extended-Capabilities, erhalten. Anwendungssoftware, die über SymbianSigned zertifiziert wurde, wird vor Erteilung des Zertifikates geprüft. Bis jetzt ist noch kein Fall von gefälschten Zertifikaten bekannt geworden, jedoch ist es durchaus denkbar, dass manipulierte Anwendungssoftware mit gefälschten Zertifikaten versehen wird, um dem Nutzer eine vermeintlich seriöse Anwendung vorzutäuschen. Eine solche Anwendungssoftware hätte dann vollen Zugriff auf das mobile Endgerät und könnte verschiedene Manipulationen durchführen.

Ein weiteres Problem stellen so genannte Symbian Hacks[59] dar. Diese ermöglichen es, Sicherheitseinstellungen und -maßnahmen zu umgehen und bspw. unsignierte Anwendungssoftware zu installieren oder als Nutzer vollen Systemzugriff zu erlangen. Gehäuft erscheinen Berichte nicht nur über geknackte Versionen von Symbian OS, sondern auch

---

57 Eine Capability besteht aus einer Referenz auf ein schützenswertes Objekt (z. B. eine Funktion, API, Anwendung) und der Zugriffsrechte auf dieses Objekt [EnWe08; Espo09, 27].

58 Für eine ausführliche Beschreibung der Capabilities von Symbian OS vgl. z. B. [EnWe08; Enz07].

59 Vgl. hier zum Beispiel [Open08].

über die Behebung der entsprechenden Sicherheitslücken, die einen solchen Hack ermöglicht haben. Für die Anwendung eines solchen, recht zeitaufwändigen Hacks ist jedoch der Besitz des mobilen Endgerätes erforderlich. Allerdings sind danach vielfältige Manipulationsmöglichkeiten denkbar.

3.3.5.4 Mögliche Bedrohungen für Windows Mobile

Anwendungssoftware kann mit einem Zertifikat signiert werden, welches die vollen Zugriffsrechte auf das mobile Endgerät gewährleistet.[60] Dies geschieht, wie auch bei Symbian OS durch eine zentrale Instanz (Mobile2Market). Würde man Anwendungssoftware mit einem gefälschten Zertifikat signieren, könnte ein Angreifer den Anschein einer seriösen Anwendungssoftware vermitteln und den Nutzer dazu verleiten, diese zu installieren.

3.3.5.5 Mögliche Bedrohungen für Research In Motion (RIM)

BlackBerry-Geräte werden selten als Einzelgeräte betrieben. Sie sind vielmehr eine Einheit aus mobilem Endgerät und der BlackBerry-Infrastruktur, bestehend aus BlackBerry Enterpriseserver und BlackBerry Desktopsoftware. Um ein BlackBerry anzugreifen, bieten sich somit gleich mehrere Angriffspunkte als das bloße mobile Endgerät. Schwachstellen der Infrastruktur [Tech08; Tech09] lassen sich für Angriffe auf das mobile Endgerät verwenden, um bspw. den Verschlüsselungsschlüssel in Erfahrung zu bringen, der auf dem dazugehörigen PC-System und dem Exchange-Server des Unternehmens abgespeichert ist. Mittels dieses Schlüssels kann ein Angreifer die gesendeten Daten des BlackBerry wieder entschlüsseln.

Auf einem BlackBerry lässt sich lediglich Java-Anwendungssoftware installieren. Diese hat begrenzte Zugriffsrechte und kann nur auf den für die Java-Virtuelle-Maschine (JVM) reservierten Speicher zugreifen [Diet04, 7]. Lediglich von RIM signierte Java-Anwendungssoftware kann auf erweiterte APIs zugreifen (z. B. Netzwerkressourcen, Telefonbucheinträge etc.). RIM prüft die Anwendungssoftware jedoch nicht vor dem Signieren. Es wird lediglich vermerkt, welcher Hersteller die erweiterten APIs nutzt. Somit ist es denkbar, dass Schadsoftware signiert wird und als vertrauenswürdige Anwendungssoftware erscheint. Ist eine solche Anwendung signiert, kann sie sich selbst starten und auch in den Hintergrund versetzen, so dass sie vom Nutzer unbemerkt arbeiten kann [O'Co07, 18].

---

[60] Eine detaillierte Beschreibung der Zugriffsmodelle von Windows Mobile vgl. z. B. [EnWe08; Enz07].

Anwendungssoftware kann sowohl SMS senden als auch empfangen [O'Co07, 18 ff.]. Mit einem kompromittierten Endgerät ist es denkbar, unbefugten Dritten das Senden und Empfangen von SMS zu ermöglichen und Hintertüren für Kontrollkommandos zu öffnen, um sensible Daten an Dritte zu versenden oder Internetverbindungen aufzubauen. Ist die Anwendungssoftware für ein solches Vorhaben bspw. als Spiel, mit der Funktion des Versendens von Spielständen per SMS, getarnt, muss der Nutzer die Anwendung lediglich einmal für die SMS-Nutzung autorisieren. Danach kann die Anwendung ungehindert SMS verschicken und empfangen. In Verbindung mit der im Absatz zuvor erwähnten Möglichkeit signierter Anwendungssoftware sich selbst in den Autostart- und in den Hintergrundmodus zu versetzen, müsste der Nutzer die Anwendungssoftware nur ein einziges Mal starten, damit sie ihre Aufgabe dauerhaft erfüllen kann.

3.3.6 Bedrohungen, die vom Nutzer des mobilen Endgerätes ausgehen

Es ist notwendig, das Verhalten des Nutzers eines mobilen Endgerätes in die Betrachtungen einer Bedrohungsanalyse mit einzubeziehen, da dieser aus Unwissenheit, Fahrlässigkeit, Bequemlichkeit oder mit Vorsatz dafür sorgen kann, dass etablierte Sicherheitsmaßnahmen keine Wirkung haben.

Ein Angriff, der als Social Engineering oder auch als Social Hacking bezeichnet wird, zielt darauf ab, die Nutzer derart zu täuschen, dass diese freiwillig Informationen preisgeben, die einem Angreifer nützlich sein können, um einen geplanten Angriff vorzubereiten bzw. durchzuführen [Ecke08, 23, 58; Hump04, 17]. Dies können Informationen über die verwendete Software oder Hardware sein, aber auch Zugangsdaten zu sicherheitskritischen Systeme. Angreifer täuschen dazu oft eine falsche Identität vor, bspw. geben sie sich als Systemadministrator aus, der angeblich für wichtige Wartungsarbeiten die Zugangsdaten benötigt.

Auch der falsche Umgang mit Passwörtern kann zu einer Bedrohung für das mobile Endgerät und für die Systeme werden, zu denen das mobile Endgerät Zugang hat. Angreifern wird dadurch der Zugang zu vertraulichen Inhalten erleichtert. Zum falschen Umgang zählen:

- Passwort- bzw. PIN-Abfragen aus Bequemlichkeit deaktivieren,
- Verwendung von schwachen Passwörter und PIN-Nummern,

- Übermitteln von Passwörtern über ungesicherte Kommunikationswege bzw. unverschlüsselt,
- Preisgabe von Passwörtern gegenüber unbefugten Personen (z. B. durch Social Engineering oder durch Beobachtung der Passworteingabe nach einer erzwungenen Neuanmeldung am mobilen Endgerät).

Firewalls, Virenscanner, Intrusion-Detection-Software oder Verschlüsselungen (Kommunikations- und Speicherverschlüsselung) können aus Leistungsgründen abgeschaltet werden, um mehr Rechenleistung auf dem mobilen Endgerät zur Verfügung zu haben. Dies kann zur Folge haben, dass Angreifer nicht an bestimmten Angriffen gehindert werden können bzw. dass Daten unverschlüsselt vorliegen.

Ist in einem mobilen Endgerät keine Vorsorge dafür getroffen, dass Anwendungssoftwareinstallationen nur von Administratoren durchgeführt werden können bzw. dürfen auch nicht oder nur schwach zertifizierte Anwendungen[61] installiert werden, so kann die Installation von Anwendungssoftware aus ungeprüften Quellen zur Kompromittierung des mobilen Endgerätes führen.

Schnittstellen, wie WLAN, Bluetooth oder IrDA können für Erkundungsangriffe genutzt werden, insofern sie auch nach der Nutzung unnötig aktiviert bleiben [BSI06, 23].

Nutzer, die unzureichend für Sicherheitsaspekte im Umgang mit mobilen Endgeräten sensibilisiert sind oder die wider besseres Wissen handeln, können den in Abschnitt 3.3.5.1.4 dargestellten Manipulationsangriff ermöglichen, indem sie das mobile Endgerät mit einem manipulierten PC-System verbinden.

Die Verwendung von präparierten Wechselspeichermedien kann zur Kompromittierung des mobilen Endgerätes führen. Mobile Endgeräte sind oft mit Erweiterungssteckplätzen ausgerüstet, die Wechselspeichermedien aufnehmen können. Sind solche Wechselspeichermedien entsprechend präpariert, z. B. mit sich selbst ausführender Schadsoftware, so kann ein bloßes Einstecken dieser Wechselspeichermedien zur Kompromittierung des mobilen Endgerätes führen.

[61] Symbian, RIM und Microsoft bieten Zertifizierungsdienste für Anwendungen ihrer Plattformen an. In den mobilen Endgeräten ist es dann möglich, festzulegen welches Zertifikatsniveau eine Anwendung aufweisen muss [Enz07; O'Co07, 6].

Aus Unachtsamkeit und Zeitmangel kann es vorkommen, dass Nutzer auf ihren mobilen Endgeräten Daten mit sich führen, die nicht permanent auf diesem vorgehalten werden müssten. Kann ein Angreifer sich Zugriff auf das mobile Endgerät verschaffen, ist der Umfang der Kenntnisnahme vertraulicher Informationen größer, als hätte der Nutzer eine höhere Sorgfalt bei der Auswahl der mitgeführten Daten walten lassen.

Unachtsamkeit im Umgang mit dem mobilen Endgerät kann zum Diebstahl oder zum Liegenlassen des mobilen Endgerätes führen. Daraufhin könnten sich unbefugte Dritte vertrauliche Informationen beschaffen oder das mobile Endgerät zu Manipulationszwecken missbrauchen.

Auch die Innentäterproblematik gilt es zu berücksichtigen. Verschiedene Aktionen, wie die Preisgabe von Zugangsdaten, das Übermitteln von sensiblen Unternehmensdaten, das Entwenden von mobilen Endgeräten, das Verwenden von manipulierten mobilen Endgeräten etc. kann auch, motiviert durch Bestechung oder Spionage, absichtlich durch einen Nutzer vorgenommen werden.

3.4 Bedrohungsbäume und Bedrohungskatalog

3.4.1 Erstellung der Bedrohungsbäume

Die mittels der Bedrohungsanalyse ermittelten Bedrohungen werden in Bedrohungsteilbäume überführt. Dabei haben wir die in Abschnitt 3.3 vorgenommene Einteilung übernommen. Abb. 3-3 zeigt diese Einteilung:

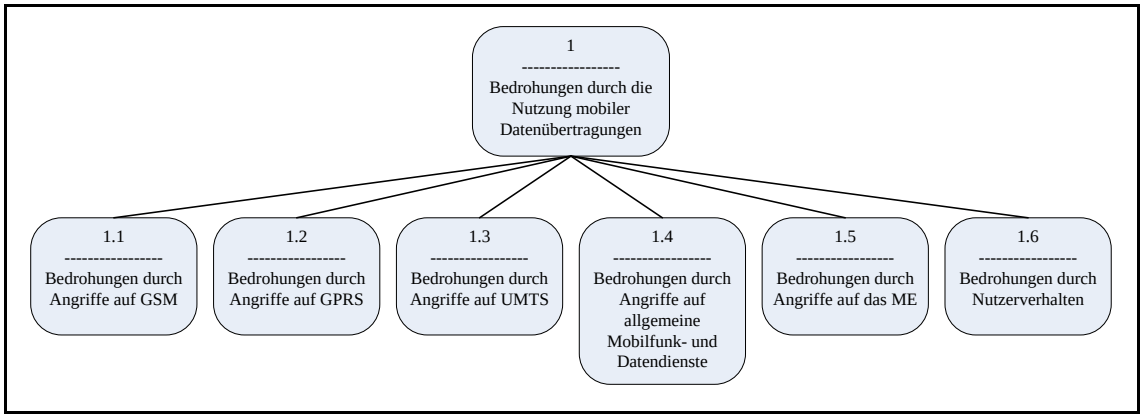

Abb. 3-3: Hauptbedrohungsbaum

Zusätzlich zu dieser Aufteilung haben wir die Bedrohungsteilbäume nochmals unterteilt, um eine bessere Übersichtlichkeit zu gewährleisten. Aufgrund der Ähnlichkeiten, z. B. bei GSM und UMTS, kann es in den verschiedenen Bedrohungsteilbäumen zur Mehrfachnen-

nung von gleichen Bedrohungen bzw. Angriffen unter verschiedenen Knoten-Nummern kommen. Identische Knoten, die unter verschiedenen Knoten-Nummern aufgeführt sind, sind im Bedrohungskatalog kenntlich gemacht. In der Spalte 'Bemerkungen' befindet sich ein Verweis auf alle identischen Knoten der gleichen Bedrohung. Um unnötige Mehrfachnennungen zu vermeiden, wird z. B. bei einem Lauschangriff davon ausgegangen, dass zuvor ein Erkundungs- oder Manipulationsangriff stattgefunden hat. Die durch die vorausgegangenen Angriffe entstehenden Bedrohungen bzw. die dafür notwendigen Angriffsschritte sind daher im Bedrohungsteilbaum für den Lauschangriff nicht aufgeführt. Für die Modellierung der Bedrohungsbäume werden zwei Knotentypen unterschieden. Knoten, die lediglich der Strukturierung innerhalb der Bedrohungsbäume dienen, sind blau (dunkel). Knoten, die Bedrohungen bzw. die dafür notwendigen Angriffsschritte darstellen, sind weiß (hell) eingefärbt.

Die Darstellung aller Bedrohungsteilbäume ist den Abbildungen im Anhang A.1 zu entnehmen.

3.4.2 Wirkungsanalyse und Erstellung des Bedrohungskataloges

Für jede Bedrohung haben wir durch eine Wirkungsanalyse ermittelt, zu welchen denkbaren Konsequenzen/Folgen diese Bedrohung führen kann und wie dadurch die Sicherheit der mobilen Datenübertragung gefährdet wird [Stel93, 218 ff., 234 ff,]. Dabei haben wir berücksichtigt, dass eine Bedrohung auch gleichzeitig zu mehreren Konsequenzen führen kann. Mögliche Konsequenzen sind die Zerstörung bzw. der Verlust, der Ausfall, die Nutzung, die Veränderung und die Kenntnisnahme sicherheitsrelevanter Objekte. In Folge dieser Konsequenzen entsteht eine Gefährdung der Sicherheit, die sich durch die Beeinträchtigung von Sicherheitsziele dokumentieren lässt. In Tab. 3-2 ist dargestellt, welche Sicherheitsziele von welchen Angriffen beeinträchtigt werden können.

Sicherheitsziele (Abk.)	Bedrohungen durch typische Angriffe
Vertraulichkeit (VT)	Sniffing, Trojanische Pferde, Schadsoftware, Social Engineering, Backdoors, Passwort-Cracking
Integrität (IN)	Schadsoftware, Man-in-The-Middle-Angriffe, Umleitung von Proxyverbindungen, Web-Spoofing
Verfügbarkeit (VF)	Schadsoftware, Denial-of-Service-Angriffe, Redirect-Angriffe
Authentizität (AU)	Mail-Spoofing, ARP-Spoofing, IP-Spoofing, Passwort-Cracking
Verbindlichkeit (VB)	Ablehnung von Bestellungen, Ablehnung von Empfangsbestätigungen
Anonymität (AN)	Ermittlung von Identitäten, Erstellen von Bewegungsprofilen

Tab. 3-2: Beeinträchtigungen von Sicherheitszielen durch Angriffe [Raep01, 99]

Anhand der Tab. 3-2 haben wir die Zuordnung der durch die Bedrohungsanalyse ermittelten Bedrohungen (Abschnitt 3.3) zu den gefährdeten Sicherheitszielen vorgenommen. Für die Einschätzung der durch die Bedrohungen möglichen Beeinträchtigungen von Sicherheitszielen haben wir die in Abb. 3-4 dargestellten Zusammenhänge herangezogen.

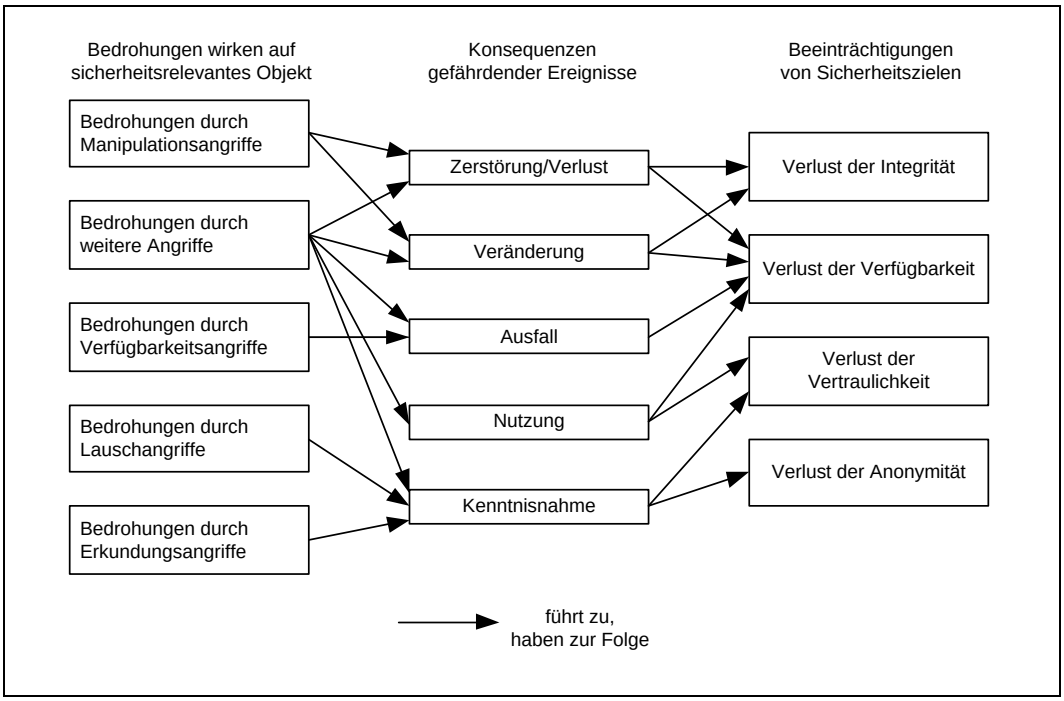

Abb. 3-4: Bedrohungen, Folgen und Beeinträchtigungen von Sicherheitszielen[62]

Im Anschluss an die Wirkungsanalyse haben wir die Bedrohungsteilbäume in einen *Bedrohungskatalog* umgewandelt, in dem alle Bedrohungen mit ihren Eigenschaften tabellarisch auflistet sind. Der Katalog gibt in fortlaufend nummerierten Einträgen jede Bedrohung aus den Bedrohungsteilbäumen anhand ihrer Knoten-Nummer wieder. Der zu einer Bedrohung führende Angriff wird genannt und die durch ihn entstehende Bedrohung kurz erläutert. Das einer Bedrohung zugeordnete, gefährdete Sicherheitsziel wird in der Spalte 'beeinträchtigtes Sicherheitsziel' aufgeführt. Des Weiteren sind in der Spalte 'Maßnahmen-Nummer' die Nummern der Sicherheitsmaßnahmen verzeichnet, die die aufgeführte Bedrohung mindern bzw. abwenden können. In den 'Bemerkungen' finden sich die Verweise auf identische Knoten, die unter unterschiedlichen Knoten-Nummern aufgeführt sind.

Beispielhaft ist in Tab. 3-3 die Bedrohung Nr. 12 mit der Knoten-Nummer '1.1.1.1' dargestellt. Der Bedrohung des Auslesens der IMSI-Nummer eines Mobilfunkteilnehmers liegt eine Schwachstelle des GSM-Mobilfunkstandards zu Grunde. Im GSM-Mobilfunkstandard

62 Eigene Darstellung in Anlehnung an [Stel93, 37].

ist keine gegenseitige Authentisierung zwischen mobilem Endgerät und Mobilfunknetz vorgesehen. Lediglich das mobile Endgerät muss sich authentisieren. Somit kann ein Angreifer gegenüber einem mobilen Endgerät den IMSI-Catcher wie eine Basisstation eines Mobilfunknetzes erscheinen lassen und vom mobilen Endgerät die IMSI-Nummer erfragen. Es findet eine Kenntnisnahme der Identität eines Mobilfunkteilnehmers statt.[63] Die Kenntnisnahme hat zur Folge, dass die Anonymität (AN) und die Vertraulichkeit (VT) beeinträchtigt werden.

Nr.	Knoten-Nr.	Bedrohung	Verknüpfung	Bedrohungsbeschreibung	beeintr. Sicherheitsziel	Maßnahmen-Nr.	Bemerkungen
12	1.1.1.1	Auslesen der IMSI-Nummer	ODER	Eine Kenntnisnahme vertraulicher Identitätsinformationen ist möglich.	VT, AN	OM 22, OM 23	Punkt ist identisch mit: 1.3.1.1
13	1.1.1.1.1	Vortäuschen einer GSM-Basisstation	UND	Mittels eines IMSI-Catchers ist es möglich, eine GSM-Basisstation vorzutäuschen. Mobile Endgeräte können keinen Unterschied zu einer "echten" GSM-Basisstation erkennen. Sie nutzen daher die vermeintliche GSM-Basisstation, um sich mit dem Mobilfunknetz zu verbinden. Eine solche, falsche GSM-Basisstation kann verschiedene Informationen aus dem mobilen Endgerät auslesen, die Verschlüsselung des mobilen Endgerätes abschalten und den Standort des mobilen Endgerätes näher bestimmen. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN	TM 1	Punkt ist identisch mit: 1.1.1.2.1 , 1.1.1.3.1, 1.3.1.1.1, 1.3.1.2.1, 1.3.1.3.1

Tab. 3-3: Auszug aus dem Bedrohungskatalog (Beispiel 1)

Ergänzend zu Tab. 3-3 zeigt Tab. 3-4 die Zuordnung der bedrohten Sicherheitsziele beispielhaft anhand der Bedrohung „Entwendung des MEs“. Die im Bedrohungskatalog den Bedrohungen zugeordneten beeinträchtigten Sicherheitsziele haben wir anhand des beabsichtigten Ziels eines Angriffes zugeordnet und nicht anhand aller überhaupt denkbaren bedrohten Sicherheitsziele. Wird ein mobiles Endgerät entwendet, so sind Gefährdungen für alle Sicherheitsziele denkbar. Für Bedrohung Nr. 219 ist kein genaues Angriffsziel spezifiziert, daher sind alle Sicherheitsziele als möglicherweise beeinträchtigte Sicherheitsziele in die Tabelle eingetragen. Bei Bedrohung Nr. 168 allerdings wird das mobile Endgerät entwendet, um die Verfügbarkeitsangriff durchzuführen. Daher ist als beeinträchtigtes Sicherheitsziel lediglich die Verfügbarkeit aufgeführt.

[63] Durch die Kenntnisnahme der IMSI-Nummer ist eine eindeutige Identifizierung eines Mobilfunkteilnehmers möglich, da diese Nummer, im Gegensatz zur TMSI-Nummer, dem Mobilfunkteilnehmer permanent zugeordnet ist, solange er die gleiche (U)SIM-Karte nutzt.

Nr.	Knoten-Nr.	Bedrohung	Ver-knüp-fung	Bedrohungsbeschreibung	beeintr. Sicherheits-ziel	Maßnahmen-Nr.	Bemerkungen
168	1.5.3.5	Entwendung des MEs	ODER	Um bestimmte Angriffe ausführen zu können, muss ein Angreifer das mobile Endgerät in seinen Besitz bringen.	VF	TM, 25, TM 26 OM 9, OM 10, OM 11, OM 12, OM 13, OM 31	Punkt ist identisch mit: 1.5.1.2.1, 1.6.10.1
219	1.6.10.1	Entwendung des MEs	ODER	Verliert der Nutzer ein mobiles Endgerät, lässt er es unbeaufsichtigt zurück oder verleiht er es an jemanden, ist eine Kenntnisnahme vertraulicher Informationen möglich. Weiterhin kann sich dann ein Unbefugter Zugriff auf das lokale Unternehmensnetzwerk verschaffen bzw. das Endgerät kann dann manipuliert und anschließend zurückgegeben werden etc..	VT, IN, VF, AU, VB, AN	TM 25, TM26, TM 37 OM 4, OM 9, OM 11, OM 12, OM 13, OM 21, OM 31	Punkt ist identisch mit: 1.5.1.2.1, 1.5.3.5

Tab. 3-4: Auszug aus dem Bedrohungskatalog (Beispiel 2)

Der vollständige Bedrohungskatalog mit allen 221 bewerteten Bedrohungen befindet sich im Anhang A.2.

4 Sicherheitsmaßnahmenkatalog

Für die Zusammenstellung relevanter Maßnahmen zur Sicherung der Datenübertragung über Mobilfunknetze haben wir vornehmlich zwei Arbeiten des Bundesamtes für Sicherheit in der Informationstechnik [BSI06; BSI08a] verwendet sowie weitere Fachliteratur, Dokumentationen und Publikationen ausgewertet. In einem zweiten Schritt haben wir durch Expertendiskussionen, persönliche Einschätzungen und den Test einzelner Maßnahmen den Katalog weiterentwickelt. Es entstand ein Katalog mit 70 Maßnahmen zur Sicherung der Datenübertragung über Mobilfunknetze.

4.1 Aufbau des Sicherheitsmaßnahmenkataloges

Sicherheitsmaßnahmen können bspw. nach dem Vorbild der Maßnahmenklassifikation der IT-Grundschutzkataloge des BSI[64] oder nach dem Ebenenmodell der Sicherheit der Informationsverarbeitung nach Stelzer[65] gegliedert werden [BSI09; Stel93].[66] Daran angelehnt haben wir die Sicherheitsmaßnahmen in unserem Katalog zunächst nach technischen und organisatorischen Sicherheitsmaßnahmen gegliedert.

64 Das BSI unterscheidet Maßnahmen für die Bereiche Infrastruktur, Organisation, Personal, Hardware/ Software, Kommunikation und Notfallvorsorge [BSI09, 20].

65 Im Ebenenmodell der Sicherheit der Informationsverarbeitung unterscheidet Stelzer physische, logische, organisatorisch-soziale sowie rechtlich-wirtschaftliche Maßnahmen [Stel93, 26 ff.].

66 In der Literatur gibt es weitere Ansätze zur Klassifikation von Sicherheitsmaßnahmen, vgl. z. B. [ITU91; Mart73].

Bei den technischen Sicherheitsmaßnahmen unterscheiden wir weiterhin in Maßnahmen für die Kommunikationssicherheit, Maßnahmen für die Endgerätesicherheit und sonstige technische Sicherheitsmaßnahmen. *Maßnahmen für die Kommunikationssicherheit* enthalten Maßnahmen, die der Absicherung von Verbindungen, die über Mobilfunknetze zustande kommen, dienen und das mobile Endgerät vor Bedrohungen durch Mobilfunkkommunikation schützen. *Maßnahmen für die Endgerätesicherheit* stellen Maßnahmen zum Schutz des mobilen Endgerätes vor Bedrohungen dar und werden auf dem mobilen Endgerät angewandt, wie z. B. Antivirussoftware auf dem mobilen Endgerät. Unter *sonstige technische Sicherheitsmaßnahmen* haben wir alle Maßnahmen zusammengefasst, die von einer zentralen Stelle/Instanz durchgeführt werden bzw. die zum Schutz des lokalen Unternehmensnetzwerkes beitragen. Jedoch gehen wir auf Maßnahmen zum Schutz des lokalen Unternehmensnetzwerks nicht detailliert ein, da für den Schutz dieser Netzwerke bereits ausführliche Abhandlungen existieren.[67]

Die organisatorischen Sicherheitsmaßnahmen beinhalten Verhaltensregeln für den Umgang mit mobilen Endgeräten und mit sensiblen Daten, die sich auf diesen Geräten befinden, sowie Maßnahmen zur Mitarbeitersensibilisierung und Verpflichtung der Mitarbeiter zur Einhaltung der Sicherheitsmaßnahmen.

Eingeordnet in die einzelnen Kategorien enthält der Katalog die Sicherheitsmaßnahmen mit einer Beschreibung der jeweiligen Maßnahme und die mit der Sicherheitsmaßnahme verfolgten Sicherheitsziele. In der Spalte 'Bemerkung' befinden sich die Quellengaben für die jeweilige Maßnahme und soweit verfügbar, die Nennungen von Beispielen der in der Praxis existierenden Hardware- bzw. Softwarelösung für die jeweilige Sicherheitsmaßnahme.

4.2 Überblick über die Sicherheitsmaßnahmen

Der Sicherheitsmaßnahmenkatalog umfasst 37 technische und 33 organisatorische Maßnahmen. Diese sind jeweils fortlaufend nummeriert. TM steht für technische Sicherheitsmaßnahme und OM für organisatorische Sicherheitsmaßnahme.

Auf die detaillierte Erläuterung jeder einzelnen Sicherheitsmaßnahme haben wir verzichtet. Stattdessen befindet sich im Sicherheitsmaßnahmenkatalog für jede Maßnahme eine kurze

[67] Vgl. hier z. B. [Alex06; Hunt98]

Beschreibung. Außerdem haben wir dort auf Publikationen verwiesen, die genauere Erläuterungen zu den einzelnen Maßnahmen enthalten.

Des Weiteren haben wir darauf verzichtet, zu jeder technischen Sicherheitsmaßnahme, z. B. „TM 21 - Einsatz von Firewallsoftware“, eine gleichnamige organisatorische Sicherheitsmaßnahme einzuführen, die lediglich die Durchsetzung der technischen Sicherheitsmaßnahme gewährleistet. Stattdessen wurden die Maßnahmen „OM 5 - Nutzer für die Sicherheitsmaßnamen sensibilisieren“, „OM 6 - Nutzer im Umgang mit den Sicherheitsmaßnamen schulen“ und „OM 7 - Nutzer zur Einhaltung und Anwendung von Sicherheitsmaßnahmen verpflichten“ erstellt. Diese Maßnahmen sollen die Durchsetzung und Einhaltung der Sicherheitsmaßnahmen gewährleisten. Auf diese drei organisatorischen Maßnahmen haben wir noch einmal gesondert in denjenigen technischen Sicherheitsmaßnahmen verwiesen, bei denen die Gefahr besonders groß ist, dass Nutzer diese aus Bequemlichkeitsgründen nicht anwenden.

Tab. 4-1 zeigt einen Auszug aus dem Sicherheitsmaßnahmenkatalog. Der vollständige Sicherheitsmaßnahmenkatalog befindet sich im Anhang A.3.

Nr.	Sicherheitsmaßnahme	verfolgte Sicherheits-ziele	Bemerkung (Quellenangabe, Bsp. für Sicherheitslösungen)
	Technische Sicherheitsmaßnahmen		
	Maßnahmen für die Kommunikationssicherheit		
TM 2	**(Sprach-)Datenverbindungsverschlüsselung einsetzen (Ende-zu-Ende-Verschlüsselung):** Eine Verschlüsselung der Datenübertragung (bei WLAN BT GSM/UMTS) ist zwingend notwendig. Sofern die Verschlüsselung nicht bereits von den verwendeten Server- und Client-Komponenten vorgesehen ist, muss eine dienstunabhängige Lösung mit Crypto-Sprach-Ein-Ausgabemodulen (Hardware) oder Crypto-Software (z. B. mittels VPN-Tunnel o. ä.) implementiert werden. (Einhaltung dieser Maßnahme mittels der Maßnahmen OM 5, OM 6 und OM 7 gewährleisten.)	VT, IN, VB, AN	Vgl. [BSI08a, 25] Bsp.: CORISECIO Mobile Suite – Enterprise, TheGreenBow VPN Mobile, Cellcrypt Mobile for Blackberry, Cryptophone, T-Systems - SiMKo 2
	Organisatorische Sicherheitsmaßnahmen		
OM 5	**Nutzer im Umgang mit den Sicherheitsmaßnahmen schulen:** Die Nutzer müssen mit der Bedienung und den Funktionen der Sicherheitsmechanismen vertraut gemacht werden. Kann ein Nutzer z. B. nicht mit einem VPN-Client umgehen, so wird er diesen auch nicht benutzen, sondern eine unsichere Verbindung aufbauen.	VF	
OM 6	**Nutzer zur Einhaltung und Anwendung von Sicherheitsmaßnahmen verpflichten:** Auch wenn ein Nutzer wie in den Maßnahmen OM 5 und 6 für die Sicherheitsmaßnahmen sensibilisiert und geschult wurde, so kann er dennoch versuchen, gewisse "lästige" Maßnahmen abzuschalten. Daher sollten Mitarbeiter zusätzlich durch organisatorische Regelungen oder durch rechtliche Verpflichtungen (Arbeitsvertrag etc.) dazu angehalten werden, etablierte Sicherheitsmaßnahmen anzuwenden.	VF	
OM 7	**Nutzer für den Umgang mit sensiblen Daten schulen:** Schulung und Sensibilisierung der Nutzer im Umgang mit sensiblen Daten vornehmen; insbesondere bezogen auf das Mitführen sensibler Daten auf mobilen Endgeräten; Es sollten nur immer die Daten das Unternehmen verlassen, die auch wirklich benötigt werden. Mittel- und langfristig nicht benötigte Daten sollten von den mobilen Endgeräten unwiederbringlich gelöscht werden. (In diesem Zusammenhang ist Maßnahme TM 24 zu beachten.) Zum Umgang mit sensiblen Daten zählen nicht nur elektronische Dokumente, sondern auch alle anderen Daten und Informationen das Unternehmen betreffend (bspw. verwendete Hardware, verwendete Software, Zugangsdaten, zyklische Erneuerung von Zugangsdaten etc.).	VT, AU, VB, AN	

Tab. 4-1: Auszug aus dem Sicherheitsmaßnahmenkatalog

4.3 Kreuzreferenztabellen

Welche Sicherheitsmaßnahmen welche Bedrohungen mindern bzw. abwenden können, haben wir in Form von Kreuzreferenztabellen dargestellt. Sie ermöglicht eine bessere Übersicht der bereits im Bedrohungskatalog vorgenommenen Zuordnung der 70 Sicherheitsmaßnahmen zu den 221 Bedrohungen. Die Zuordnung erfolgte einerseits auf Grundlage von Plausibilitätsüberlegungen und andererseits objektiv anhand der jeweils beeinträchtigten bzw. verfolgten Sicherheitsziele der Bedrohungen bzw. Maßnahmen.

Die Kreuzreferenztabellen zeigen, dass 160 Bedrohungen mit Hilfe einer oder sogar mehrerer Sicherheitsmaßnahmen verhindert bzw. abgeschwächt werden können. Für 61 Bedrohungen konnten wir jedoch keine adäquaten Sicherheitsmaßnahmen finden.

Die vollständigen Kreuzreferenztabellen sind dem Anhang A-4 zu entnehmen.

5 Schlussbemerkungen

Der Einsatz mobiler Endgeräte und mobiler Datenübertragungen nimmt zu [IDC09]. Damit verbunden sind häufig Sicherheitsdefizite, da im mobilen Umfeld viele Bedrohungen und Schwachstellen existieren, die durch Angreifer gezielt ausgenutzt werden können [BSI06, 17 ff.; BSI08a, 21 ff.]. Es ist daher zwingend erforderlich, mobile Endgeräte und die von ihnen genutzten Dienste bei der Erstellung von Sicherheitskonzepten in Unternehmen und Behörden mit zu berücksichtigen und entsprechend ausreichende Sicherheitsmaßnahmen zu ergreifen.

Für die sichere Gestaltung mobiler Datenübertragungen haben wir einen Katalog von Sicherheitsmaßnahmen entwickelt. Hierzu strukturieren wir den Untersuchungsgegenstand „mobile Datenübertragung“ in die Betrachtungsebenen Infrastrukturebene, technische Ebene (mit Hard- und Software) sowie organisatorische und Nutzer-Ebene. Mit Hilfe einer Bedrohungsanalyse konnten wir typische Bedrohungen bei mobilen Datenübertragungen ermitteln und diese in Form von Bedrohungsbäumen dokumentieren. Wir konzentrierten uns hierbei auf die Systeme, die an der Datenübertragung direkt beteiligt sind: mobiles Endgerät, Mobilfunknetz (GSM/UMTS), Internet und lokales Unternehmensnetzwerk. Für jede Bedrohung haben wir untersucht, zu welchen Konsequenzen/Folgen diese führen kann und welche Sicherheitsziele dadurch gefährdet werden. Unser Bedrohungskatalog enthält 221 Bedrohungen. Auf Grundlage einer Literaturrecherche und Expertengesprächen ermit-

telten wir Sicherheitsmaßnahmen, die geeignet sind, die dokumentierten Bedrohungen zu verringern bzw. zu beseitigen. Unser Maßnahmenkatalog umfasst 70 Sicherheitsmaßnahmen, die wir in technische und organisatorische Maßnahmen untergliedern. Mit Hilfe von Kreuzreferenztabellen konnten wir abschließend darstellen, dass nicht für alle Bedrohungen adäquate Sicherheitsmaßnahmen zur Verfügung stehen.

Mit Hilfe der Bedrohungsanalyse konnten wir eine große Anzahl von Bedrohungen und Schwachstellen bei der mobilen Datenübertragung aufdecken und bewerten. Die Verwendung von Bedrohungsbäumen ermöglichte uns hierbei ein strukturiertes und nachvollziehbares Vorgehen. Jedoch nehmen wir nicht an, dass wir alle möglichen Bedrohungen und vorhandenen Schwachstellen bei der mobilen Datenübertragung dokumentiert haben. Allein schon durch die von uns vorgenommene Eingrenzung der betrachteten sicherheitsrelevanten Elemente (vgl. Abschnitte 2.4 und 3.2) war das nicht möglich. Des Weiteren gehen wir davon aus, dass Angreifer immer neue Wege und Techniken finden werden, um mobile Systeme zu gefährden. Auch die stetigen technischen Weiterentwicklungen (neue Endgeräte, Betriebssysteme, Dienste etc.) verändern die Bedrohungssituation. Eine der aktuell größten Veränderungen im mobilen Bereich ist die Einführung der vierten Generation von Mobilfunknetze, die auf der neuen Funktechnologie Long Term Evolution (LTE) basieren. Für diese LTE-Mobilfunknetze bleibt zu hoffen, dass bekannte Schwachstellen aus den GSM- und UMTS-Netzen beseitigt wurden. Es ist jedoch auch denkbar, dass neue Schwachstellen hinzukommen werden. Vergleichbare Weiterentwicklungen gibt es natürlich aber auch in Bezug auf das Angebot an Sicherheitsmaßnahmen. Ein Beispiel für neuartige Ansätze sind Mobile Honeypots bzw. Mobile Honeynets [Müll08, 283]. Sie sollen Angreifer von ihren eigentlichen Zielobjekten ablenken bzw. helfen, deren Angriffsmethoden zu analysieren.

Folglich ist ein ständige und zeitlich der Geschwindigkeit des technischen Fortschritts angepasste Überprüfung der Sicherheit der eingesetzten Systeme für mobile Datenübertragungen zwingend notwendig. Nur so kann auf neue Bedrohungen und Sicherungsmaßnahmen reagiert werden. Ausgehend davon sind die Bedrohungs- und Maßnahmenkataloge zu pflegen und ggf. zu erweitern.

Literaturverzeichnis

[AbMü09] Abts, D.; Mülder, W.: Grundkurs Wirtschaftsinformatik - Eine kompakte und praxisorientierte Einführung. 6. Auflage, Vieweg+Teubner, Wiesbaden 2009.

[Ahle09] Ahlers, E.: Performance-Patch für den BlackBerry entpuppt sich als Schnüffelware. Hannover 2009, http://www.heise.de/mobil/meldung/Performance-Patch-fuer-den-Blackberry-entpuppt-sich-als-Schnueffelware-6869.html, Abruf: 2010-09-09.

[AKHa03] Ahrens, P.; Karpf, K.; Hausner, W. (Hrsg.): GSM Basics – Die Grundkonzepte des Global System for Mobile Communications. Schlembach-Fachverl., Wilburgstetten 2003.

[Alby08] Alby, T.: Das mobile Web. Carl Hanser Verlag, München 2008.

[Alex06] Alexander, M.: Netzwerke und Netzwerksicherheit - Das Lehrbuch. Hüthig Verlag, Heidelberg 2006.

[Augu09] Augsten, S.: Schadcode für Symbian-OS verbreitet sich via SMS. o.O. 2009, http://www.searchsecurity.de/themenbereiche/bedrohungen/viren-wuermer-trojaner/articles/171785/, Abruf: 2011-05-14.

[Bach05] Bachfeld, D.: Forscher knacken Bluetooth-PINs gekoppelter Geräte. Hannover 2005, http://www.heise.de/newsticker/meldung/Forscher-knacken-Bluetooth-PINs-gekoppelter-Geraete-Update-108140.html, Abruf: 2009-10-12.

[Bach07a] Bachfeld, D.: Bluetooth-Sniffing für Jedermann. Hannover 2007, http://www.heise.de/security/meldung/Bluetooth-Sniffing-fuer-Jedermann-164061.html, Abruf: 2011-04-28.

[Bach07b] Bachfeld, D.: Windows-Mobile-Anwendungen anfällig für DoS-Angriffe. Hannover 2007, http://www.heise.de/newsticker/meldung/Windows-Mobile-Anwendungen-anfaellig-fuer-DoS-Angriffe-140524.html, Abruf: 2009-09-14.

[Bach09] Bachfeld, D.: Bluetooth-Lücke in Windows Mobile ermöglicht Zugriff auf beliebige Dateien. Hannover 2009, http://www.heise.de/security/

meldung/Bluetooth-Luecke-in-Windows-Mobile-ermoeglicht-Zugriff-auf-beliebige-Dateien-202873.html, Abruf: 2011-05-02.

[Back07] Back, W.: Die doppelte SIM-Karte. o.O. 2007, http://www.cczwei.de/index.php?blogid=83&id=blog, Abruf: 2011-04-14.

[BGTe04] Banet, F.-J.; Gärtner, A.; Teßmar, G.: UMTS - Netztechnik, Dienstarchitektur, Evolution. Hüthig Verlag, Bonn 2004.

[BITK03] Bundesverband für Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) (Hrsg.): Sicherheit für Systeme und Netze in Unternehmen. 2. Aufl., Berlin 2003, http://www.bitkom.org/files/ documents/acf897.pdf, Abruf: 2009-06-24.

[Bran05] Brands, G.: IT-Sicherheitsmanagement - Protokolle, Netzwerksicherheit, Prozessorganisation. Springer, Berlin 2005.

[BSI03] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Kommunikations- und Informationstechnik 2010+3: Neue Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit. Bonn 2003, https://www.bsi-fuer-buerger.de/ContentBSI/Publikationen/Studien/trend2010/index_htm.html, Abruf: 2010-05-25.

[BSI06] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Mobile Endgeräte und mobile Applikationen - Sicherheitsgefährdungen und Schutzmaßnahmen. Bonn 2006, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/MobilEndgeraete/mobile_endgeraete_pdf.pdf?__blob=publicationFile, Abruf: 2011-05-14.

[BSI08a] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte. Bonn 2008, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/OeffentlMobilfunk/oefmobil_pdf.pdf?__blob=publicationFile, Abruf: 2011-04-09.

[BSI08b] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Common Criteria Protection Profile, Mobile Synchronisation Services (MSS PP) - BSI-CC-PP-0048. Bonn 2008, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ReportePP/pp0048b_pdf.pdf?__blob=publicationFile, Abruf: 2011-05-05.

[BSI09] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutzkataloge. 11. Aufl., Bundesanzeiger, Köln 2009.

[BSI10] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Mobile Endgeräte. o.O. o.J., https://www.bsi.bund.de/DE/Themen/weitere Themen/MobileSecurity/MobileEndgeraete/mobileendgeraete_node.html, Abruf: 2011-01-22.

[BSI92] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Sicherheitshandbuch: Handbuch für die sichere Anwendung der Informationstechnik. Bundesanzeiger, Köln 1992.

[DBCr01] Dunsmore, B.; Brown, J.; Cross, M.: Mission Critical! Internet Security. Syngress Publishing Inc., Rockland 2001.

[Detk06] Detken, K.-O.; Eren, E.: Bluetooth-Sicherheit - Schwachstellen und potentielle Angriffe. In: Horster, P. (Hrsg.): D.A.C.H Mobility 2006, syssec, Klagenfurt 2006, S.173-186.

[Detk97] Detken, K.-O.: GSM - Global System for Mobile Communication - DerMobilfunkstandard. Verlag Mainz, Aachen 1997.

[Diet04] Dietrich, K.: Sicherheitsanalyse - BlackBerry Mobile Data Service. Zentrum für sichere Informationstechnologie - Wien 2004, http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=19390, Abruf: 2010-12-09.

[Ecke08] Eckert, C.: IT-Sicherheit: Konzepte – Verfahren – Protokolle. 5. Aufl., Oldenbourg Verlag, München 2008.

[EnWe08] Enz, R.; Weber, J.: Sicherheitskonzepte von Symbian OS und Windows Mobile. Hannover 2008, http://www.heise.de/developer/artikel/Sicherheitskonzepte-von-Symbian-OS-und-Windows-Mobile-227118.html, Abruf: 2011-05-05.

[Enz07] Enz, R.: Sicherheit mobiler Plattformen - Ein technischer Überblick über Symbian OS und Windows Mobile. o.O. 2007, http://www.securitymanager.de/magazin/artikel_1622_sicherheit_mobiler_plattformen_teil_1.html, http://www.securitymanager.de/magazin/artikel_1630_sicherheit_mobiler_plattformen_teil_2.html, Abruf: 2009-09-28.

[Eren07] Eren, E.: VoIP Security: Konzepte und Lösungen für sichere VoIP-Kommunikation. Hanser Fachbuch, München 2007.

[Erte07] Ertel, W.: Angewandte Kryptographie. 2. Aufl., Carl Hanser Verlag, München 2007.

[Espo09] Esponda, M.: Betriebssysteme - Schutz und Sicherheit. Berlin 2009, http://www.esponda.de/BS_09/slides/BS_V17_Sicherheit_Teil_1.pdf, Abruf: 2009-10-29.

[Fede99] Federrath, H.: Sicherheit mobiler Kommunikation: Schutz in GSM-Netzen, Mobilitätsmanagement und mehrseitige Sicherheit. Vieweg Verlag, Braunschweig 1999.

[FePf00] Federrath, H.; Pfitzmann, A.: Schutzziele in IT-Systemen. In: Datenschutz und Datensicherheit, Nr. 12 (2000), S. 704-710.

[FiMa10] Fischer, D.; Markscheffel, B.: The German Wireless LAN Security Survey 2009 – How Security Measures are used in Companies and Federal Authorities? In: International Journal for Infonomics (IJI), Volume 3, Issue 2 (2010), S. 383-392.

[Fisc06] Fischer, K.: Konzeption und Entwicklung eines Hilfsmittels zur Auswahl von Maßnahmen zur Sicherung von Wireless LAN-Infrastrukturen. TU Ilmenau, Ilmenau 2006.

[Fisc08] Fischer, S.: Der Fischer Weltalmanach 2008. Fischer Taschenbuch Verlag, Frankfurt am Main 2008. http://www.bpb.de/wissen/VWWV1X,5,0, Griechenland.html#art5, Abruf: 2009-09-09.

[Fox02] Fox, D.: Der IMSI-Cacher. In: DuD – Datenschutz und Sicherheit Nr. 26 (2002), S. 212-215.

[Fox05] Fox, D.: BlackBerry Security, Das Sicherheitskonzept – Übersicht und-Bewertung. In: DuD – Datenschutz und Sicherheit, Nr. 29 (2005), S. 647-650.

[FRRö00] Fischer, S.; Rensing, C.; Rödig, U.: Open Internet Security. Springer, Berlin, Heidelberg, New York 2000.

[FSKr06] Fischer, D.; Stelzer, D.; Kreyßel, D.: Verbreitung und Sicherheit von Wireless LAN-Infrastrukturen – Eine empirische Untersuchung unter deutschen Unternehmen und Behörden. In: Ilmenauer Beiträge zur Wirtschaftsinformatik, Nr. 2006-03. Ilmenau 2006.

[Gart10] Gartner Inc.: Gartner Says Worldwide Mobile Phone Sales Grew 35 Percent in Third Quarter 2010; Smartphone Sales Increased 96 Percent. Press Release, o.O. November 2010, http://www.gartner.com/it/page.jsp?id= 1466313, Abruf: 2010-12-15.

[Gemp09] Gemplus: Mobile telecommunications - OTA (Over The Air). o.O. o.J., http://www.gemplus.com/pss/telecom/technos/ota/index.html, Abruf: 2009-08-13.

[Grie08] Grieser, F.: Malware für Windows Mobile, Symbian-Plattformen und Palm-OS. o.O. 2008, http://www.searchsecurity.de/themenbereiche/bedrohungen/viren-wuermer-trojaner/articles/61321/index.html, Abruf: 2011-04-14.

[Hemp09] Hempel, P.: Angriff auf Symbian S60 Handys per SMS. o.O. 2009, http://www.searchsecurity.de/themenbereiche/applikationssicherheit/kommunikations-sicherheit/articles/166511/, Abruf: 2011-04-14.

[Hinz06] Walter Hinz: Zur Sicherheit von neuen Chipkartenbetriebssystemen. In: Horster, P. (Hrsg.): D.A.C.H Security 2006, syssec, Klagenfurt 2006, S. 292-301.

[Hump04] Humpert, F.: IT-Sicherheit. In: HMD – Praxis in der Wirtschaftsinformatik. Nr. 236 (April 2004), S. 7-18.

[Hunt98] Hunt, C.: TCP/IP Netzwerk Administration. 2. Aufl., O'Reilly Verlag, Köln 1998.

[IDC09] IDC Central Europe GmbH (Hrsg.): IT-Sicherheit bei mobilen Endgeräten und bei drahtloser Datenübertragung: Status Quo und Trends in Deutschland 2008/2009. Frankfurt am Main 2009.

[ITU91] International Telecommunication Union: X.800, Security Architecture for Open Systems Interconnection for CCITT Applications, 1991.

[Jano07] Janowicz, K.: Sicherheit im Internet. 3. Aufl., O'Reilly, Beijing [u.a.] 2007.

[Jung02] Jung, V.: Handbuch für die Telekommunikation. 2. Auflage, Springer, Berlin 2002.

[Kapp07] Kappes, M.: Netzwerk- und Datensicherheit - Eine praktische Einführung. Vieweg Verlag, Braunschweig 2007.

[Kism11] KISMET: Homepage. http://www.kismetwireless.net, o.O., o. J., Abruf: 2011-05-02.

[KrWe07] Kraft, P.; Weyert, A.: Network Hacking. Franzis Verlag, Poing 2007.

[Mart73] Martin, J.: Security, Accuracy and Privacy in Computer Systems. Prentice-Hall PTR, Englewood Cliffs 1973.

[MeWe04] Meyer, U.; Wetzel, S.: A Man-in-the-Middle Attack on UMTS. In: Proceedings of the 2004 ACM Workshop on Wireless Security. Philadelphia, Pennsylvania, 2004, S. 90-97, http://www.cdc.informatik.tu-darmstadt.de/~umeyer/umts-mim.pdf, Abruf: 2011-05-11.

[Micr10a] Microsoft TechNet: Security Roles for Windows Mobile 5.0 and Windows Mobile 6. o.O. 2010, http://technet.microsoft.com/en-us/library/cc182289.aspx, Abruf: 2010-12-15.

[Micr10b] Microsoft TechNet: Security Policies for Windows Mobile 5.0 and Windows Mobile 6. , o.O. 2010, http://technet.microsoft.com/en-us/library/cc182305.aspx, Abruf: 2010-12-15.

[Müll08] Müller, K.-R.: IT-Sicherheit mit System. 3. Aufl., Vieweg & Sohn Verlag, Wiesbaden 2008.

[NETZW09] o.V.: Handy-Ortung: Spionieren mit dem Mobiltelefon. Hamburg 2009, http://www.netzwelt.de/news/71963-handy-ortung-spionieren-mobiltelefon.html, Abruf: 2009-10-11.

[neue09] neues-Magazin: Handy-Blocker. o.O. o.J., http://www.3sat.de/page/?source=/neues/sendungen/magazin/84041/index.html, Abruf: 2009-08-05.

[O'Co07] O'Connor, J.: Attack Surface - Analysis of BlackBerry Devices. Ireland 2007, http://www.symantec.com/avcenter/reference/attack.surface.analysis.of.blackberry.devices.pdf, Abruf: 2011-05-09.

[Oech03] Oechslin, P.: Making a Faster Cryptanalytic Time-Memory Trade-Off. In: The 23rd Annual International Cryptology Conference, CRYPTO '03, Vol. 2729, Santa Barbara, California 2003, S. 617-630, http://lasecwww.epfl.ch/pub/lasec/doc/Oech03.pdf, Abruf: 2011-05-29.

[Open08] OpenMobileBlog.com: Modding - S60 hacked! http://www.symbian60.mobi/2008/05/06/modding-s60-hacked, o.O. 06.05.2008, Abruf: 2009-12-02.

[Papa06] Papagrigoriou, P.: Smart Card und sichere Anwendungen für Smartphones und PDAs. In: Horster, P. (Hrsg.): D.A.C.H Mobility 2006, syssec, Klagenfurt 2006, S. 257-268.

[RaEf08] Rankl, W.; Effing, W.: Handbuch der Chipkarten. 5. Aufl., Carl Hanser Verlag, München 2008.

[Raep01] Raepple, M.: Sicherheitskonzepte für das Internet -Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung. 2. Aufl., dpunkt-Verlag, Heidelberg 2001.

[Rieg05] Rieger, H.: IT-Sicherheit – Risiken und Gefährdungspotentiale. In: Schoolmann, J.; Rieger, H. [Hrsg.]: Praxishandbuch IT-Sicherheit : Risiken, Prozesse, Standards. Symposion Publishing, Düsseldorf 2005, S. 19-36.

[Ries09] Ries, U.: Per SMS Handy-Websessions entführen. Hannover 2009, http://www.heise.de/security/meldung/Per-SMS-Handy-Websessions-entfuehren-213779.html, Abruf: 2009-09-28.

[Ruck06] Ruck, M.: Mobile Endgeräte: Fluch oder Segen? In: Horster, P. (Hrsg.): D.A.C.H Mobility 2006, syssec, Klagenfurt 2006, S. 1-12.

[Rütt07] Rütten, C.: Lauschgelegenheit - Handy-Gespräche bald abhörbar. In: c't Magazin Nr. 24/07, Hannover 2007, http://www.heise.de/ct/Abhoerziel-Handy--/artikel/126270, Abruf: 2011-05-24.

[Sack08] Sackmann, S.: IT-Sicherheit. In: Kurbel, K.; Becker, J.; Gronau, N.; Sinz, E.; Suhl, L. (Hrsg.): Enzyklopädie der Wirtschaftsinformatik – Online-Lexikon. 4. Auflage. Oldenbourg, München 2008. http://www.enzyklopaedie-der-wirtschaftsinformatik.de/wi-enzyklopaedie/lexikon/technologien-methoden/Informatik--Grundlagen/IT-Sicherheit, Abruf: 2010-12-20.

[SACO06] Shorey, R.; Ananda, A.; Chan, M. C.; Ooi, W. T.: Mobile, Wireless, and Sensor Networks: Technology, Applications, and Future Directions. Wiley-IEEE Press, Hoboken, NJ 2006.

[Saut08] Sauter, M.: Grundkurs Mobile Kommunikationssysteme - Von UMTS und HSDPA, GSM und GPRS zu Wireless LAN und Bluetooth Piconetzen. 3. Aufl., Vieweg & Sohn Verlag, Wiesbaden 2008.

[Schä03] Schäfer, G.: Netzsicherheit. dpunkt-Verlag, Heidelberg 2003.

[Schn04] Schneier, B.: Secrets & Lies: IT-Sicherheit in einer vernetzten Welt. dpunkt-Verlag, Heidelberg 2004.

[Schn99] Schneier, B.: Attack Trees. o. O. 1999, http://www.schneier.com/paper-attacktrees-ddj-ft.html, Abruf: 2010-12-18.

[Schw05] Schwenk, J.: Sicherheit und Kryptographie im Internet - Von sicherer E-Mail bis zu IP-Verschlüsselung. 2. Aufl., Vieweg Verlag, Braunschweig 2005.

[SESP11] SESP Group: Produktübersicht – Störsender. o. O. o. J., http://www.sesp.eu/Stoersender-Jammer-Mobilfunkblocker.htm, Abruf: 2011-05-03.

[ShWo05] Shaked, Y.; Wool, A.: Cracking the Bluetooth PIN. Proceeding MobiSys '05 Proceedings of the 3rd international conference on Mobile systems, applications, and services, o. O. 2005, S. 39-50, http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05, Abruf: 2011-05-02.

[Stei09] Steiner, M.: SMS-Angriffe bedrohen Smartphones - Cyberkriminelle kapern Handys über Kurznachrichten. Wien 2009, http://www.pressetext.com/news/20090420030, Abruf: 2010-09-28.

[Stel93] Stelzer, D.: Sicherheitsstrategien in der Informationsverarbeitung - Ein wissensbasiertes, objektorientiertes System für die Risikoanalyse. Deutscher Universitäts-Verlag, Wiesbaden 1993.

[Ster06] Sterzik, I. K.: Die Mobile Welt – Mobilkommunikation aus technischer, wirtschaftlicher und gesellschaftlicher Perspektive. VDM Verlag Dr. Müller, Saarbrücken 2006.

[StPO11] Bundesministerium der Justiz: Strafprozeßordnung. o.O. o. J., http://www.gesetze-im-internet.de/stpo, Abruf: 2011-05-02.

[Tech08] IDG Business Media GmbH - TecChannel: BlackBerry-Desktop-Software enthält kritische Lücke. München 2008, http://www.tecchannel.de/sicherheit/news/1778818/blackberry_desktop_software_enthaelt_kritische_luecke/index.html, Abruf: 2009-09-09.

[Tech09] IDG Business Media GmbH - TecChannel: BlackBerry: RIM warnt vor PDF-Sicherheitslücke im BES und Unite. München 2009, http://www.tecchannel.de/kommunikation/news/1782132/blackberry_rim_warnt_vor_pdf_sicherheitsluecke_im_bes_und_unite/index.html, Abruf: 2009-09-09.

[Tern05] Ternes, B.; Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Technische Richtlinie Sicheres WLAN. München 2005, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03103/TRS_WLAN_Praesentation_pdf.pdf?__blob=publicationFile, Abruf: 2011-05-08.

[THC11] The Hacker's Choice: Homepage. o.O. o. J., http://www.thc.org, Abruf: 2011-04-25.

[Wang09] Wang, J.: Computer network security - Theory and practice. Springer-Verlag, Berlin 2009.

[WaPi02] Wallbaum, M.; Pils C.: Technologische Grundlagen des Mobile Commerce. In: Teichmann, R.; Lehnert, F. (Hrsg.): Mobile Commerce - Strategien, Geschäftsmodelle, Fallstudien. Springer, Berlin 2002, S. 51-109.

[Webe08] Weber, V.: Indien will BlackBerry-Datenverkehr abhören. Hannover 2008, http://www.heise.de/security/meldung/Indien-will-BlackBerry-Datenverkehr-abhoeren-209016.html, Abruf: 2009-09-09.

[WeLu99] Weis, R.; Lucks, S.: Sicherheitsprobleme bei Authentifizierung und Verschlüsselung in GSM-Netzen. In: DuD – Datenschutz und Sicherheit Nr. 22 (1999), S. 1-4.

[Wiec02] Wiecker, M.: Endgeräte für mobile Anwendungen. In: Gora, W.; Röttger-Gerigk, S. (Hrsg.): Handbuch Mobile-Commerce - Technische Grundlagen, Marktchancen und Einsatzmöglichkeiten. Springer, Berlin 2002, S. 405-418.

[Wieh04] Wiehler, G.: Mobility, Security und Web Services: Neue Technologien und Service-orientierte Architekturen für zukunftsweisende IT-Lösungen. Publicis Corporate Publishing, Erlangen 2004.

[Witt96] Witt, B.C.: IT-Sicherheit kompakt und verständlich - Eine praxisorientierte Einführung. Vieweg, Wiesbaden 2006.

[Wurs04] Wurster, F.: Ein Werkzeug für Angriffsbäume. In: HMD – Praxis in der Wirtschaftsinformatik, April Nr. 236 (2004), S. 79-85.

[Zieg08] Ziegler, P. S.: Netzwerkangriffe von innen. O'Reilly Verlag, Köln 2008.

Anhang

A.1 Bedrohungsbäume

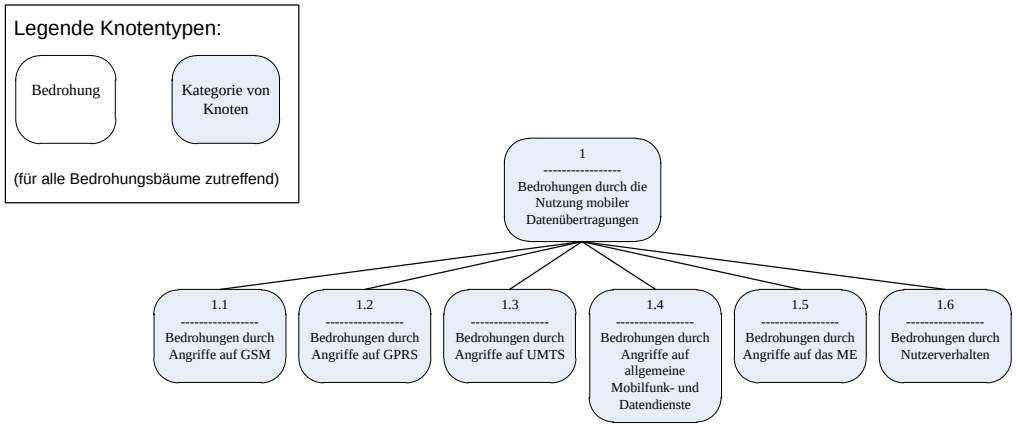

Abb. 5-1: Bedrohungen für mobile Datenübertragungen (Hauptbedrohungsbaum)

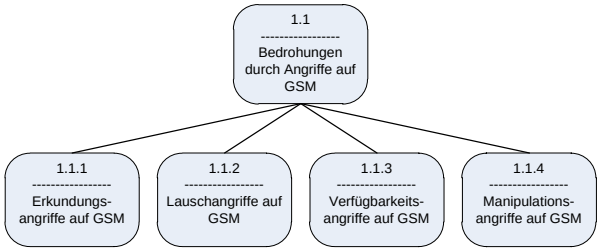

Abb. 5-2: Bedrohungen durch Angriffe auf GSM (grafisch)

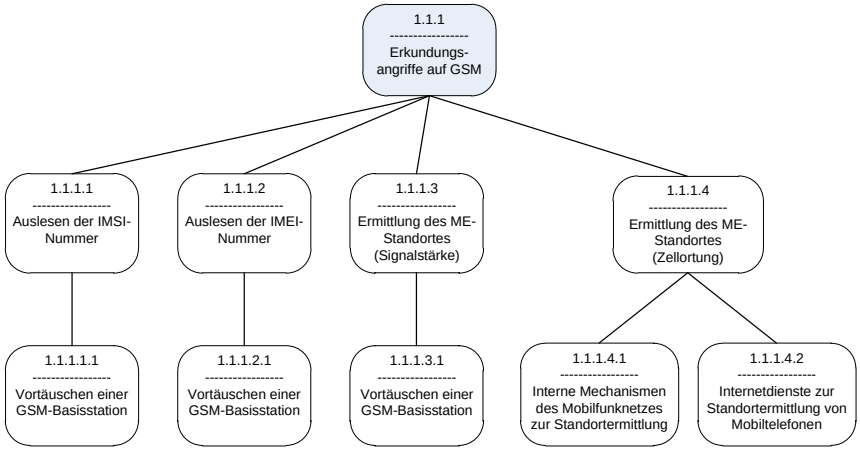

Abb. 5-3: Bedrohungen durch Erkundungsangriffe auf GSM (grafisch)

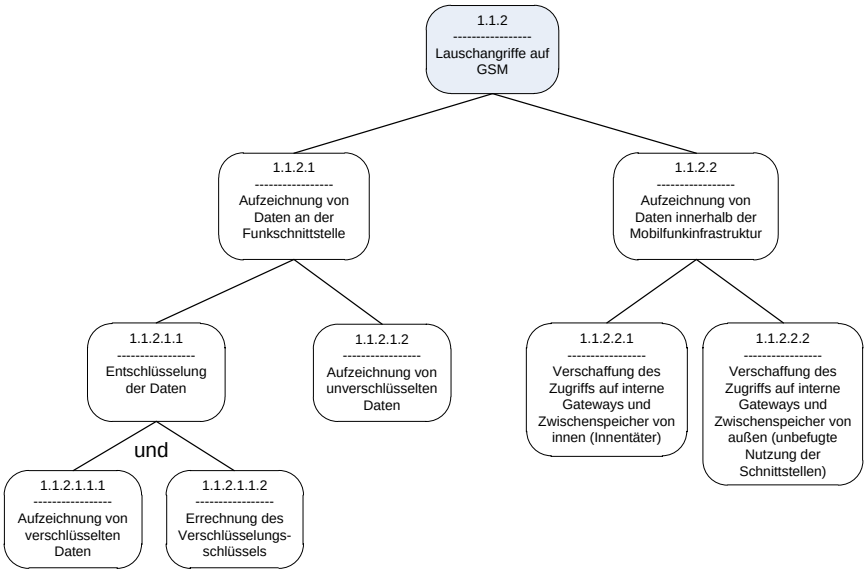

Abb. 5-4: Bedrohungen durch Lauschangriffe auf GSM (grafisch)

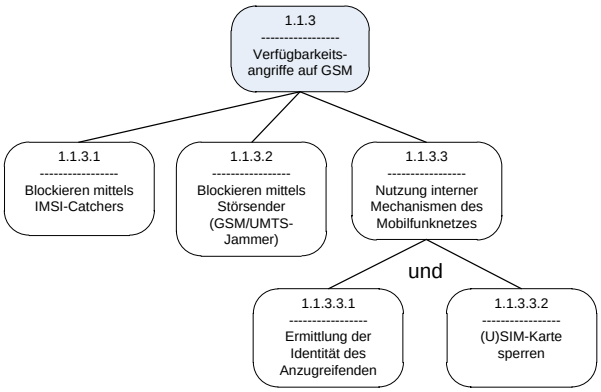

Abb. 5-5: Bedrohungen durch Verfügbarkeitsangriffe auf GSM (grafisch)

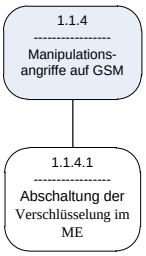

Abb. 5-6: Bedrohungen durch Manipulationsangriffe auf GSM (grafisch)

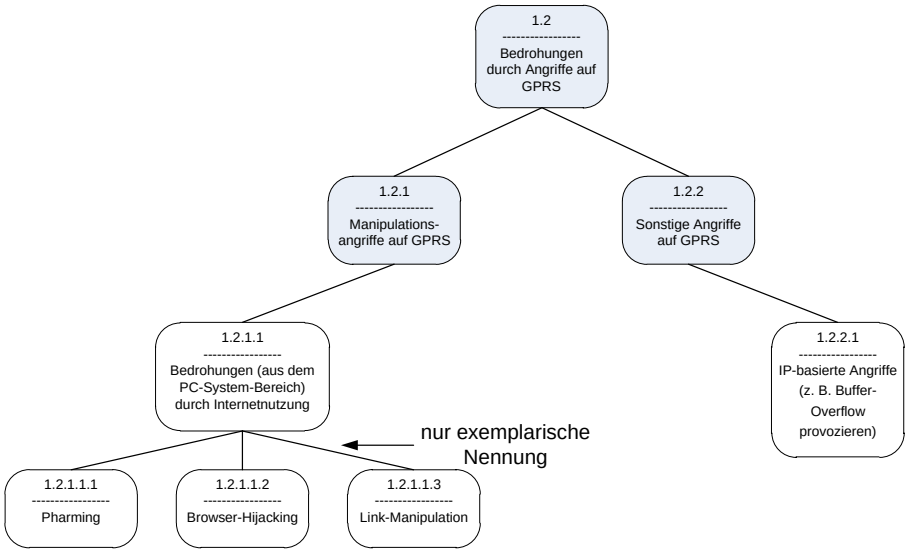

Abb. 5-7: Bedrohungen durch Angriffe auf GPRS (grafisch)

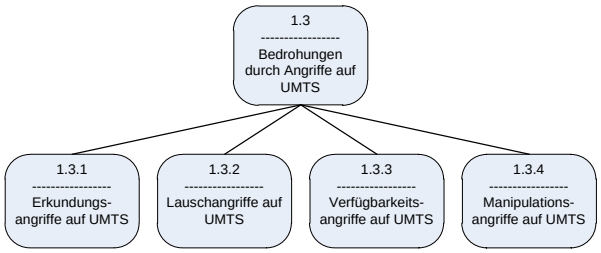

Abb. 5-8: Bedrohungen durch Angriffe auf UMTS (grafisch)

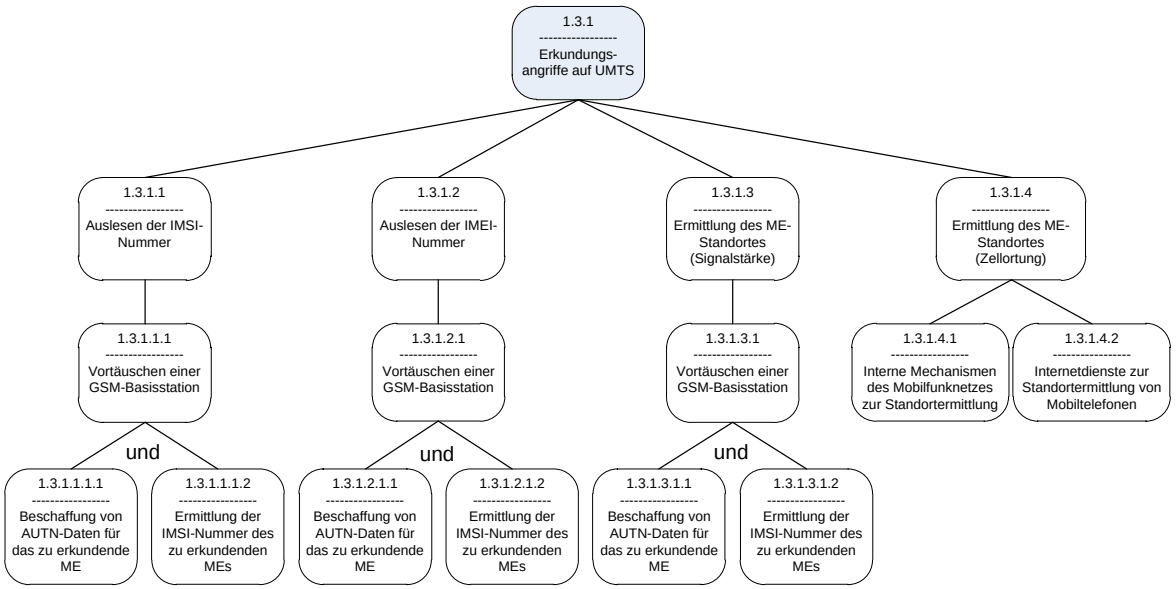

Abb. 5-9: Bedrohungen durch Erkundungsangriffe auf UMTS (grafisch)

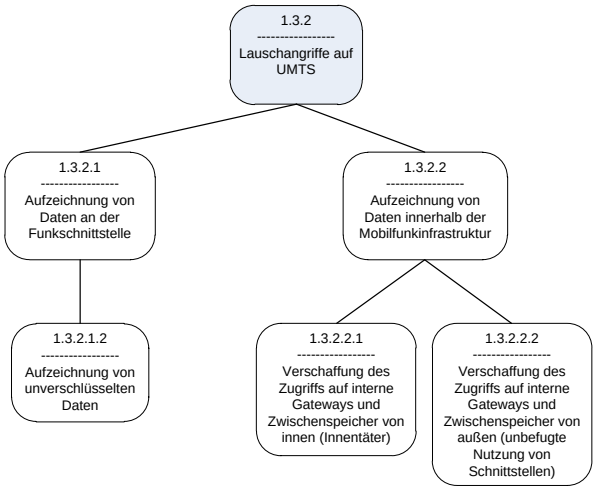

Abb. 5-10: Bedrohungen durch Lauschangriffe auf UMTS (grafisch)

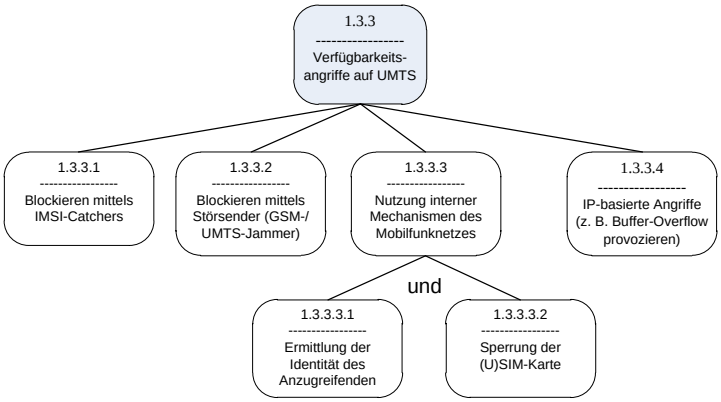

Abb. 5-11: Bedrohungen durch Verfügbarkeitsangriffe auf UMTS (grafisch)

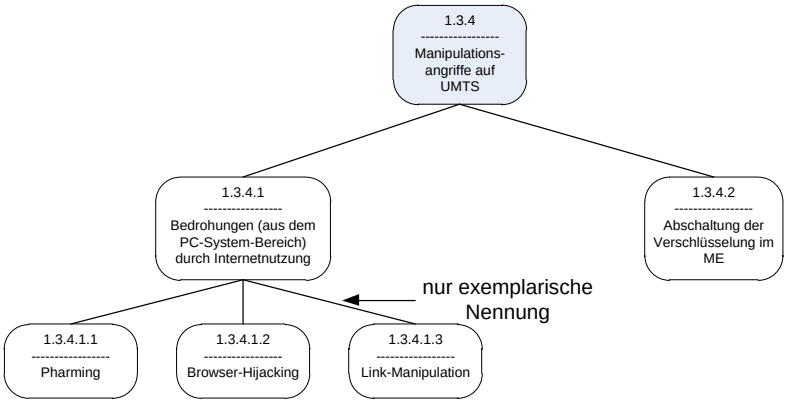

Abb. 5-12: Bedrohungen durch Manipulationssangriffe auf UMTS (grafisch)

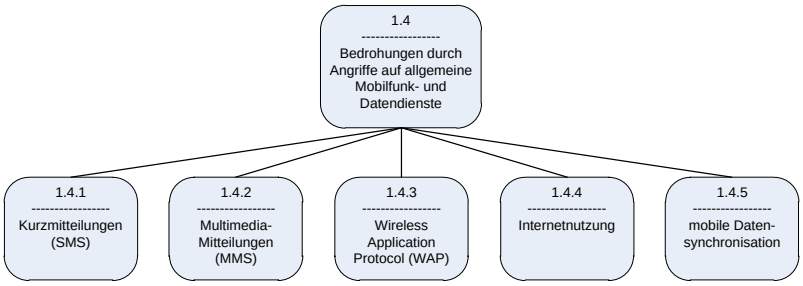

Abb. 5-13: Bedrohungen durch Angriffe auf allgemeine Mobilfunk- und Datendienste (grafisch)

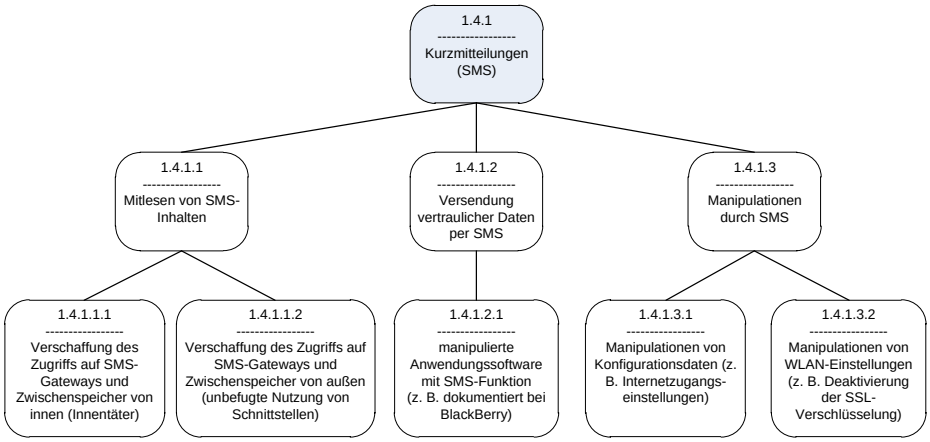

Abb. 5-14: Bedrohungen durch Bedrohungen durch Kurzmitteilungen (SMS) (grafisch)

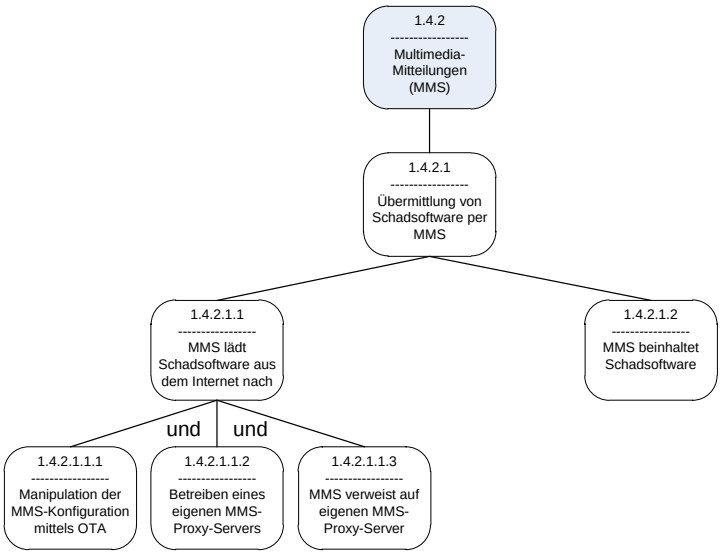

Abb. 5-15: Bedrohungen durch Multimedia-Mitteilungen (MMS) (grafisch)

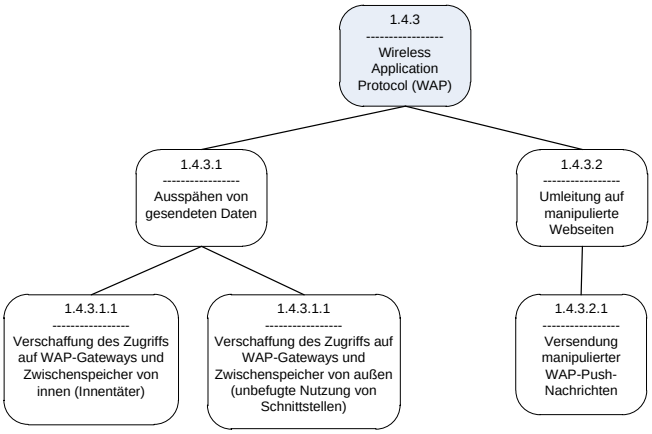

Abb. 5-16: Bedrohungen durch das Wireless Application Protocol (WAP) (grafisch)

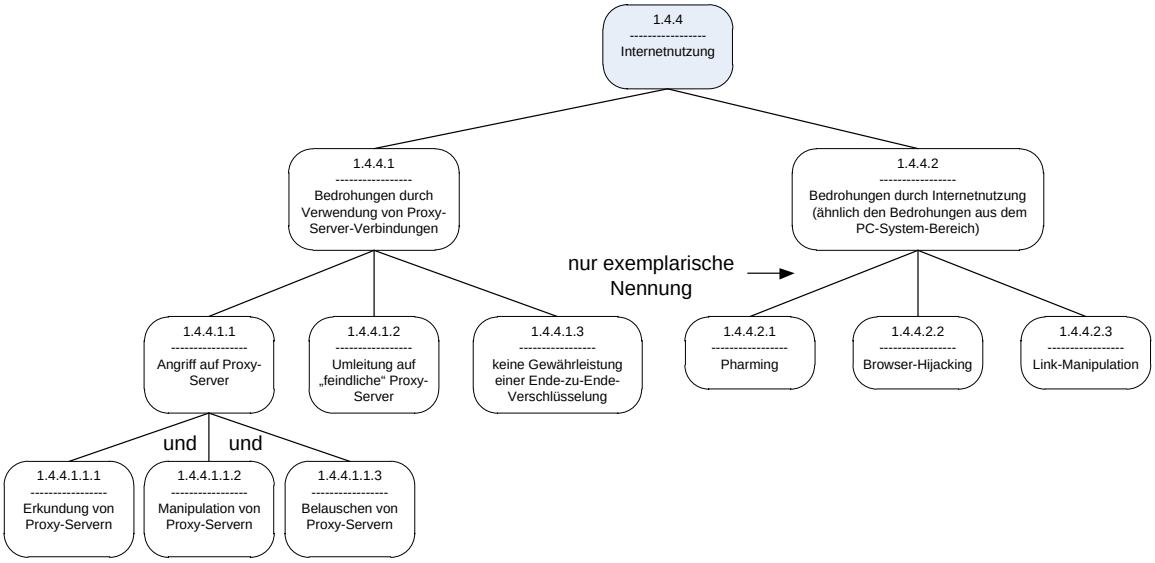

Abb. 5-17: Bedrohungen durch die Internetnutzung (grafisch)

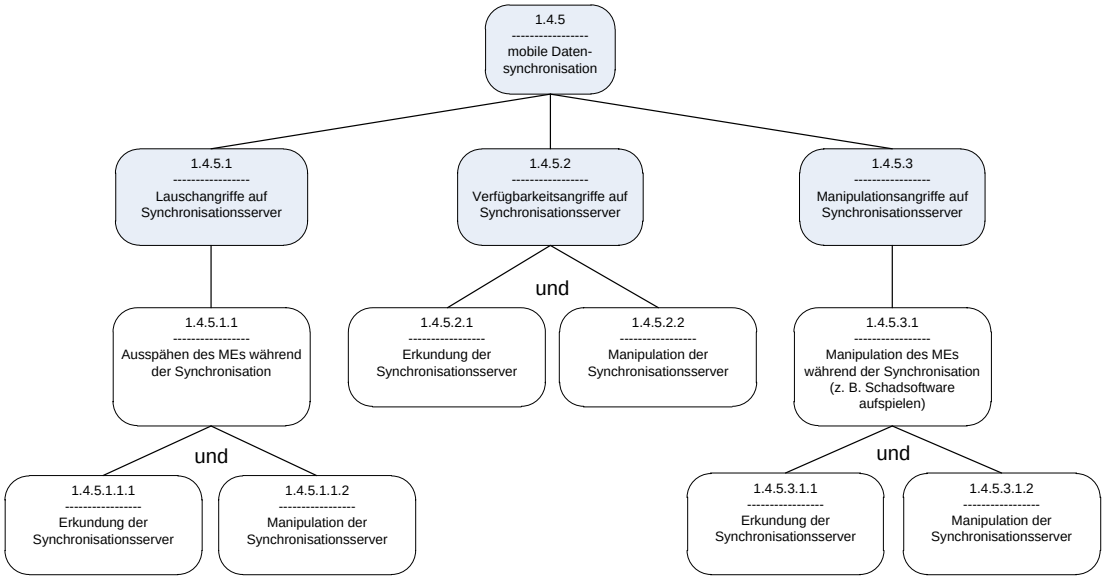

Abb. 5-18: Bedrohungen durch die mobile Datensynchronisation (grafisch)

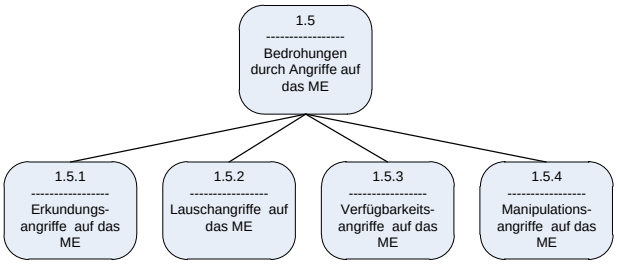

Abb. 5-19: Bedrohungen durch Angriffe auf das mobile Endgerät (grafisch)

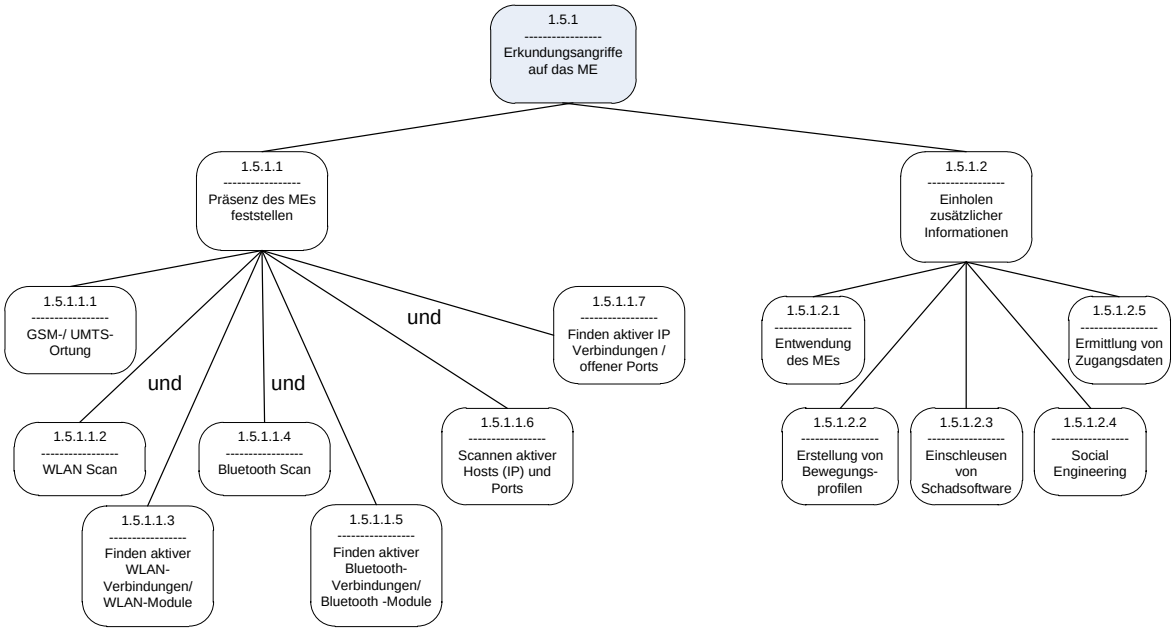

Abb. 5-20: Bedrohungen durch Erkundungsangriffe auf das mobile Endgerät (grafisch)

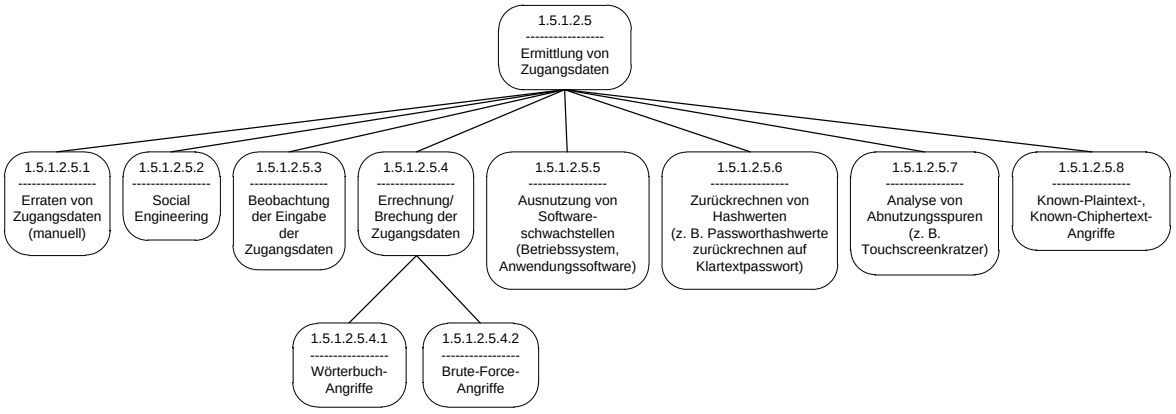

Abb. 5-21: Bedrohungen durch Ermittlung von Zugangsdaten (grafisch)

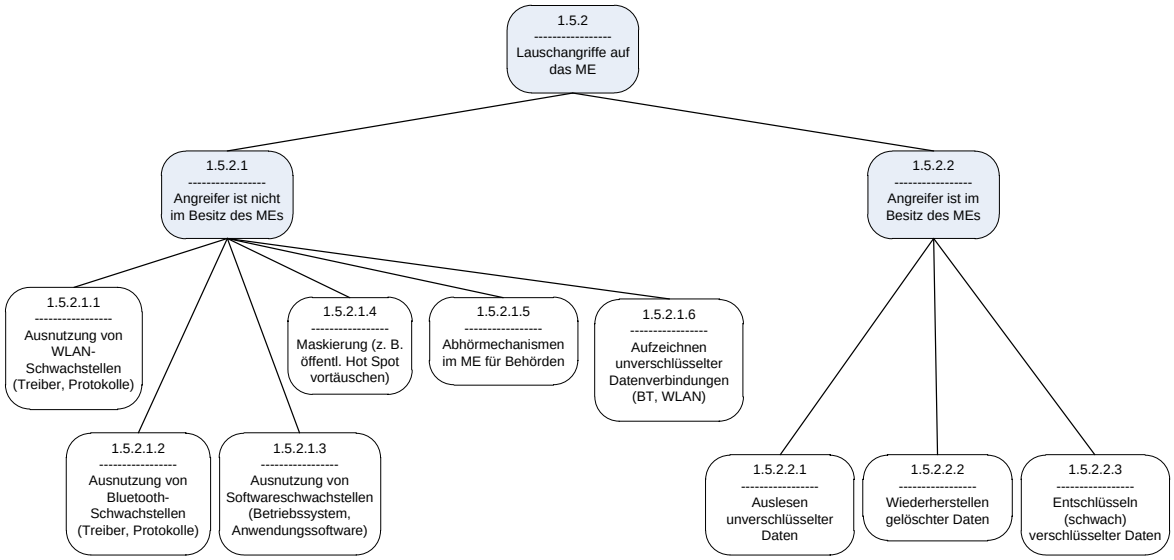

Abb. 5-22: Bedrohungen durch Lauschangriffe auf das mobile Endgerät (grafisch)

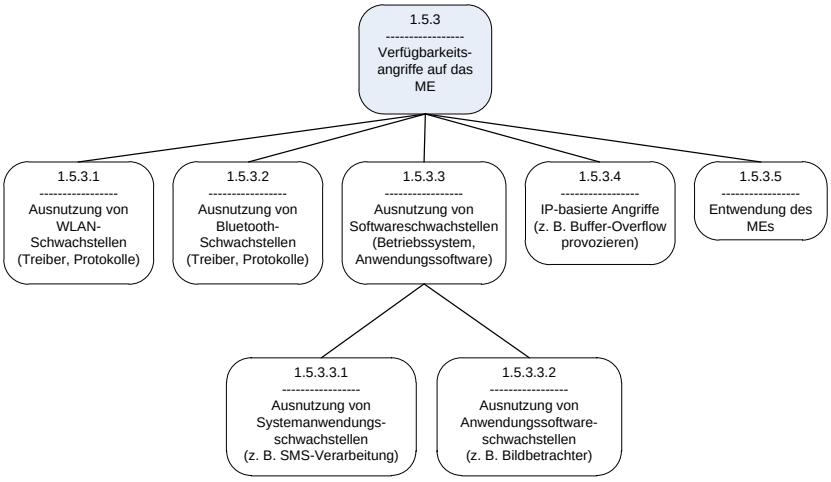

Abb. 5-23: Bedrohungen durch Verfügbarkeitsangriffe auf das mobile Endgerät (grafisch)

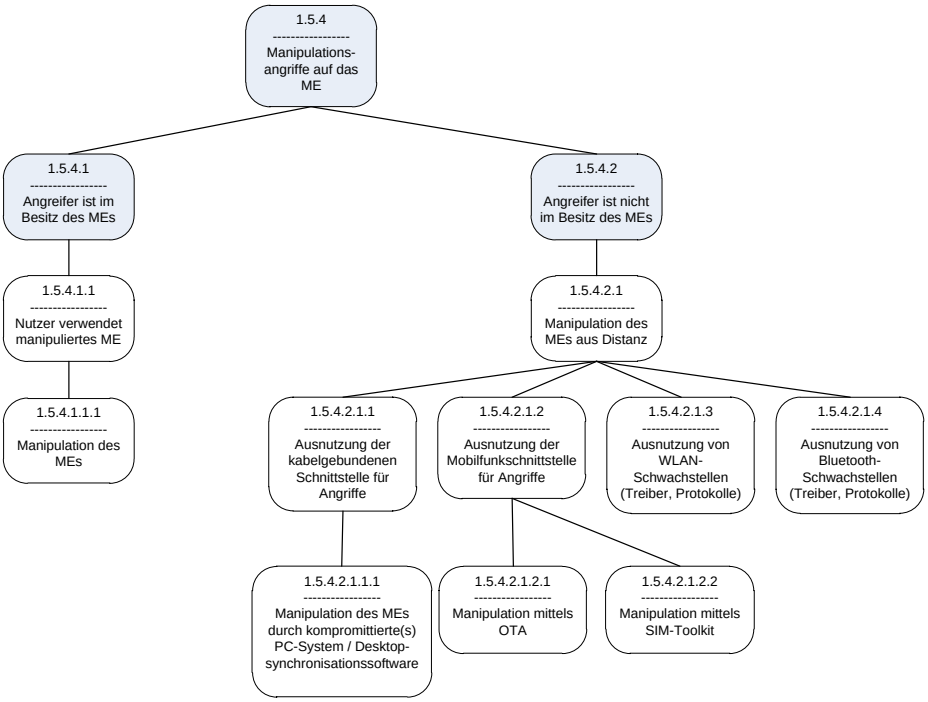

Abb. 5-24: Bedrohungen durch Manipulationsangriffe auf das mobile Endgerät (grafisch)

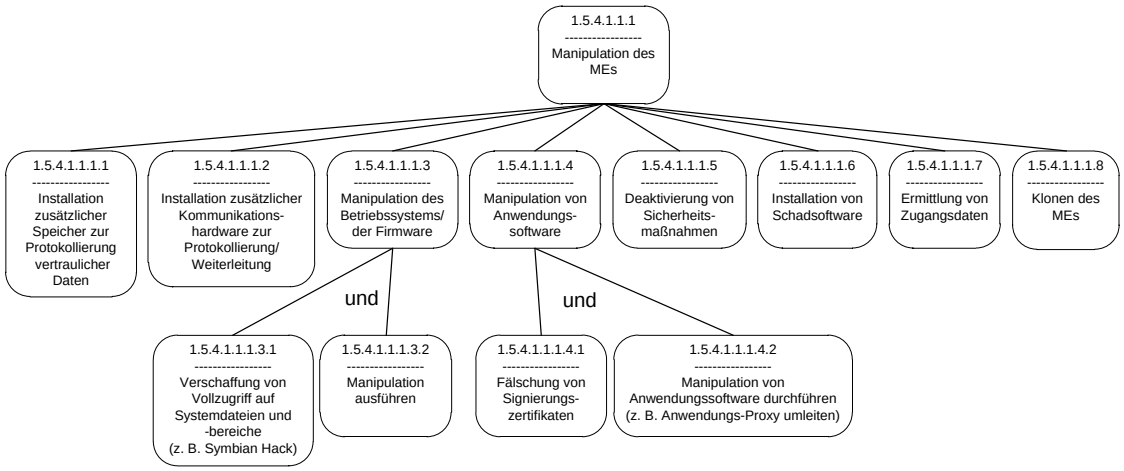

Abb. 5-25: Bedrohungen durch Manipulation des mobilen Endgerätes (grafisch)

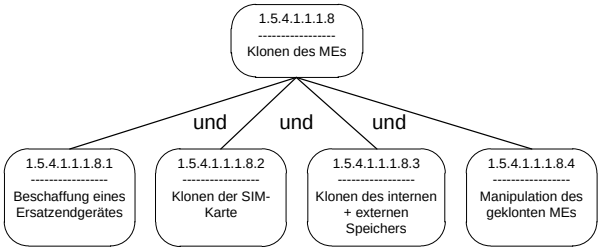

Abb. 5-26: Bedrohungen durch Klonen des mobilen Endgerätes (grafisch)

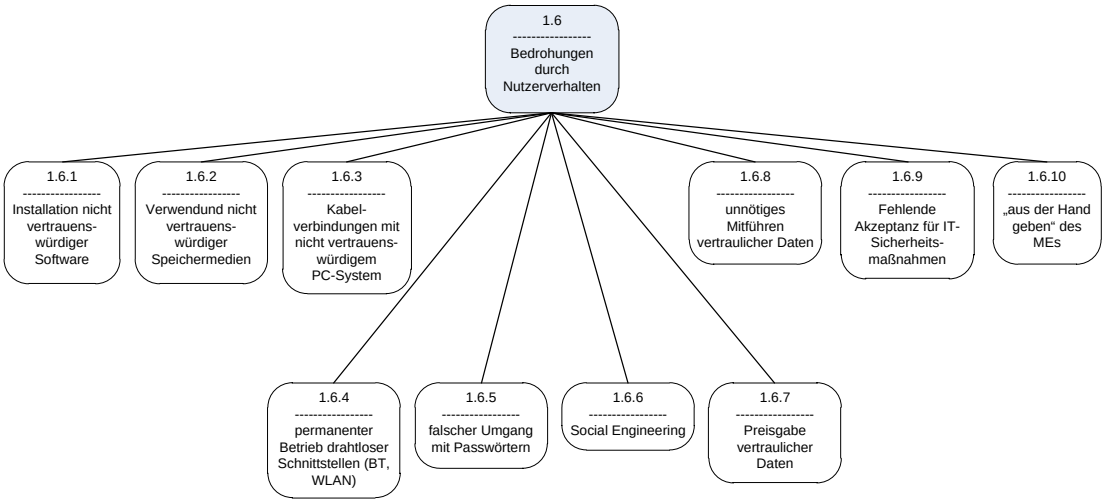

Abb. 5-27: Bedrohungen durch das Nutzerverhalten (grafisch)

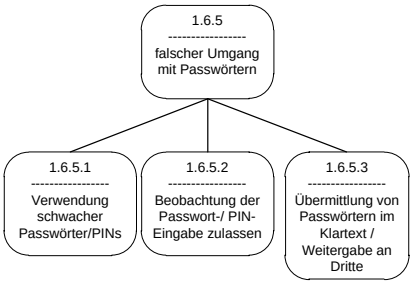

Abb. 5-28: Bedrohungen durch durch den falschen Umgang mit Passwörtern (grafisch)

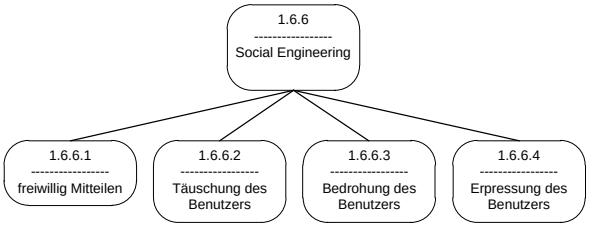

Abb. 5-29: Bedrohungen durch Social Engineering (grafisch)

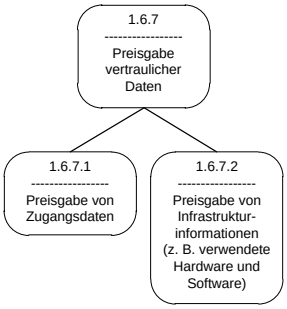

Abb. 5-30: Bedrohungen durch Preisgabe vertraulicher Daten (grafisch)

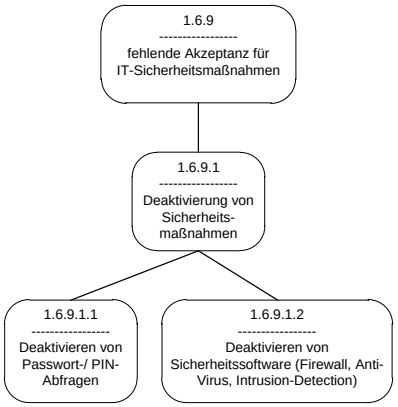

Abb. 5-31: Bedrohungen durch fehlende Akzeptanz für IT-Sicherheitsmaßnahmen (grafisch)

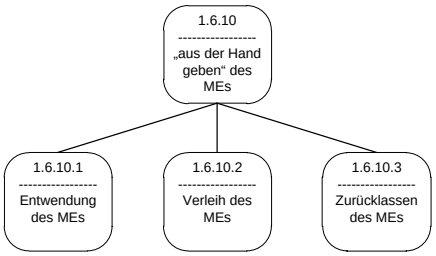

Abb. 5-32: Bedrohungen durch das „aus der Hand geben“ des mobilen Endgerätes (grafisch)

A.2 Bedrohungskatalog

Legende:

VT Vertraulichkeit, IN Integrität, VF Verfügbarkeit, AU Authentizität, VB Verbindlichkeit, AN Anonymität, OM Organisatorische Maßnahme, TM Technische Maßnahme

Nr.	Knoten-Nr.	Bedrohung	Ver-knüp-fung	Bedrohungsbeschreibung	beeintr. Sicherheits-ziel	Maßnahmen-Nr.	Bemerkungen
1	1	Bedrohungen durch die Nutzung mobiler Datenübertragungen	ODER	Durch die Nutzung der mobilen Datenübertragungen treten besondere Bedrohungen zusätzlich zu den bereits vorhandenen Bedrohungen auf. Es kann zu Zerstörung/Verlust, Veränderung, Ausfall, Nutzung oder Kenntnisnahme von Daten außerhalb eines Unternehmens kommen.	VT, IN, VF, AU, VB, AN	OM 1, OM 2	
2	1.1	Bedrohungen durch Angriffe auf GSM	ODER				
3	1.2	Bedrohungen durch Angriffe auf GPRS	ODER				
4	1.3	Bedrohungen durch Angriffe auf UMTS	ODER				
5	1.4	Bedrohungen durch Angriffe auf allgemeine Mobilfunk- u. Datendienste	ODER				
6	1.5	Bedrohungen durch Angriffe auf das ME	ODER				
7	1.6	Bedrohungen durch Nutzerverhalten	ODER				
8	1.1.1	Erkundungsangriffe auf GSM	ODER	Diese Angriffe stellen Bedrohungen dar, die eine Datenübertragung kompromittieren können, wenn für die Übertragung ein GSM-Mobilfunknetz genutzt wird.			
9	1.1.2	Lauschangriffe auf GSM	ODER				
10	1.1.3	Verfügbarkeitsangriffe auf GSM	ODER				
11	1.1.4	Manipulationsangriffe auf GSM	ODER				
12	1.1.1.1	Auslesen der IMSI-Nummer	ODER	Eine Kenntnisnahme vertraulicher Identitätsinformationen ist möglich.	VT, AN	OM 22, OM 23	Punkt ist identisch mit: 1.3.1.1
13	1.1.1.1.1	Vortäuschen einer GSM-Basisstation	UND	Mittels eines IMSI-Catchers ist es möglich, eine GSM-Basisstation vorzutäuschen. Mobile Endgeräte können keinen Unterschied zu einer "echten" GSM-Basisstation erkennen. Sie nutzen daher die vermeintliche GSM-Basisstation, um sich mit dem Mobilfunknetz zu verbinden. Eine solche, falsche GSM-Basisstation kann verschiedene Informationen aus dem mobilen Endgerät auslesen, die Verschlüsselung des mobilen Endgerätes abschalten und den Standort des mobilen Endgerätes näher bestimmen. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN	TM 1	Punkt ist identisch mit: 1.1.1.2.1 , 1.1.1.3.1, 1.3.1.1.1, 1.3.1.2.1, 1.3.1.3.1
14	1.1.1.2	Auslesen der IMEI-Nummer	ODER	Eine Kenntnisnahme vertraulicher Identitätsinformationen ist möglich.	VT, AN	OM 22, OM 23	Punkt ist identisch mit: 1.3.1.2
15	1.1.1.2.1	Vortäuschen einer GSM-Basisstation	UND	Mittels eines IMSI-Catchers ist es möglich, eine GSM-Basisstation vorzutäuschen. Mobile Endgeräte können keinen Unterschied zu einer "echten" GSM-Basisstation erkennen. Sie nutzen daher die vermeintliche GSM-Basisstation, um sich mit dem Mobilfunknetz zu verbinden. Eine solche, falsche GSM-Basisstation kann verschiedene Informationen aus dem mobilen Endgerät auslesen, die Verschlüsselung des mobilen Endgerätes abschalten und den Standort des mobilen Endgerätes näher bestimmen. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN	TM 1	Punkt ist identisch mit: 1.1.1.1.1 , 1.1.1.3.1 , 1.3.1.1.1 , 1.3.1.2.1 , 1.3.1.3.1

16	1.1.1.3	Ermittlung des ME-Standortes (Signalstärke)	ODER	Der Aufenthaltsort eines mobilen Endgerätes kann mittels eines IMSI-Catchers näher bestimmt werden, da die Reichweite des IMSI-Catchers stark begrenzt ist. Dadurch können Angriffe vorbereitet werden.	VT, AN	OM 22, OM 23	Punkt ist identisch mit:1.3.1.3
17	1.1.1.3.1	Vortäuschen einer GSM-Basisstation	UND	Mittels eines IMSI-Catchers ist es möglich, eine GSM-Basisstation vorzutäuschen. Mobile Endgeräte können keinen Unterschied zu einer "echten" GSM-Basisstation erkennen. Sie nutzen daher die vermeintliche GSM-Basisstation, um sich mit dem Mobilfunknetz zu verbinden. Eine solche, falsche GSM-Basisstation kann verschiedene Informationen aus dem mobilen Endgerät auslesen, die Verschlüsselung des mobilen Endgerätes abschalten und den Standort des mobilen Endgerätes näher bestimmen. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN	TM 1	Punkt ist identisch mit: 1.1.1.1.1 , 1.1.1.2.1, 1.3.1.1.1 , 1.3.1.2.1, 1.3.1.3.1
18	1.1.1.4	Ermittlung des ME-Standortes (Zellortung)	UND	Der Aufenthaltsort (Mobilfunkzelle) eines mobilen Endgerätes kann durch den Mobilfunkprovider oder durch so genannte Ortungsdienste im Internet jederzeit ermittelt werden. Dadurch können bestimmte Angriffe vorbereitet werden.	VT, AN	OM 22, OM 23	Punkt ist identisch mit: 1.3.1.4
19	1.1.1.4.1	Interne Mechanismen des Mobilfunknetzes zur Standortermittlung von Mobiltelefonen	ODER		VT, AN	OM 22, OM 23	Punkt ist identisch mit: 1.3.1.4.1
20	1.1.1.4.2	Internetdienste zur Standortermittlung von Mobiltelefonen	ODER		VT, AN	OM 22, OM 23	Punkt ist identisch mit: 1.3.1.4.2
21	1.1.2.1	Aufzeichnung von Daten an der Funkschnittstelle	ODER	Daten, die über eine Funkstrecke gesendet werden, sind grundsätzlich abhörbar. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT	TM 2, TM 3, TM 4, TM 11, TM 26 OM 4, OM 5, OM 6	Punkt ist identisch mit: 1.3.2.1
22	1.1.2.1.1	Entschlüsselung der Daten	ODER	Sind die über eine Funkstrecke gesendeten Daten verschlüsselt, können diese unter Umständen entschlüsselt werden. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN	TM 2, TM 3, TM 4, TM 11, TM 26 OM 4, OM 5, OM 6	Zusätzlich zur Verschlüsselung durch das ME bzw. Durch das Mobilfunknetz sollte daher eine VPN-Lösung verwendet werden, um zusätzliche Sicherheit zu schaffen.
23	1.1.2.1.1.1	Aufzeichnung von verschlüsselten Daten	UND	Wird eine verschlüsselte Datenübertragung aufgezeichnet, besteht die Möglichkeit, dass diese anschließend entschlüsselt wird und auf die unverschlüsselten Daten zurückgerechnet wird bzw. dass der Verschlüsselungsschlüssel aufgedeckt wird. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT	TM 2, TM 3, TM 4, TM 11, TM 26 OM 4, OM 5, OM 6	
24	1.1.2.1.1.2	Errechnung des Verschlüsselungsschlüssels	UND		VT, AN	TM 2, TM 3, TM 4, TM 11, TM 26 OM 4, OM 5, OM 6	
25	1.1.2.1.2	Aufzeichnung von unverschlüsselten Daten	ODER	Ist eine Mobilfunknetz-Verschlüsselung deaktiviert, können die über eine Funkstrecke gesendeten Daten unverschlüsselt aufgezeichnet werden. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN	TM 1, TM 2, TM 3, TM 4, TM 11, M 26 OM 4, OM 5, OM 6	Punkt ist identisch mit: 1.3.2.1.1
26	1.1.2.2	Aufzeichnung von Daten innerhalb der Mobilfunkinfrastruktur	ODER	Innerhalb der Mobilfunkinfrastruktur liegen die gesendeten Daten ab der Basisstation unverschlüsselt vor. Verschafft man sich Zugriff auf diese Infrastruktur, können Daten ausgespäht werden. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN	TM 2, TM 3, TM 4, TM 11, TM 26 OM 4, OM 5, OM 6	Punkt ist identisch mit: 1.3.2.2
27	1.1.2.2.1	Verschaffung des Zugriffs auf interne Gateways und Zwischenspeicher von innen (Innentäter)	ODER		VT, AN		Punkt ist identisch mit: 1.3.2.2.1
28	1.1.2.2.2	Verschaffung des Zugriffs auf interne Gateways und Zwischenspeicher von außen (unbefugte Nutzung der Schnittstellen)	ODER		VT, AN		Punkt ist identisch mit:1.3.2.2.2
29	1.1.3.1	Blockieren mittels IMSI-Catchers	ODER	Durch das Aufstellen eines Störsenders oder anderer Hilfsmittel kann die Funkverbindung eines MEs zu einer Basisstation gestört werden. Es kann zu Verbindungsabbrüchen bzw. der Unmöglichkeit eines Verbindungsaufbaus kommen.	VF		Punkt ist identisch mit: 1.3.3.1
30	1.1.3.2	Blockieren mittels Störsender (GSM-/ UMTS-Jammer)	ODER		VF		Punkt ist identisch mit: 1.3.3.2

31	1.1.3.3	Nutzung interner Mechanismen des Mobilfunknetzes	ODER	Mittels interner Mechanismen zur Sperrung von SIM-Karten (bspw. bei nicht bezahlten Rechnungen) können Nutzer an einem Verbindungsaufbau gehindert werden. Es kann zu Verbindungsabbrüchen bzw. der Unmöglichkeit eines Verbindungsaufbaus kommen.	VF		Punkt ist identisch mit: 1.3.3.3
32	1.1.3.3.1	Ermittlung der Identität des Anzugreifenden	UND		AN	OM 22, OM 23	Punkt ist identisch mit: 1.3.3.3.1
33	1.1.3.3.2	Sperrung der (U)SIM-Karte	UND		VF	OM 22, OM 23	Punkt ist identisch mit: 1.3.3.3.2
34	1.1.4.1	Abschaltung der Verschlüsselung im ME	ODER	Das Mobilfunknetz teilt dem ME die Art der verwendeten Verbindungsverschlüsselung mit. Wird durch einen IMSI-Catcher eine GSM-Basisstation vorgetäuscht, kann das ME mittels eines entsprechenden Kommandos dazu veranlasst werden, die Verbindungsverschlüsselung mittels des Algorithmus A5/0 vorzunehmen, was keiner Verbindungsverschlüsselung entspricht. Alle gesendeten Daten liegen somit unverschlüsselt vor. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN	TM 1 OM 22, OM 23	Punkt ist identisch mit: 13.4.2
35	1.2.1	Manipulationsangriffe auf GPRS	ODER	Diese Angriffe stellen Bedrohungen dar, die eine Datenübertragung kompromittieren können, wenn für die Übertragung der GPRS-Datendienst genutzt wird.			
36	1.2.1.1	Bedrohungen (aus dem PC-System- Bereich) durch Internetnutzung	ODER	Wird mit einem ME das Internet genutzt, so können die gleichen Bedrohungen für das ME entstehen, wie sie für PC-Systeme bei der Nutzung des Internets entstehen. Daher sind beispielhaft einige Angriffe aufgelistet. Diese können dazu führen, dass ein mobiles Endgerät mittels präparierter Webseiten manipuliert wird.	VT, VF, IN, AU, VB, AN	TM 7, TM 17, TM 18, TM 19, TM 20, TM 21, TM 22, TM 23, TM 26, TM 34 OM 3, OM 4, OM 5, OM 6, OM 17, OM 21, OM 23	Punkt ist identisch mit: 1.3.4.1, 1.4.4.2 Ausführlich wird diese Problematik z. B. [Raep01] oder [Jano07] behandelt.
37	1.2.1.1.1	Pharming	ODER				Punkt ist identisch mit: 1.3.4.1.1, 1.4.4.2.1
38	1.2.1.1.2	Browser-Hijacking	ODER				Punkt ist identisch mit: 1.3.4.1.2, 1.4.4.2.2
39	1.2.1.1.3	Link-Manipulation	ODER				Punkt ist identisch mit: 1.3.4.1.3, 1.4.4.2.3
40	1.2.2	sonstige Angriffe auf GPRS	ODER	Diese Angriffe stellen Bedrohungen dar, die eine Datenübertragung kompromittieren können, wenn für die Übertragung der GPRS-Datendienst genutzt wird.			
41	1.2.2.1	IP-basierte Angriffe (z. B. Buffer-Overflow provozieren)	ODER	Unter Ausnutzung von Schwachstellen in den Internetprotokollen können verschiedene Angriffe (vor allem Verfügbarkeitsangriffe) durchgeführt werden.	VT, VF, AU, VB, AN	TM 21, TM 22, TM 23, TM 34 OM 4, OM 5, OM 6	Punkt ist identisch mit: 1.3.3.4, 1.5.3.4
42	1.3.1	Erkundungsangriffe auf UMTS	ODER	Diese Angriffe stellen Bedrohungen dar, die eine Datenübertragung kompromittieren können, wenn für die Übertragung ein UMTS-Mobilfunknetz genutzt wird.			
43	1.3.2	Lauschangriffe auf UMTS	ODER				
44	1.3.3	Verfügbarkeitsangriffe auf UMTS	ODER				
45	1.3.4	Manipulationsangriffe auf UMTS	ODER				
46	1.3.1.1	Auslesen der IMSI-Nummer	UND	Eine Kenntnisnahme vertraulicher Identitätsinformationen ist möglich.	VT, AN	OM 22, OM 23	Punkt ist identisch mit: 1.1.1.1

47	1.3.1.1.1	Vortäuschen einer GSM-Basisstation	UND	Mittels eines IMSI-Catchers ist es möglich, eine GSM-Basisstation vorzutäuschen. Mobile Endgeräte können keinen Unterschied zu einer "echten" GSM-Basisstation erkennen. Sie nutzen daher die vermeintliche GSM-Basisstation, um sich mit dem Mobilfunknetz zu verbinden. Eine solche, falsche GSM-Basisstation kann verschiedene Informationen aus dem mobilen Endgerät auslesen, die Verschlüsselung des mobilen Endgerätes abschalten und den Standort des mobilen Endgerätes näher bestimmen. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN	TM 1, TM 5	Punkt ist identisch mit: 1.1.1.1.1, 1.1.1.2.1, 1.1.1.3.1, 1.3.1.2.1, 1.3.1.3.1
48	1.3.1.1.1.1	Beschaffung von AUTN-Daten für das zu erkundende ME	UND	Als Vorbereitung für das Vortäuschen einer GSM-Basisstation gegenüber einem UMTS-Endgerät müssen Authentisierungsdaten beschafft werden und die IMSI-Nummer des Anzugreifenden erlangt werden. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT	OM 22, OM 23	Punkt ist identisch mit: 1.3.1.2.1.1, 1.3.1.3.1.1
49	1.3.1.1.1.2	Ermittlung der IMSI-Nummer des zu erkundenden MEs	UND		VT, AN	OM 22, OM 23	Punkt ist identisch mit: 1.3.1.2.1.2, 1.3.1.3.1.2
50	1.3.1.2	Auslesen der IMEI-Nummer	UND	Eine Kenntnisnahme vertraulicher Identitätsinformationen ist möglich.	VT, AN	OM 22, OM 23	Punkt ist identisch mit: 1.1.1.2
51	1.3.1.2.1	Vortäuschen einer GSM-Basisstation	UND	Mittels eines IMSI-Catchers ist es möglich, eine GSM-Basisstation vorzutäuschen. Mobile Endgeräte können keinen Unterschied zu einer "echten" GSM-Basisstation erkennen. Sie nutzen daher die vermeintliche GSM-Basisstation, um sich mit dem Mobilfunknetz zu verbinden. Eine solche, falsche GSM-Basisstation kann verschiedene Informationen aus dem mobilen Endgerät auslesen, die Verschlüsselung des mobilen Endgerätes abschalten und den Standort des mobilen Endgerätes näher bestimmen. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN	TM 1, TM 5	Punkt ist identisch mit: 1.1.1.1.1, 1.1.1.2.1, 1.1.1.3.1, 1.3.1.1.1, 1.3.1.3.1
52	1.3.1.2.1.1	Beschaffung von AUTN-Daten für das zu erkundende ME	UND	Als Vorbereitung für das Vortäuschen einer GSM-Basisstation gegenüber einem UMTS-Endgerät müssen Authentisierungsdaten beschafft werden und die IMSI-Nummer des Anzugreifenden erlangt werden. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT	OM 22, OM 23	Punkt ist identisch mit: 1.3.1.1.1.1, 1.3.1.3.1.1
53	1.3.1.2.1.2	Ermittlung der IMSI-Nummer des zu erkundenden MEs	UND		VT, AN	OM 22, OM 23	Punkt ist identisch mit: 1.3.1.1.1.2, 1.3.1.3.1.2
54	1.3.1.3	Ermittlung des ME-Standortes (Signalstärke)	UND	Der Aufenthaltsort eines mobilen Endgerätes kann mittels eines IMSI-Catchers näher bestimmt werden, da die Reichweite des IMSI-Catchers stark begrenzt ist. Dadurch können Angriffe vorbereitet werden.	VT, AN	OM 22, OM 23	Punkt ist identisch mit:1.1.1.3
55	1.3.1.3.1	Vortäuschen einer GSM-Basisstation	UND	Mittels eines IMSI-Catchers ist es möglich, eine GSM-Basisstation vorzutäuschen. Mobile Endgeräte können keinen Unterschied zu einer "echten" GSM-Basisstation erkennen. Sie nutzen daher die vermeintliche GSM-Basisstation, um sich mit dem Mobilfunknetz zu verbinden. Eine solche, falsche GSM-Basisstation kann verschiedene Informationen aus dem mobilen Endgerät auslesen, die Verschlüsselung des mobilen Endgerätes abschalten und den Standort des mobilen Endgerätes näher bestimmen. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN	TM 1, TM 5	Punkt ist identisch mit: 1.1.1.1.1, 1.1.1.2.1, 1.1.1.3.1, 1.3.1.1.1, 1.3.1.2.1
56	1.3.1.3.1.1	Beschaffung von AUTN-Daten für das zu erkundende ME	UND	Als Vorbereitung für das Vortäuschen einer GSM-Basisstation gegenüber einem UMTS-Endgerät müssen Authentisierungsdaten beschafft werden und die IMSI-Nummer des Anzugreifenden erlangt werden. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT	OM 22, OM 23	Punkt ist identisch mit: 1.3.1.1.1.1, 1.3.1.2.1.1
57	1.3.1.3.1.2	Ermittlung der IMSI-Nummer des zu erkundenden MEs	UND		VT, AN	OM 22, OM 23	Punkt ist identisch mit: 1.3.1.1.1.2, 1.3.1.2.1.2
58	1.3.1.4	Ermittlung des ME-Standortes (Zellortung)	UND	Der Aufenthaltsort (Mobilfunkzelle) eines mobilen Endgerätes kann durch den Mobilfunkprovider oder durch so genannte Ortungsdienste im Internet jederzeit ermittelt werden. Dadurch können bestimmte Angriffe vorbereitet werden.	VT, AN	OM 22, OM 23	Punkt ist identisch mit: 1.1.1.4
59	1.3.1.4.1	Interne Mechanismen des Mobilfunknetzes zur Standortermittlung von Mobiltelefonen	ODER		VT, AN	OM 22, OM 23	Punkt ist identisch mit: 1.1.1.4.1

60	1.3.1.4.2	Internetdienste zur Standortermittlung von Mobiltelefonen	ODER		VT, AN	OM 22, OM 23	Punkt ist identisch mit: 1.1.1.4.2
61	1.3.2.1	Aufzeichnung von Daten an der Funkschnittstelle	ODER	Daten, die über eine Funkstrecke gesendet werden, sind grundsätzlich abhörbar. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT	TM 2, TM 3, TM 4, TM 11, TM 26 OM 4, OM 5, OM 6	Punkt ist identisch mit: 1.1.2.1
62	1.3.2.1.1	Aufzeichnung von unverschlüsselten Daten	ODER	Ist eine Mobilfunknetz-Verschlüsselung deaktiviert, können die über eine Funkstrecke gesendeten Daten unverschlüsselt aufgezeichnet werden. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN	TM1, TM 2, TM 3, TM 4, TM 5, TM 11, TM 26 OM 4, OM 5, OM 6	Punkt ist identisch mit: 1.1.2.1.2 Zusätzlich zur Verschlüsselung durch das ME bzw. durch das Mobilfunknetz sollte daher eine VPN-Lösung verwendet werden, um zusätzliche Sicherheit zu schaffen.
63	1.3.2.2	Aufzeichnung von Daten innerhalb der Mobilfunkinfrastruktur	ODER	Innerhalb der Mobilfunkinfrastruktur liegen die gesendeten Daten ab der Basisstation unverschlüsselt vor. Verschafft man sich Zugriff auf diese Infrastruktur, können Daten ausgespäht werden. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN	TM 2, TM 3, TM 4, TM 11, TM 26 OM 4, OM 5, OM 6	Punkt ist identisch mit: 1.1.2.2
64	1.3.2.2.1	Verschaffung des Zugriffs auf interne Gateways und Zwischenspeicher von innen (Innentäter)	ODER		VT, AN		Punkt ist identisch mit:1.1.2.2.1
65	1.3.2.2.2	Verschaffung des Zugriffs auf interne Gateways und Zwischenspeicher von außen (unbefugte Nutzung von Schnittstellen)	ODER		VT, AN		Punkt ist identisch mit: 1.1.2.2.2
66	1.3.3.1	Blockierung mittels IMSI-Catchers	ODER	Durch das Aufstellen eines Störsenders oder anderer Hilfsmittel kann die Funkverbindung eines MEs zu einer Basisstation gestört werden. Es kann zu Verbindungsabbrüchen bzw. der Unmöglichkeit eines Verbindungsaufbaus kommen.	VF		Punkt ist identisch mit: 1.1.3.1
67	1.3.3.2	Blockierung mittels Störsender (GSM-/ UMTS-Jammer)	ODER		VF		Punkt ist identisch mit: 1.1.3.2
68	1.3.3.3	Nutzung interner Mechanismen des Mobilfunknetzes	ODER	Mittels interner Mechanismen zur Sperrung von (U)SIM-Karten (bspw. bei nicht bezahlten Rechnungen) können Nutzer an einem Verbindungsaufbau gehindert werden. Es kann zu Verbindungsabbrüchen bzw. der Unmöglichkeit eines Verbindungsaufbaus kommen.	VF		Punkt ist identisch mit: 1.1.3.3
69	1.3..3.3.1	Ermittlung der Identität des Anzugreifenden	UND		AN	OM 22, OM 23	Punkt ist identisch mit: 1.1.3.3.1
70	1.3.3.3.2	Sperrung der (U)SIM-Karte	UND		VF		Punkt ist identisch mit: 1.1.3.3.2
71	1.3.3.4	IP-basierte Angriffe (z. B. Buffer-Overflow provozieren)	ODER	Unter Ausnutzung der Schwachstellen in den Internetprotokollen können verschiedene Angriffe (vor allem Verfügbarkeitsangriffe) durchgeführt werden.	VF	TM 21, TM 22, TM 23, TM 34 OM 4, OM 5, OM 6	Punkt ist identisch mit: 1.2.2.1, 1.5.3.4
72	1.3.4.1	Bedrohungen (aus dem PC-System-Bereich) durch Internetnutzung	ODER	Wird mit einem ME das Internet genutzt, so können die gleichen Bedrohungen für das ME entstehen, wie sie für PC-Systeme bei der Nutzung des Internets entstehen. Daher sind beispielhaft einige dieser Bedrohungen aufgelistet.	VT, VF, IN, AU, VB, AN	TM 7, TM 17, TM 18, TM 19, TM 20, TM 21, TM 22, TM 23, TM 26, TM 34 OM 3, OM 4, OM 5, OM 6, OM 17, OM 21, OM 23	Punkt ist identisch mit: 1.2.1.1, 1.4.4.2
73	1.3.4.1.1	Pharming	ODER				Punkt ist identisch mit: 1.2.1.1.1, 1.4.4.2.1
74	1.3.4.1.2	Browser-Hijacking	ODER				Punkt ist identisch mit: 1.2.1.1.2, 1.4.4.2.2
75	1.3.4.1.3	Link-Manipulation	ODER				Punkt ist identisch mit: 1.2.1.1.3, 1.4.4.2.3

76	1.3.4.2	Abschaltung der Verschlüsselung im ME	ODER	Das Mobilfunknetz teilt dem ME die Art der verwendeten Verbindungsverschlüsselung mit. Wird durch einen IMSI-Catcher eine GSM-Basisstation vorgetäuscht, kann das ME mittels eines entsprechenden Kommandos dazu veranlasst werden, die Verbindungsverschlüsselung mittels des Algorithmus A5/0 vorzunehmen, was keiner Verbindungsverschlüsselung entspricht. Alle gesendeten Daten liegen somit unverschlüsselt vor. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN	TM 1, TM 5 OM 22, OM 23	Punkt ist identisch mit: 1.1.4.1
77	1.4.1	Kurzmitteilungen (SMS)	ODER	Diese Angriffe stellen Bedrohungen dar, die durch Kurzmitteilungen entstehen bzw. Bedrohungen, die eine Datenübertragung kompromittieren können, wenn für die Übertragung der Kurzmitteilungsdienst genutzt wird.			
78	1.4.2	Multimedia-Mitteilungen (MMS)	ODER	Diese Angriffe stellen Bedrohungen dar, die durch Multimediamitteilungen entstehen bzw. Bedrohungen, die eine Datenübertragung kompromittieren können, wenn für die Übertragung der Multimediamitteilungsdienst genutzt wird.			
79	1.4.3	Wireless Application Protocol (WAP)	ODER	Diese Angriffe stellen Bedrohungen dar, die durch WAP entstehen bzw. Bedrohungen, die eine Datenübertragung kompromittieren können, wenn für die Übertragung WAP genutzt wird.			
80	1.4.4	Internetnutzung	ODER	Diese Angriffe stellen Bedrohungen dar, die durch das Internet entstehen bzw. Bedrohungen, die eine Datenübertragung kompromittieren können, wenn für die Übertragung das Internet genutzt wird.			
81	1.4.5	mobile Datensynchronisation	ODER	Diese Angriffe stellen Bedrohungen dar, die durch mobile Datensynchronisation entstehen bzw. Bedrohungen, die eine Datenübertragung kompromittieren können, wenn die mobile Datensynchronisation genutzt wird.			[BSI08b] befasst sich umfassend mit dem Schutz von Synchronisationslösungen
82	1.4.1.1	Mitlesen von SMS-Inhalten	ODER	Kurzmitteilungsnachrichten liegen innerhalb des Mobilfunknetzes (Funkstrecke ausgenommen) unverschlüsselt vor. Verschafft sich ein Angreifer Zugriff auf die mobilfunknetzinternen Gateways und Zwischenspeicher, ist eine Kenntnisnahme vertraulicher Informationen möglich.	VT, AN	TM 3 OM 4, OM 5, OM 6	
83	1.4.1.1.1	Verschaffung des Zugriffs auf SMS-Gateways und Zwischenspeicher von innen (Innentäter)	ODER		VT, AN		
84	1.4.1.1.2	Verschaffung des Zugriffs auf SMS-Gateways und Zwischenspeicher von außen (unbefugte Nutzung von Schnittstellen)	ODER		VT, AN		
85	1.4.1.2	Versendung vertraulicher Daten per SMS	ODER	Kurzmitteilungsnachrichten können dazu genutzt werden, vertrauliche Informationen von einem mobilen Endgerät an einen Angreifer zu versenden. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN	TM 3 OM 4, OM 5, OM 6	
86	1.4.1.2.1	manipulierte Anwendungssoftware mit SMS-Funktion (z. B. dokumentiert bei BlackBerry)	ODER		VT, AN	TM 6, TM 15 OM 19, OM 29	Vgl. [Diet04, 7].
87	1.4.1.3	Manipulationen durch SMS	ODER	Kurzmitteilungsnachrichten können dazu genutzt werden, Manipulationen an mobilen Endgeräten vorzunehmen. Die Integrität und Verfügbarkeit von bestimmten Diensten und Funktionen kann somit beeinträchtigt werden.	IN, VF		
88	1.4.1.3.1	Manipulationen von Konfigurationsdaten (z. B. Internetzugangseinstellungen)	ODER		IN, VF	TM 6, TM 9, TM 31 OM 3, OM 19	
89	1.4.1.3.2	Manipulationen von WLAN-Einstellungen (z. B. Deaktivierung der SSL-Verschlüsselung)	ODER		IN, VF	TM 6, TM 9, TM 31 OM 3, OM 19	
90	1.4.2.1	Übermittlung von Schadsoftware per MMS	ODER	Multimediamitteilungen können dazu genutzt werden, Schadsoftware auf ein mobiles Endgerät zu übertragen. Dabei kann die MMS auf eine Webseite verweisen, welche mittels aktiver Inhalte Schadsoftware auf das mobile Endgerät überträgt. Die Integrität und Verfügbarkeit von bestimmten Diensten und Funktionen kann somit beeinträchtigt werden. Es kann zur Zerstörung oder Veränderung von Daten kommen. Außerdem ist eine Kenntnisnahme vertraulicher Informationen möglich.	VT, IN, VF, AU, VB, AN	TM 6, TM 7, TM 15, TM 17, TM 18, TM 19, TM 20, TM 22, TM 23, TM 34 OM 3, OM 4, OM 5, OM 6, OM 18, OM 29	

91	1.4.2.1.1	MMS lädt Schadsoftware aus dem Internet nach	ODER		VT, IN, VF,AU, VB, AN	TM 6, TM 7, TM 15,TM 17, TM 18, TM 19, TM 20, TM 22, TM 23, TM 34 OM 3, OM 4, OM 5,OM 6, OM 18, OM 29	
92	1.4.2.1.1.1	Manipulation der MMS-Konfiguration mittels OTA	UND		IN, VF	TM 6, TM 9, TM 31 OM 3, OM 19	
93	1.4.2.1.1.2	Betreiben eines eigenen MMS-Proxy-Servers	UND		VT, IN, AN		
94	1.4.2.1.1.3	MMS verweist auf eigenen MMS-Proxy-Server	UND		VT, AN		
95	1.4.2.1.2	MMS beinhaltet Schadsoftware	ODER	Multimediamitteilungen können dazu genutzt werden, Schadsoftware auf ein mobiles Endgerät zu übertragen. Dabei kann die MMS die Schadsoftware als versteckten aktiven Inhalt enthalten. Die Integrität und Verfügbarkeit von bestimmten Diensten und Funktionen kann somit beeinträchtigt werden. Es kann zur Zerstörung oder Veränderung der Daten kommen, außerdem ist eine Kenntnisnahme vertraulicher Informationen möglich.	VT, IN, VF, AU, VB, AN	TM 6, TM 7, TM 15, TM 17, TM 18, TM 19, TM 20, TM 22, TM 23, TM 34 OM 3, OM 4, OM 5, OM 6, OM 18, OM 29	
96	1.4.3.1	Ausspähen von gesendeten Daten	ODER	Wird WAP 1.x für die Datenübertragung genutzt, so stellt das WAP-Gateway sowohl für das mobile Endgerät als auch für die Gegenseite das Ende der Verbindungsverschlüsselung dar. Verschafft sich ein Angreifer Zugriff auf dieses Gateway, so kann es zur Kenntnisnahme vertraulicher Informationen kommen.	VT, AN	TM 2, TM 11, TM 26 OM 4, OM 5, OM 6	
97	1.4.3.1.1	Verschaffung des Zugriffs auf WAP-Gateways und Zwischenspeicher von innen (Innentäter)	ODER		VT, AN		
98	1.4.3.1.2	Verschaffung des Zugriffs auf WAP-Gateways und Zwischenspeicher von außen (unbefugte Nutzung von Schnittstellen)	ODER		VT, AN		
99	1.4.3.2	Umleitung auf manipulierte Webseiten	ODER	WAP-Push Nachrichten können Links enthalten, die den Nutzer auf eine manipulierte Webseite leiten. Diese Webseite lädt automatisch Schadsoftware auf das mobile Endgerät. Eine Kompromittierung des mobilen Endgerätes und die Kenntnisnahme vertraulicher Informationen sind möglich.	VT, AN	TM 26	
100	1.4.3.2.1	Versendung manipulierter WAP-Push-Nachrichten	ODER		VT, AN	TM 7, TM 8, TM 15, TM 17, TM 18, TM 19, TM 20, TM 21, TM 22, TM 23, TM 34 OM 3, OM 4, OM 5, OM 6, OM 17, OM 18, OM 21, OM 29	
101	1.4.4.1	Bedrohungen durch Verwendung von Proxy-Server-Verbindungen	ODER	Bei der Verwendung von Proxy-Servern kann es zur Kompromittierung der Datenübertragung kommen, da nicht ausgeschlossen werden kann, dass der verwendete Proxy-Server kompromittiert ist. Ist ein solcher Server kompromittiert, können die über ihn übertragenen Daten an Dritte weitergeleitet bzw. von Dritten aufgezeichnet werden. Eine Blockierung, Manipulation oder Verzögerung der gesendeten Daten ist ebenfalls möglich. Es kann außerdem zu einer Kenntnisnahme vertraulicher Informationen kommen.	VT, IN, VF,VB, AN, AU	TM 7, OM 32	

102	1.4.4.1.1	Angriff auf Proxy-Server	ODER	Verschafft sich ein Angreifer Zugriff auf einen Proxy-Server, ist eine Blockierung, Manipulation oder Verzögerung der gesendeten Daten möglich. Es kann außerdem zu einer Kenntnisnahme vertraulicher Informationen kommen.	VT, IN, VF, VB, AN	TM 35, TM 36	
103	1.4.4.1.1.1	Erkundung von Proxy-Servern	UND				
104	1.4.4.1.1.2	Manipulation von Proxy-Servern	UND				
105	1.4.4.1.1.3	Belauschen von Proxy-Servern	UND				
106	1.4.4.1.2	Umleitung auf „feindliche“ Proxy-Server	ODER	Wurde ein mobiles Endgerät so manipuliert, dass das mobile Endgerät eine Verbindung über einen "feindlichen" Proxy-Server aufbaut, ist eine Blockierung, Manipulation oder Verzögerung der gesendeten Daten möglich. Es kann außerdem zu einer Kenntnisnahme vertraulicher Informationen kommen.	VT, IN, VF, VB, AN, AU	TM 7, TM 9, TM 26, TM 31 OM 18, OM 32	
107	1.4.4.1.3	keine Gewährleistung einer Ende-zu-Ende-Verschlüsselung	ODER	Bei der Verwendung eines Proxy-Servers kann keine Ende-zu-Ende-Verschlüsselung gewährleistet werden, da der Proxy-Server aus jeder Verbindungsrichtung den Endpunkt der Verschlüsselung bedeutet. Es kann also nicht ausgeschlossen werden, dass auf dem Übertragungsweg zwischen Proxy-Server und Endstelle der Übertragung eine Kompromittierung der Datenübertragung eintritt.	VT, IN, VF, VB, AN, AU	TM 7	
108	1.4.4.2	Bedrohungen (aus dem PC-System- Bereich) durch Internetnutzung	ODER	Wird mit einem ME das Internet genutzt, so können die gleichen Bedrohungen für das ME entstehen, wie sie für PC-Systeme bei der Nutzung des Internets entstehen. Daher sind beispielhaft einige Angriffe aufgelistet. Diese können z. B. dazu führen, das ein mobiles Endgerät mittels präparierter Webseiten manipuliert wird.	VT, IN, VF, VB, AN, AU	TM 7, TM 17, TM 18, TM 19, TM 20, TM 21, TM 22, TM 23, TM, 26, TM 34 OM 3, OM 4, OM 5, OM 6, OM 17 OM 21, OM 23	Punkt ist identisch mit: 1.2.1.1, 1.3.4.1
109	1.4.4.2.1	Pharming	ODER				Punkt ist identisch mit: 1.2.1.1.1, 1.3.4.1.1
110	1.4.4.2.2	Browser-Hijacking	ODER				Punkt ist identisch mit: 1.2.1.1.2, 1.3.4.1.2
111	1.4.4.2.3	Link-Manipulation	ODER				Punkt ist identisch mit: 1.2.1.1.3, 1.3.4.1.3
112	1.4.5.1	Lauschangriffe auf Synchronisationsserver	ODER	Besteht eine Verbindung zwischen einem mobilen Endgerät und einem Synchronisationsserver, so kann es während dieser Verbindung zur Kompromittierung des mobilen Endgerätes kommen, wenn der Synchronisationsserver vorher manipuliert wurde. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN		
113	1.4.5.1.1	Ausspähen des MEs während der Synchronisation	ODER			TM 2, TM 11	
114	1.4.5.1.1.1	Erkundung der Synchronisationsserver	UND		VT	TM 35, TM 36	Punkt ist identisch mit: 1.4.5.2.1, 1.4.5.3.1.1
115	1.4.5.1.1.2	Manipulation der Synchronisationsserver	UND		VT, AN	TM 35, TM 36	
116	1.4.5.2	Verfügbarkeitsangriffe auf Synchronisationsserver	ODER	Um eine Kommunikation zwischen Synchronisationsserver und mobilem Endgerät zu verhindern, ist es denkbar, dass diese Server angegriffen werden bis sie ihre Dienste nicht mehr zur Verfügung stellen können. Dies kann geschehen, um einen maskierten Server statt des "echten" Servers mit dem mobilen Endgerät zu verbinden oder um den wiederholten Verbindungsaufbau durch das mobile Endgerät zu analysieren.	VF		
117	1.4.5.2.1	Erkundung der Synchronisationsserver	UND		VT	TM 35, TM 36	Punkt ist identisch mit: 1.4.5.1.1.1, 1.4.5.3.1.1
118	1.4.5.2.2	Manipulation der Synchronisationsserver	UND		VF	TM 35, TM 36	
119	1.4.5.3	Manipulationsangriffe auf Synchronisationsserver	ODER	Besteht eine Verbindung zwischen einem mobilen Endgerät und einem Synchronisationsserver, so kann es während dieser Verbindung zur Kompromittierung des mobilen Endgerätes kommen, wenn der Synchronisationsserver vorher manipuliert wurde. Eine Kenntnisnahme vertraulicher Informationen ist möglich. Des Weiteren kann das mobile Endgerät manipuliert werden, um fortlaufend Daten aus diesem mobilen Endgerät auszulesen bzw. um die von diesem mobilen Endgerät übertragenen Daten auszuspähen.	VT, IN, VF, AU, VB, AN		
120	1.4.5.3.1	Manipulation des MEs während der Synchronisation (z. B. Schadsoftware aufspielen)	ODER		VT, IN, VF, AU, VB, AN	TM 20, TM 21, TM 22 OM 4, OM 5, OM 6	
121	1.4.5.3.1.1	Erkundung der Synchronisationsserver	UND		VT	TM 35, TM 36	Punkt ist identisch mit: 1.4.5.1.1.1, 1.4.5.2.1
122	1.4.5.3.1.2	Manipulation der Synchronisationsserver	UND		VT, IN, VF, AU, VB, AN	TM 35, TM 36	

123	1.5.1	Erkundungsangriffe auf das ME	ODER	Diese Angriffe stellen Bedrohungen dar, die durch die Nutzung von mobilen Endgeräten für eine Datenübertragung entstehen.			
124	1.5.2	Lauschangriffe auf das ME	ODER				
125	1.5.3	Verfügbarkeitsangriffe auf das ME	ODER				
126	1.5.4	Manipulationsangriffe auf das ME	ODER				
127	1.5.1.1	Präsenz des MEs feststellen	ODER	Das Aufspüren eines mobilen Endgerätes bietet einen Einstiegspunkt für Angriffe auf das mobile Endgerät. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN		
128	1.5.1.1.1	GSM-/ UMTS-Ortung	ODER		VT, AN	OM 22, OM 23	
129	1.5.1.1.2	WLAN Scan	UND		VT, AN	TM 10, TM 30 OM 4, OM 6	
130	1.5.1.1.3	Finden aktiver WLAN-Verbindungen/ WLAN-Modulen	UND				
131	1.5.1.1.4	Bluetooth Scan	UND		VT, AN	TM 12, TM 30 OM 4, OM 6	
132	1.5.1.1.5	Finden aktiver Bluetooth- Verbindungen/ Bluetooth -Module	UND				
133	1.5.1.1.6	Scannen aktiver Hosts (IP) und Ports	ODER		VT, AN	TM 21 OM 4, OM 6	
134	2.5.1.1.7	Finden aktiver IP-Verbindungen / offener Ports					
135	1.5.1.2	Einholen zusätzlicher Informationen	ODER	Zusätzliche Informationen über ein mobiles Endgerät bzw. über die von einem Unternehmen generell eingesetzten mobilen Endgeräte (Social Engineering) einzuholen, dient der weiteren Vorbereitung von Angriffen. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN		
136	1.5.1.2.1	Entwendung des MEs	ODER		VT, AN	TM, 25, TM 26 OM 9, OM 10, OM 11, OM 12, OM 13, OM 31	Punkt ist identisch mit: 1.5.3.5, 1.6.10.1
137	1.5.1.2.2	Erstellung von Bewegungsprofilen	ODER		VT, AN	TM 10, TM 12, TM 30 OM 22, OM 23	
138	1.5.1.2.3	Einschleusen von Schadsoftware	ODER		VT, AN	TM 15, TM 17, TM 18, TM 19, TM 20, TM 21, TM 22, TM 23, TM 25, TM 26, TM 29, TM 34 OM 3, OM 4, OM 5,OM 6, OM 9, OM 10, OM 11, OM 12, OM 14, OM 20	
139	1.5.1.2.4	Social Engineering	ODER		VT, AN	OM 7, OM 8	Punkt ist identisch mit: 1.5.1.2.5.2, 1.6.6
140	1.5.1.2.5	Ermittlung von Zugangsdaten	ODER		VT, AN	TM 13, TM 23, TM 26, TM 34 OM 7, OM 8, OM 14, OM 15, OM 16, OM 17, OM 18, OM 19, OM 20	Punkt ist identisch mit: 1.5.4.1.1.7

141	1.5.1.2.5.1	Erraten von Zugangsdaten (manuell)	ODER	Die Zugangsdaten können erraten werden (kein computergestützter Wörterbuchangriff, sondern Eingabe häufig verwendeter Passwörter). Es kann eine unberechtigte Nutzung, sowie eine Manipulation des mobilen Endgerätes erfolgen. Daten, die auf dem mobilen Endgerät gespeichert sind, können verändert oder ausgelesen werden.	VT, AU	OM 14, OM 15, OM 16	
142	1.5.1.2.5.2	Social Engineering	ODER	Die Zugangsdaten können mittels Social Engineering (Preisgabe durch den Nutzer) erlangt werden. Es kann eine unberechtigte Nutzung, sowie eine Manipulation des mobilen Endgerätes erfolgen. Daten, die auf dem mobilen Endgerät gespeichert sind, können verändert oder ausgelesen werden.	VT, AU, AN	OM 7, OM 8	Punkt ist identisch mit: 1.5.1.2.4, 1.6.6
143	1.5.1.2.5.3	Beobachtung der Eingabe der Zugangsdaten	ODER	Die Zugangsdaten können durch Beobachtung der Zugangsdateneingabe erlangt werden. Es kann eine unberechtigte Nutzung, sowie eine Manipulation des mobilen Endgerätes erfolgen. Daten, die auf dem mobilen Endgerät gespeichert sind, können verändert oder ausgelesen werden.	VT, AU, AN	OM 8, OM 14	
144	1.5.1.2.5.4	Errechnung/ Brechung der Zugangsdaten	ODER	Die Zugangsdaten können erraten werden (computergestütztes Erraten durch Probieren). Es kann eine unberechtigte Nutzung, sowie eine Manipulation des mobilen Endgerätes erfolgen. Daten, die auf dem mobilen Endgerät gespeichert sind, können verändert oder ausgelesen werden.	VT, AU	OM 14, OM 15, OM 16	
145	1.5.1.2.5.4.1	Wörterbuch-Angriffe	ODER				
146	1.5.1.2.5.4.2	Brute-Force-Angriffe	ODER				
147	1.5.1.2.5.5	Ausnutzung von Softwareschwachstellen (Betriebssystem, Anwendungssoftware)	ODER	Weisen Anwendungssoftware oder Betriebssysteme Schwachstellen auf, so können diese dazu genutzt werden, Daten auszulesen, unberechtigten Zugang zu erhalten oder Schadsoftware einzuschleusen. Daten, die auf dem mobilen Endgerät gespeichert sind, können verändert oder ausgelesen werden.	VT, AU	TM 13, TM 21, TM 22, TM 23, TM 34 OM 4, OM 5, OM 6, OM 20, OM 21, OM 22, OM 23, OM 29	
148	1.5.1.2.5.6	Zurückrechnen von Hashwerten (Passworthashwerte zurückrechnen auf Klartextpasswort)	ODER	Ist ein Zugriff auf das mobile Endgerät möglich, kann aus dem Hashwert eines Passwortes mittels Wörterbuchtabellen auf das Klartextpasswort geschlossen werden. Daten, die auf dem mobilen Endgerät gespeichert sind, können verändert oder ausgelesen werden.	VT, AU		
149	1.5.1.2.5.7	Analyse von Abnutzungsspuren (z. B. Touchscreenkratzer)	ODER	Berührungsempfindliche Bildschirme erhalten Abnutzungsspuren bei häufiger Eingabe von Passwörtern. Diese können analysiert werden und erleichtern das Ermitteln dieser Passwörter. Daten, die auf dem mobilen Endgerät gespeichert sind, können verändert oder ausgelesen werden.	VT, AU	OM 20	
150	1.5.1.2.5.8	Known-Plaintext, Known-Ciphertext-Angriffe	ODER	Über verschiedene kryptographische Angriffe ist es möglich, verschlüsselte Daten zu entschlüsseln, bzw. den verwendeten Schlüssel zu errechnen. Sind Zugangsdaten in verschlüsselten Dateien abgelegt (Passwortmanager), können diese unter Umständen entschlüsselt werden und der Angreifer kann sich die benötigten Zugangsdaten verschaffen. Daten, die auf dem mobilen Endgerät gespeichert sind, können verändert oder ausgelesen werden.	VT, AU		
151	1.5.2.1	Angreifer ist nicht im Besitz des MEs	ODER	Diese Angriffe stellen Bedrohungen dar, die auf ein mobiles Endgerät einwirken können, wenn der Angreifer nicht im Besitz des mobilen Endgerätes ist.			
152	1.5.2.1.1	Ausnutzung von WLAN-Schwachstellen (Treiber, Protokolle)	ODER	Weisen Treiber oder Protokolle, die für WLAN-Verbindungen genutzt werden, Schwachstellen auf, können diese von einem Angreifer dazu genutzt werden, Daten auszulesen, Daten zu verändern, sich unberechtigt Zugang zu verschaffen oder Schadsoftware einzuschleusen.	VT, AN	TM 2, TM 10, TM 11, TM 21, TM 22, TM 23, TM 30, TM 34 OM 4, OM 5, OM 6	Punkt ist identisch mit: 1.5.3.1, 1.5.4.2.3

153	1.5.2.1.2	Ausnutzung von Bluetooth-Schwachstellen (Treiber, Protokolle)	ODER	Weisen Treiber oder Protokolle, die für Bluetooth-Verbindungen genutzt werden, Schwachstellen auf, können diese von einem Angreifer dazu genutzt werden, Daten auszulesen, Daten zu verändern, sich unberechtigt Zugang zu verschaffen oder Schadsoftware einzuschleusen.	VT, AN	TM 12, TM 21, TM 22, TM 23, TM 30, TM 34 OM 4, OM 5, OM 6, OM 19	Punkt ist identisch mit: 1.5.3.2, 1.5.4.2.4
154	1.5.2.1.3	Ausnutzung von Softwareschwachstellen (Betriebssystem, Anwendungssoftware)	ODER	Weisen Anwendungssoftware oder Betriebssysteme Schwachstellen auf, so können diese von einem Angreifer dazu genutzt werden, Daten auszulesen, Daten zu verändern, sich unberechtigt Zugang zu verschaffen oder Schadsoftware einzuschleusen.	VT, AN	TM 13, TM 21, TM 22, TM 23, TM 34 OM 4, OM 5, OM 6, OM 29	Punkt ist identisch mit: 1.5.3.3
155	1.5.2.1.4	Maskierung (z. B. öffentl. Hot Spot vortäuschen)	ODER	Maskierung von Infrastrukturkomponenten (z. B. Hot Spots) hat zur Folge, dass mobile Endgeräte bzw. deren Nutzer nicht zwischen einer "echten" Infrastrukturkomponente und einer "gefälschten" Infrastrukturkomponente unterscheiden können. Das mobile Endgerät wird mit der vermeintlich "echten" Infrastrukturkomponente verbunden. Diese kann dann die Verbindung kontrollieren, den Verschlüsselungsschlüssel in Erfahrung bringen, oder die Verschlüsselung abschalten. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN	TM 2, TM 4, TM 11, TM 21 OM 4, OM 5, OM 6	
156	1.5.2.1.5	Abhörmechanismen im ME für Behörden	ODER	Es besteht die Möglichkeit, dass Mechanismen in mobile Endgeräte integriert sind, die es Strafverfolgungsbehörden erlauben, sich Zugriff auf das mobile Endgerät zu verschaffen oder deren Kommunikation zu überwachen. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN	TM 2, TM 3, TM 4,TM 11, TM 13 OM 4, OM 5, OM 6	
157	1.5.2.1.6	Aufzeichnen unverschlüsselter Datenverbindungen (BT, WLAN)	ODER	Werden Übertragungen über drahtlose Kommunikationsschnittstellen nicht verschlüsselt, so kann jeder, der sich in Empfangsreichweite befindet, die unverschlüsselten Daten empfangen und aufzeichnen. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN	TM 2 OM 4, OM 5, OM 6, OM 19	
158	1.5.2.2	Angreifer ist im Besitz des MEs	ODER	Diese Angriffe stellen Bedrohungen dar, die auf ein mobiles Endgerät einwirken können, wenn der Angreifer im Besitz des mobilen Endgerätes ist.			Punkt ist identisch mit: 1.5.4.1
159	1.5.2.2.1	Auslesen unverschlüsselter Daten	ODER	Ist ein Angreifer im Besitz des mobilen Endgerätes, kann er sich Zugang zum Speicher des mobilen Endgerätes verschaffen. Dabei können Daten ausgelesen, entschlüsselt und wiederhergestellt werden. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN	TM 24, TM 25, TM 26, TM 29, TM 33 OM 4, OM 5, OM 6, OM 7, OM 14, OM 16, OM 20, OM 31	
160	1.5.2.2.2	Wiederherstellen gelöschter Daten	ODER		VT, AN	TM 24, TM 25, TM 26, TM 29, TM 33 OM 4, OM 5, OM 6, OM 7, OM 14, OM 16, OM 20, OM 31	
161	1.5.2.2.3	Entschlüsseln (schwach) verschlüsselter Daten	ODER		VT, AN	TM 24, TM 25, TM 26, TM 29, TM 33 OM 4, OM 5, OM 6, OM 7, OM 14, OM 16, OM 20, OM 31	

162	1.5.3.1	Ausnutzung von WLAN-Schwachstellen (Treiber, Protokolle)	ODER	Weisen Treiber oder Protokolle, die für WLAN-Verbindungen genutzt werden, Schwachstellen auf, können diese von einem Angreifer dazu genutzt werden, Daten auszulesen, Daten zu verändern, sich unberechtigt Zugang zu verschaffen oder Schadsoftware einzuschleusen.	VF	TM 10, TM 21, TM 23,TM 30, TM 34 OM 4, OM 5, OM 6	Punkt ist identisch mit: 1.5.2.1.1, 1.5.4.2.3
163	1.5.3.2	Ausnutzung von Bluetooth-Schwach-stellen (Treiber, Protokolle)	ODER	Weisen Treiber oder Protokolle, die für Bluetooth-Verbindungen genutzt werden, Schwachstellen auf, können diese von einem Angreifer dazu genutzt werden, Daten auszulesen, Daten zu verändern, sich unberechtigt Zugang zu verschaffen oder Schadsoftware einzuschleusen.	VF	TM 12, TM 21, TM 22, TM 23, TM 30, TM 34 OM 4, OM 5, OM 6, OM 19	Punkt ist identisch mit: 1.5.2.1.2, 1.5.4.2.4
164	1.5.3.3	Ausnutzung von Softwareschwachstellen (Betriebssystem, Anwendungssoftware)	ODER	Weisen Anwendungssoftware oder Betriebssysteme Schwachstellen auf, so können diese von einem Angreifer dazu genutzt werden, Daten auszulesen, Daten zu verändern, sich unberechtigt Zugang zu verschaffen oder Schadsoftware einzuschleusen.	VF	TM 13, TM 21, TM 22, TM 23, TM 34 OM 4, OM 5, OM 6,OM 29	Punkt ist identisch mit:1.5.2.1.3
165	1.5.3.3.1	Ausnutzung von Systemanwendungs-schwachstellen (z. B. SMS-Verarbeitung)	ODER		VF	TM 21, TM 22, TM 23, TM 34 OM 4, OM 5, OM 6	
166	1.5.3.3.2	Ausnutzung von Anwendungs-softwareschwachstellen (z. B. Bild-betrachter)	ODER		VF	TM 13, TM 21, TM 22, TM 23, TM 34 OM 4, OM 5, OM 6, OM 20, OM 22, OM 23, OM 29	
167	1.5.3.4	IP-basierte Angriffe (z. B. Buffer-Overflow provozieren)	ODER	Unter Ausnutzung von Schwachstellen in den Internetprotokollen können verschiedene Angriffe (vor allem Verfügbarkeitsangriffe) durchgeführt werden.	VF	TM 21, TM 22, TM 23, TM 34 OM 4, OM 5, OM 6	Punkt ist identisch mit: 1.2.2.1, 1.3.3.4
168	1.5.3.5	Entwendung des MEs	ODER	Um bestimmte Angriffe ausführen zu können, muss ein Angreifer das mobile Endgerät in seinen Besitz bringen.	VF	TM, 25, TM 26 OM 9, OM 10, OM 11, OM 12, OM 13, OM 31	Punkt ist identisch mit: 1.5.1.2.1, 1.6.10.1
169	1.5.4.1	Angreifer ist im Besitz des MEs	ODER	Diese Angriffe stellen Bedrohungen dar, die auf ein mobiles Endgerät einwirken können, wenn der Angreifer im Besitz des mobilen Endgerätes ist.			Punkt ist identisch mit: 1.5.2.2
170	1.5.4.1.1	Nutzer verwendet manipuliertes ME	ODER	Wurde ein mobiles Endgerät entwendet, um es zu manipulieren, oder wurde ein Endgerät geklont, so ist es notwendig, es dem rechtmäßigen Besitzer wiederzugeben. Dies kann ohne sein Wissen geschehen oder aber indem der Angreifer einen "ehrlichen" Finder vortäuscht. Verwendet ein Nutzer ein zuvor verloren gegangenes mobiles Endgerät ohne vorherige Prüfung durch einen Techniker, kann es zur Kenntnisnahme vertrauenswürdiger Informationen kommen.	VT, IN, VF, AU, AN	TM 37 OM 4, OM 31	
171	1.5.4.1.1.1	Manipulation des MEs	ODER	Ein mobiles Endgerät kann auf verschiedene Arten manipuliert werden. Die Manipulation kann einen Angriff vorbereiten bzw. selbst einen Angriff darstellen.	IN	TM 13, TM 14, TM 15, TM 16, TM 22, TM 25, TM 26, TM 27, TM 28, TM 29, TM 32 OM 4, OM 5, OM 6, OM 14, OM 16, OM 19, OM 20	

172	1.5.4.1.1.1.1	Installation zusätzlicher Speicher zur Protokollierung vertraulicher Daten	ODER	Auf zusätzlichen Speichern können alle Aktivitäten des mobilen Endgerätes protokolliert werden (z. B. Passworteingaben des Nutzers). Weiterhin können vertrauliche Daten, die auf dem regulären Speicher verschlüsselt abgelegt werden, zuvor auf dem Zusatzspeicher unverschlüsselt abgelegt werden.	VT, AN	TM 14, TM 27, TM 28 OM 30, OM 31	
173	1.5.4.1.1.1.2	Installation zusätzlicher Kommunikationshardware zur Protokollierung/ Weiterleitung	ODER	Durch zusätzliche Kommunikationshardware können Daten während der regulären Übertragung gleichzeitig an unbefugte Dritte übermittelt werden. Auch kann zusätzliche Kommunikationshardware dazu genutzt werden, Befehle an das mobile Endgerät zu übermitteln.	VT, AN	TM 14, TM 27, TM 28 OM 30, OM 31	
174	1.5.4.1.1.1.3	Manipulation des Betriebssystems/ der Firmware	ODER	Das Betriebssystem bzw. die Firmware eines mobilen Endgerätes kann dahingehend manipuliert werden, dass es Befehle von entfernten Angreifern annimmt, ohne Rückmeldungen an den Benutzer Internetverbindungen aufbaut, Authentifizierungsvorgänge protokolliert, oder dass Sicherheitssoftware wirkungslos ist bzw. nicht startet etc..	VT, IN, VF, AU, VB	TM 13, TM 22, TM 23, TM 25, TM 26, TM 29, TM 32, TM 34 OM 1, OM 4, OM 5, OM 6, OM 14, OM 20, OM 19	
175	1.5.4.1.1.1.3.1	Verschaffung des Vollzugriffs auf Systemdateien und -bereiche (z. B. Symbian Hack)	UND		IN, VB	TM 13, TM 15 OM 4, OM 5, OM7, OM 19	
176	1.5.4.1.1.1.3.2	Manipulation ausführen	UND		IN		
177	1.5.4.1.1.1.4	Manipulation von Anwendungssoftware	ODER	Anwendungssoftware kann manipuliert werden, um unbemerkt Internetverbindungen aufzubauen, über welche dann Daten versendet werden oder um Befehle von entfernten Angreifern entgegen zu nehmen, oder um Verbindungen umzuleiten (Manipulation von Proxy-Verbindungen). Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, IN, VB	TM 13, TM 22, TM 23, TM 25, TM 26, TM 29, TM 32, TM 34 OM 1, OM 4, OM 5, OM 6, OM 14, OM 18, OM 19, OM 23	
178	1.5.4.1.1.1.4.1	Fälschung von Signierungszertifikaten	UND	Um manipulierte Anwendungssoftware auf einem mobilen Endgerät einzuschleusen, muss oftmals nicht nur die Anwendungssoftware manipuliert werden, sondern es müssen auch Zertifikate gefälscht werden, damit sich diese Anwendungssoftware installieren lässt.	VT, IN, VB		
179	1.5.4.1.1.1.4.2	Manipulation von Anwendungssoftware durchführen (z. B. Anwendungs-Proxy umleiten)	UND		VT, IN, VB		
180	1.5.4.1.1.1.5	Deaktivierung von Sicherheitsmaßnahmen	ODER	Sicherheitsmaßnahmen wie Sicherheitssoftware oder Authentifikationsmechanismen können deaktiviert werden, um andere Angriffe vorzubereiten.	VT, IN, VF, AU, VB, AN	TM 13, TM 25, TM 29 OM 4, OM 5, OM 6, OM 14, OM 19, OM 20	
181	1.5.4.1.1.1.6	Installation von Schadsoftware	ODER	Schadsoftware kann für verschiedene Angriffe genutzt werden oder kann Angriffe vorbereiten.	VT, IN, VF, AU, VB, AN	TM 13, TM 15, TM 20, TM 22, TM 23, TM 25, TM 26, TM 29, TM 34 OM 4, OM 5, OM 6, OM 14, OM 19, OM 20	

182	1.5.4.1.1.1.7	Ermittlung von Zugangsdaten	ODER	Um ein mobiles Endgerät zu manipulieren, kann es zuvor notwendig sein, dass die Zugangsdaten für eine Anmeldung am mobilen Endgerät ermittelt werden. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AN	TM 13, TM 23, TM 24, TM 26, TM 29 OM 4, OM 5, OM 6,OM 7, OM 8, OM 14, OM 15, OM 16, OM 18, OM 19, OM 20	Punkt ist identisch mit:1.5.1.2.5
183	1.5.4.1.1.1.8	Klonen des MEs	ODER	Ist die Manipulation des mobilen Endgerätes des Anzugreifenden nicht möglich, kann es sein, dass ein anderes mobiles Endgerät dem zu ersetzenden mobilen Endgerät nachempfunden wird, um es mit dem mobilen Endgerät des Anzugreifenden auszutauschen.	VT, IN, VF, AU, AN	TM 13, TM 25, TM 26, TM 27, TM 28, TM 29 OM 4, OM 5, OM 6, OM 8, OM 9, OM 10, OM 11, OM 12, OM 14, OM 16, OM 19	
184	1.5.4.1.1.1.8.1	Beschaffung eines Ersatzendgerätes	UND	Ein mobiles Endgerät, welches dem Endgerät des Anzugreifenden entspricht, muss beschafft werden.			
185	1.5.4.1.1.1.8.2	Klonen der SIM-Karte	UND	Um Manipulationen auch an der SIM-Karte vornehmen zu können, kann ein Klonen der SIM-Karte erforderlich sein. Dies ist jedoch nur mit SIM-Karten, die vor 2001 ausgegeben wurden, möglich.	VT, IN, VF, AU, AN		
186	1.5.4.1.1.1.8.3	Klonen des internen + externen Speichers	UND	Um dem Anzugreifenden glaubhaft zu machen, er halte auch wirklich sein mobiles Endgerät in Händen, kann der Speicher des "echten" mobilen Endgerätes geklont werden.	VT, IN, VF, AN	TM 13, TM 26 OM 19	
187	1.5.4.1.1.1.8.4	Manipulation des geklonten MEs	UND	Manipulationen, die für beabsichtigte Angriffe notwendig sind, müssen am geklonten Gerät vorgenommen werden.	VT, IN, VF, AU, AN		
188	1.5.4.2	Angreifer ist nicht im Besitz des MEs	ODER	Diese Angriffe stellen Bedrohungen dar, die auf ein mobiles Endgerät einwirken können, wenn der Angreifer nicht im Besitzt des mobilen Endgerätes ist.			
189	1.5.4.2.1	Manipulation des MEs aus Distanz	ODER				
190	1.5.4.2.1.1	Ausnutzung der kabelgebundenen Schnittstelle für Angriffe	ODER	Wird ein PC-System, mit dem ein mobiles Endgerät synchronisiert wird, von einem Angreifer manipuliert, so kann dies zur Folge haben, dass das mobile Endgerät während der Synchronisation mit Schadsoftware kompromittiert wird oder dass vertrauliche Informationen vom Angreifer ausgelesen werden.			
191	1.5.4.2.1.1.1	Manipulation des MEs durch kompromittierte(s) PC-System / Desktop-Synchronisationssoftware	ODER		VT, IN, VF, AU, VB, AN	TM 13, TM 15, TM 26, TM 29, TM 35, TM 36 OM 4, OM 5, OM 6, OM 19	
192	1.5.4.2.1.2	Ausnutzung der Mobilfunkschnittstelle für Angriffe	ODER	Mobilfunkschnittstellen können Angreifern Manipulationen von mobilen Endgeräten durch die unbefugte Verwendung von Diensten (OTA, SIM-Toolkit), die eigentlich dem Mobilfunkprovider vorbehalten sind, ermöglichen.			
193	1.5.4.2.1.2.1	Manipulation mittels OTA	ODER	Mittels der OTA-Provisioning lassen sich Konfigurationsdaten des mobilen Endgerätes teilweise völlig unbemerkt vom Nutzer verändern. Dies kann zur Folge haben, dass z. B. Internet-Verbindungen auf andere Server umgeleitet werden. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, IN, VF, AN	TM 6, TM 9, TM 31 OM 19	
194	1.5.4.2.1.2.2	Manipulation mittels SIM-Toolkit	ODER	Mittels SIM-Toolkit lassen sich Manipulationen (z. B. Ändern oder Hinzufügen von Menüpunkten) am mobilen Endgerät vornehmen. Dies kann zur Vorbereitung von Angriffen genutzt werden, aber auch zur Aktivierung von bereits auf dem mobilen Endgerät befindlicher Schadsoftware.	VT, IN, VF, AN	TM 6, TM 9, TM 31 OM 19	

195	1.5.4.2.1.3	Ausnutzung von WLAN-Schwachstellen (Treiber, Protokolle)	ODER	Weisen Treiber oder Protokolle, die für WLAN-Verbindungen genutzt werden, Schwachstellen auf, können diese von einem Angreifer dazu genutzt werden, Daten auszulesen, Daten zu verändern, sich unberechtigt Zugang zu verschaffen oder Schadsoftware einzuschleusen.	VT, IN, VF, VB, AN	TM 10, TM 21, TM 23, TM 34 OM 4, OM 5, OM 6, OM 31	Punkt ist identisch mit: 1.5.2.1.1, 1.5.3.1
196	1.5.4.2.1.4	Ausnutzung von Bluetooth-Schwach-stellen (Treiber, Protokolle)	ODER	Weisen Treiber oder Protokolle, die für Bluetooth-Verbindungen genutzt werden, Schwachstellen auf, können diese von einem Angreifer dazu genutzt werden, Daten auszulesen, Daten zu verändern, sich unberechtigt Zugang zu verschaffen oder Schadsoftware einzuschleusen.	VT, IN, VF, VB, AN	TM 12, TM 21, TM 22, TM 23, TM 34 OM 4, OM 5, OM 6, OM 19, OM 31	Punkt ist identisch mit: 1.5.2.1.2, 1.5.3.2
197	1.6.1	Installation nicht vertrauenswürdiger Soft-ware	ODER	Ist es dem Nutzer erlaubt, Anwendungssoftware selbständig zu installie-ren, so kann er diese auch aus nicht vertrauenswürdigen Quellen installie-ren. Dies erhöht die Gefahr, dass Schadsoftware auf das mobile Endgerät übertragen wird.	VT, IN, VF, VB, AN	TM 15, TM 20, TM 22, TM 23, TM 32, TM 34 OM 4, OM 5, OM 6, OM 23, OM 29	
198	1.6.2	Verwendung nicht vertrauenswürdiger Speichermedien	ODER	Speichermedien können präpariert sein, um z. B. Schadsoftware auf ein mobiles Endgerät zu übertragen. Werden diese vom Nutzer ohne vorheri-ge Prüfung verwendet, besteht die Gefahr einer Kompromittierung des mobilen Endgerätes. Es kann zur Zerstörung oder Veränderung von Daten kommen, außerdem ist eine Kenntnisnahme vertraulicher Informa-tionen ist möglich.	VT, IN, VF, VB, AN	OM 6, OM 10	
199	1.6.3	Kabelverbindungen mit nicht vertrauenswür-digem PC-System	ODER	Ein PC-System kann präpariert sein, um z. B. Schadsoftware auf ein mobiles Endgerät zu übertragen. Wird das mobile Endgerät vom Nutzer mit einem "fremden" PC-System verbunden, besteht die Gefahr einer Kompromittierung des mobilen Endgerätes. Es kann zur Zerstörung oder Veränderung von Daten kommen, außerdem ist eine Kenntnisnahme vertraulicher Informationen möglich.	VT, IN, VF, VB, AN	OM 6, OM 10	
200	1.6.4	permanenter Betrieb drahtloser Schnitt-stellen (BT, WLAN)	ODER	Werden drahtlose Kommunikationsschnittstellen nach dem Gebrauch (z. B. Übertragung einer digitalen Visitenkarte) nicht wieder deaktiviert, gibt man einem Angreifer unnötig lang Zeit, das Endgerät bzw. seine Schnitt-stelle auf Schwachstellen hin zu analysieren und sich eventuell Zugriff auf das mobile Endgerät zu verschaffen.	VT, IN, VF, VB, AN	OM 4, OM 6, OM 31	
201	1.6.5	falscher Umgang mit Passwörtern	ODER				
202	1.6.5.1	Verwendung schwacher Passwörter/ PINs	ODER	Werden semantische oder einfache Passwörter (z. B. "Passwort", "12345") verwendet, können diese sehr einfach erraten werden (manuell, computergestützt). Dadurch kann sich ein Angreifer ohne großen Aufwand in kürzester Zeit Zugriff verschaffen. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AU	OM 4, OM 5, OM 6, OM 14, OM 18	
203	1.6.5.2	Beobachtung der Passwort-/ PIN-Eingabe zulassen	ODER	Werden Zugangsdaten leichtfertig "unter den Augen" anderer eingegeben, besteht die Gefahr, dass Angreifer die Eingabe beobachten und sich mittels dieser Daten Zugriff auf ein System verschaffen können. Eine Kenntnisnahme vertraulicher Informationen ist möglich.	VT, AU	OM 4, OM 5, OM 6,OM 7, OM 8, OM 17	
204	1.6.5.3	Übermittlung von Passwörtern im Klartext / Weitergabe an Dritte	ODER	Werden Zugangsdaten leichtfertig z. B. per E-Mail im Klartext übermittelt, oder an Unbefugte weitergegeben, besteht die Gefahr der Kenntnisnahme durch Dritte, die sich mittels dieser Daten Zugriff auf ein System verschaf-fen können.	VT, AU	OM 4, OM 6, OM 7	
205	1.6.6	Social Engineering	ODER	Wird ein Mitarbeiter Opfer von Social Engineering, so sind verschiedene Gefahren für das mobile Endgerät und das lokale Unternehmensnetzwerk denkbar. Das Verraten von vertraulichen Informationen (z. B. Zugangsda-ten) kann zur Kenntnisnahme weiterer vertraulicher Informationen führen.	VT, AU, AN	OM 4, OM 6, OM 7	Punkt ist identisch mit: 1.5.1.2.4, 1.5.1.2.5.2
206	1.6.6.1	freiwillig Mitteilen	ODER				
207	1.6.6.2	Täuschung des Benutzers	ODER				
208	1.6.6.3	Bedrohung des Benutzers	ODER				

209	1.6.6.4	Erpressung des Benutzers	ODER				
210	1.6.7	Preisgabe vertraulicher Daten	ODER	Geben Mitarbeiter vertrauliche Informationen preis (oftmals durch Social Engineering forciert), so kann dies Angriffe begünstigen und zur Kenntnisnahme weiterer vertraulicher Informationen führen.	VT, AN	OM 4, OM 6, OM 7	
211	1.6.7.1	Preisgabe von Zugangsdaten	ODER				
212	1.6.7.2	Preisgabe von Infrastrukturinformationen (z. B. verwendete Hardware und Software)	ODER				
213	1.6.8	unnötiges Mitführen vertraulicher Daten	ODER	Führt ein Mitarbeiter unnötig sensible Daten auf dem mobilen Endgerät mit sich, ist das Ausmaß der eventuellen Kenntnisnahme durch einen Angreifer unnötig hoch.	VT, IN, AN	TM 24 OM 4, OM 6, OM 7	
214	1.6.9	fehlende Akzeptanz für IT-Sicherheitsmaßnahmen	ODER	Versteht ein Nutzer die Notwendigkeit von Sicherheitsmaßnahmen nicht, so kann es vorkommen, dass er versucht, die eventuell durch Sicherheitsmaßnahmen entstehenden "Unannehmlichkeiten" (z. B. häufige Passworteingabe) durch die Deaktivierung der Sicherheitsmaßnahmen zu vermeiden.		OM 4, OM 5, OM 6	
215	1.6.9.1	Deaktivierung von Sicherheitsmaßnahmen	ODER	Die Deaktivierung von Sicherheitsmaßnahmen kann Angriffe begünstigen bzw. deren Erkennung und Verhinderung unmöglich machen.			
216	1.6.9.1.1	Deaktivieren von Passwörtern/ PIN-Abfragen	ODER		VT, IN, AN	OM 4, OM 5, OM 6	
217	1.6.9.1.2	Deaktivieren von Sicherheitssoftware (Firewall, Anti-Virus, Intrusion-Detection)	ODER				
218	1.6.10	"aus der Hand geben" des MEs	ODER	Verliert der Nutzer ein mobiles Endgerät, lässt er es unbeaufsichtigt zurück oder verleiht er es an jemanden, ist eine Kenntnisnahme vertraulicher Informationen möglich. Weiterhin kann sich dann ein Unbefugter Zugriff auf das lokale Unternehmensnetzwerk verschaffen bzw. das Endgerät kann dann manipuliert und anschließend zurückgegeben werden etc.	VT, IN, VF, AU, VB, AN	TM 25, TM26, TM 37 OM 4, OM 9, OM 11, OM 12, OM 13, OM 21, OM 31	Punkt ist identisch mit: 1.5.1.2.1, 1.5.3.5
219	1.6.10.1	Entwendung des MEs	ODER				
220	1.6.10.2	Verleih des MEs	ODER				
221	1.6.10.3	Zurücklassen des MEs	ODER				

Tab. 5-1: Bedrohungskatalog inklusive zugeordneter Sicherheitsmaßnahmen

A.3 Sicherheitsmaßnahmenkatalog

Legende:

VT Vertraulichkeit, IN Integrität, VF Verfügbarkeit, AU Authentizität, VB Verbindlichkeit, AN Anonymität, OM Organisatorische Maßnahme, TM Technische Maßnahme

Nr.	Sicherheitsmaßnahme	verfolgte Sicherheitsziele	Bemerkung (Quellenangabe, Bsp. für Sicherheitslösungen)
	Technische Sicherheitsmaßnahmen		
	Maßnahmen für die Kommunikationssicherheit		
TM 1	**Mobiltelefone mit Verschlüsselungsanzeige verwenden (Mobilfunk):** Verwendung von Mobiltelefonen mit Warnfunktion bei unverschlüsselter GSM-/UMTS-Verbindung (beispielsweise je nach Hersteller durch ein offenes Schloss-Symbol am oberen Bildschirmrand dargestellt)	VT, VF	Vgl. [BSI08a, 25]
TM 2	**(Sprach-)Datenverbindungsverschlüsselung einsetzen (Ende-zu-Ende-Verschlüsselung):** Eine Verschlüsselung der Datenübertragung (bei WLAN BT GSM/UMTS) ist zwingend notwendig. Sofern die Verschlüsselung nicht bereits von den verwendeten Server- und Client-Komponenten vorgesehen ist, muss eine dienstunabhängige Lösung mit Crypto-Sprach-Ein-Ausgabemodulen (Hardware) oder Crypto-Software (z. B. mittels VPN-Tunnel o. ä.) implementiert werden. (Einhaltung dieser Maßnahme mittels der Maßnahmen OM 5, OM 6 und OM 7 gewährleisten.)	VT, IN, VB, AN	Vgl. [BSI08a, 25] Bsp.: CORISECIO Mobile Suite – Enterprise, TheGreenBow VPN Mobile, Cellcrypt Mobile for Blackberry, Cryptophone, T-Systems - SiMKo 2
TM 3	**SMS-Verschlüsselungssoftware einsetzen:** Sind vertrauliche Daten mittels SMS zu übertragen, so sollte mittels entsprechender Software vor dem Versand eine Verschlüsselung der SMS auf dem mobilen Endgerät erfolgen. Entsprechende Software ist bei den Endgeräten der Kommunikationspartner zu installieren. (Einhaltung dieser Maßnahme mittels der Maßnahmen OM 5, OM 6 und OM 7 gewährleisten.)	VT, IN, VB, AN	Vgl. [BSI08a, 70] Bsp.: CircleTech – SMS007, Kryptext – 'KRYPTEXT', T-Systems - SiMKo 2
TM 4	**E-Mail-Verschlüsselungssoftware einsetzen:** Sind vertrauliche Daten mittels E-Mail zu übertragen, so sollte mittels entsprechender Software vor dem Versand eine Verschlüsselung der E-Mail auf dem mobilen Endgerät erfolgen. (Einhaltung dieser Maßnahme mittels der Maßnahmen OM 5, OM 6 und OM 7 gewährleisten.)	VT, IN, VB, AN	Bsp.: TheGreenBow CryptoMailer, T-Systems - SiMKo 2
TM 5	**Ausschließlich UMTS verwenden:** Um Man-in-the-Middle-Angriffe mittels eines IMSI-Catchers zu verhindern, kann das mobile Endgerät so konfiguriert werden, dass ausschließlich UMTS für die Mobilfunkverbindungen genutzt wird. Da der IMSI-Catcher-Einsatz nur durch einen Fallback von UMTS auf GSM ermöglicht wird, kann somit eine Verbindung nicht zustande kommen, da das mobile Endgerät nicht mittels GSM sendet.	VT, AN	
TM 6	**SMS / MMS Funktionalität deaktivieren:** Ist das Senden und Empfangen von SMS/MMS für den Nutzer nicht notwendig, kann eine Deaktivierung dieser Funktionen vorgenommen werden. Die dafür notwendigen Schritte (Eingabe eines bestimmten Codes, Deaktivierung beim Provider) werden am mobilen Endgerät vorgenommen. Es kann unter Umständen sein, dass die Möglichkeit der Sperrung/Deaktivierung von SMS/MMS erst durch den Mobilfunknetzbetreiber bestätigt werden muss. Alternativ lassen sich mit bestimmter Zusatzanwendungssoftware eingehende SMS/MMS filtern.	VT, AN	Vgl. [BSI08a, 70]
TM 7	**Proxy-Verbindungen nur selektiv einsetzen:** Die Nutzung von Anwendungs-Proxys bzw. von Informationsablagen oder -weiterleitungen auf Server im Internet ist zu vermeiden. Ist der Verzicht nicht gänzlich möglich bzw. selektiv notwendig, so sind strikte Regeln (z. B. Nutzung nur bei nicht sensiblen Datenübertragungen) für die Verwendung von Proxy-Servern festzuhalten und durchzusetzen.	VT, IN, AU, VB, AN	Vgl. [BSI08a, 89]
TM 8	**WAP-Profil löschen:** Wird das WAP-Zugangsprofil gelöscht, können keine WAP-Push-Nachrichten mehr empfangen werden. Somit entgeht man der Gefahr, durch WAP-Push-Nachrichten auf manipulierte Webseiten weitergeleitet zu werden. Allerdings kann ein Angreifer mittels OTA-Provisioning neue Konfigurationsdaten auf das Mobiltelefon übertragen.	VT, AN	Vgl. [BSI08a, 81]
TM 9	**Konfiguration des mobilen Endgeräts (techn.) regelmäßig kontrollieren:** Um die Bedrohungen durch OTA-Provisioning und ähnliche Techniken zu minimieren, sollte die Konfiguration, besonders die Konfiguration von (Internet-) Zugangsprofilen regelmäßig von einer zentralen Stelle (Fernwartungssysteme für mobile Endgeräte) kontrolliert werden.	VT, IN, VF, AN	
TM 10	**WLAN-Verbindungen absichern:** Bei der Nutzung von WLAN-Verbindungen sind die Sicherheitsrichtlinien für sicheres WLAN bei der WLAN-Konfiguration mobiler Endgeräte zu befolgen (z. B. SSID verbergen, Verschlüsselung etc.).	VT, IN, VF, AU, VB, AN	Vgl. dazu z. B. [Tern05], [Fisc06], [FiMa10]
TM 11	**Gegenseitige Geräte-Authentisierung durchführen:** Vor dem Aufbau eines sicheren Kommunikationskanals müssen sich Server und mobile Endgeräte gegenseitig authentisieren. Der Nachweis der Identität geschieht mittels Zertifikaten.	VT, AU, VB	Vgl. [BSI08a, 96]
TM 12	**BT-Schnittstelle absichern:** Die Bluetooth-Schnittstelle ist so zu konfigurieren, dass sie für andere Geräte nicht sichtbar ist und nur gesicherte Verbindungen mit bekannten Geräten akzeptiert. Darüber hinaus ermöglichen einige Geräte den Schutz der BT-Schnittstelle mit Hilfe von Antivirus- und Firewallsoftware (Geräteauswahl beachten!).	VT, VF, VB	Vgl. [BSI08a, 120]

	Maßnahmen für die Endgerätesicherheit		
TM 13	**Datenverschlüsselung auf dem mobilen Endgerät anwenden (techn.):** Zur Verschlüsselung von Daten auf dem mobilen Endgerät sollten Programme eingesetzt werden, die es ermöglichen, einzelne Dateien, Dateisystembereiche oder ganze Dateisysteme zu verschlüsseln. Des Weiteren kann man zur zusätzlichen Absicherung den Arbeitsspeicher des mobilen Endgerätes verschlüsseln, sodass aus dem Arbeitsspeicher eines entwendeten, eingeschalteten Gerätes keine vertraulichen Informationen ausgelesen werden können, die sich noch im Arbeitsspeicher befinden. Die verwendeten Verschlüsselungsprogramme sollten weiterhin die Möglichkeit bieten, nach einer vordefinierten Anzahl an falschen Authentisierungen den gesamten Speicher des mobilen Endgerätes unwiederbringlich zu löschen. (Einhaltung dieser Maßnahme mittels der Maßnahmen OM 5, OM 6 und OM 7 gewährleisten.)	VT, VB	Vgl. [BSI08a, 116]Bsp.: Kaspersky Mobile Security Enterprise Edition, Symantec Mobile Security Suite für Windows Mobile, CREDANT Mobile Guardian, NEXERA Device Management, T-Systems - SiMKo 2
TM 14	**Zugriffskontrolle für Hardwareerweiterungen begrenzen:** Um das Bedrohungspotential von Hardwareerweiterungen zu begrenzen, sind Ergänzungen oder Änderungen am Betriebssystem denkbar, die eine Nutzung von Geräteschnittstellen, wie z. B. Erweiterungssteckplätzen, begrenzen. Dies kann durch die Verwendung von SmartCards erreicht werden, da diese auch nach dem Auffinden fast nicht unautorisiert verwendet oder verändert werden können. (siehe dazu auch Maßnahme TM 26)	IN, VF	Vgl. [BSI06, 29] Bsp.: certgate Mobile SmartCard Solution
TM 15	**Zugriffskontrolle für Softwareerweiterungen begrenzen:** Um das Bedrohungspotential von Softwareerweiterungen zu begrenzen, ist der Einsatz von Anwendungssoftware denkbar, die ausschließlich das Ausführen der Anwendungen erlaubt, die zuvor in einer Liste hinterlegt wurden. Damit ist es möglich, heruntergeladene Anwendungssoftware, die Schadcode enthält, an ihrer Ausführung zu hindern. Des Weiteren sollte eine Autorisierungsabfrage (z. B. Passwort, PIN Abfrage) vor der Installation von Softwareerweiterungen, bspw. wie bei JavaCard-Betriebssystemen (Vgl. Hinz /Chipkartenbetriebssysteme/ 296), etabliert werden. Dies verhindert die Installation von Schadsoftware durch unbefugte Dritte bzw. durch den Nutzer.	IN, VF	Vgl. [BSI06, 29] Bsp.: CREDANT Mobile Guardian (Blacklist, Whitelist Feature)
TM 16	**Zugriffskontrolle für Gerätefunktionen aktivieren:** Wird ein mobiles Endgerät mittels 'full SIM-Card-Lock' an eine einzige SIM-Karte oder eine SmartCard gebunden, so kann das Auslesen von Nutzerdaten auf dem mobilen Endgerät in Verbindung mit einer Verschlüsselung der Daten auf dem mobilen Endgerät unterbunden werden. Sind die Nutzerdaten auf dem mobilen Endgerät nicht verschlüsselt, so wird ein Auslesen der Daten lediglich erschwert. Dies ist aber nur gegeben, wenn das mobile Endgerät den Zugriff auf seine Funktionen nur mit eingelegter SIM-Karte/SmartCard erlaubt. Auch ist es weiterhin möglich, den internen Speicher auf anderem Wege auszulesen, ohne am Gerät angemeldet zu sein.	VT, AN	Vgl. [BSI08a, 26]
TM 17	**Schutzmaßnahmen für aktive Inhalte einrichten:** Die für den Zugriff auf aktive Inhalte (wie z. B. JavaScript, Flash) üblichen Schutzmaßnahmen (Deaktivieren dieser Funktionen in Browsern und anderen Anwendungen) aus dem PC-System-Bereich gelten auch für den Umgang mit diesen Inhalten auf mobilen Endgeräten.	VT, IN, VF	Vgl. [BSI08a, 81]
TM 18	**Herunterladen von Inhalten nur mit Zustimmung durch den Benutzer erlauben:** Die Konfiguration von mobilen Endgeräten sollte es grundsätzlich vorsehen, dass eine Bestätigung des Nutzers vor dem Herunterladen jedweder Inhalte erforderlich ist. Dies sollte sowohl für die Internetnutzung mittels Browser als auch für MMS gelten. Über Kommunikationsschnittstellen sollten ebenfalls keine Inhalte ohne die Bestätigung des Nutzers auf das mobile Endgerät übertragen werden.	VT, IN, VF	Vgl. [BSI08a, 81]
TM 19	**Verbindungsherstellung nur mit Zustimmung durch den Benutzer erlauben:** Die Konfiguration von mobilen Endgeräten sollte es grundsätzlich vorsehen, dass eine Bestätigung des Nutzers vor dem Aufbau einer Internetverbindung erforderlich ist. Dies kann durch einen Dialog mit einer Ja/Nein Bestätigung erfolgen oder durch die vorhergehende Auswahl unter mehreren Verbindungsprofilen. Damit kann ein Verbindungsversuch vom Nutzer abgebrochen werden, sollte er diesen nicht ausgelöst haben.	VT, AU, AN	Vgl. [BSI08a]
TM 20	**Antivirussoftware auf mobilen Endgeräten einsetzen:** Die Verwendung von Antivirussoftware verbessert den Schutz vor Schadsoftware. Es soll eine aktive Überwachung der Datenübertragung stattfinden. Weiterhin sind manuelle oder automatisierte Suchroutinen vorhanden, die regelmäßig den Gerätespeicher nach Schadsoftware absuchen und gegebenenfalls entfernen. Diverse Produkte gewährleisten auch einen E-Mail- und SMS-Spam-Schutz. (Einhaltung dieser Maßnahme mittels der Maßnahmen OM 5, OM 6 und OM 7 gewährleisten.)	VT, IN, VF	Vgl. [BSI08a, 127] Bsp.: McAfee Mobile Security for Enterprise, Kaspersky Mobile Security Enterprise Edition
TM 21	**Firewallsoftware auf mobilen Endgeräten einsetzen:** Die Verwendung von Firewallsoftware verbessert den Schutz vor Angriffen über offene Ports des Endgerätes. Sie entscheidet anhand definierter Regeln, ob bestimmte Datenpakete das Endgerät verlassen bzw. auf das Endgerät gelangen dürfen. (Einhaltung dieser Maßnahme mittels der Maßnahmen OM 5, OM 6 und OM 7 gewährleisten.)	VT, VF, VB	Bsp.: F-Secure Mobile Security for Business, CORISECIO Mobile Suite – Enterprise
TM 22	**Intrusion-Detection-Software (IDS) auf mobilen Endgeräten einsetzen:** IDS geht ähnlich einer Antivirussoftware vor, indem Muster bekannter Angriffe hinterlegt werden. Treten Ereignisse auf, die zu diesen Mustern passen, so wird ein Intrusion-Alarm ausgelöst (E-Mail an den Administrator bzw. Meldung an den Nutzer) oder es wird sogar das Endgerät oder ein Teil des Endgerätes gesperrt bzw. isoliert. (Einhaltung dieser Maßnahme mittels der Maßnahmen OM 5, OM 6 und OM 7 gewährleisten.)	VF, VB	
TM 23	**Sicherheits-Updates regelmäßig auf mobile Endgeräte einspielen:** Die durch den Hersteller zur Verfügung gestellten Betriebssystemupdates und Anwendungssoftwareupdates, die eventuell von Schadsoftware genutzte Sicherheitslücken schließen, müssen unverzüglich installiert werden.	VF	

TM 24	**Vertrauliche Daten sicher löschen:** vertrauliche Daten, die auf einem mobilen Endgerät oder auf Erweiterungsspeichermedien gespeichert waren, sollten, nachdem sie nicht mehr benötigt werden, so gelöscht werden, dass sie sich nicht wiederherstellen lassen. Sollte ein Angreifer in den Besitz des mobilen Endgerätes gelangen, kann dadurch die Wiederherstellung ehemals gespeicherter, sensibler Daten verhindert werden. (In diesem Zusammenhang ist Maßnahme OM 8 zu beachten.)	VT, AN	Bsp.: NEXERA Device Management
TM 25	**Benutzer müssen sich am mobilen Endgerät authentisieren:** Um unbefugte Dritte am Zugang zu einem mobilen Endgerät zu hindern, muss sich der Nutzer am mobilen Endgerät authentisieren. Hierfür stehen verschiedene Techniken zur Verfügung: PIN-Eingabe, Passworteingabe, biometrische Merkmale oder durch die Verwendung von SmartCards. Außerdem sollte, wenn es technisch möglich ist, eine Eingabe der Authentisierungsdaten beim Wechsel der SIM-Karte erforderlich sein. (Einhaltung dieser Maßnahme mittels der Maßnahmen OM 5, OM 6, OM 7, OM 17, OM 20 gewährleisten.)	VT, IN, VF	Vgl. [BSI08a, 97]
TM 26	**Smart-Cards zur Sicherung schutzbedürftiger Anwendungssoftware und Daten einsetzen:** SmartCards können zur Sicherung von VPN-Verbindungen, Verschlüsselung von Speichern, Aufbewahrung sensibler Daten und Zertifikate, oder für starke Authentisierungen verwendet werden. Auch können sie das Aufrufen von Webseiten absichern, indem Internetlinks über in der SmartCard gespeicherte Links aufgerufen werden. So werden Link-Manipulationen (Phishing) wirkungslos.	VT, IN, AU, VB, AN	Vgl. [Hinz06] und [Papa06] Bsp.: certgate Mobile SmartCard Solution
TM 27	**Verschlussmechanismen vor Ausgabe des Gerätes versiegeln:** Schrauben, Clips und andere Verschlussmechanismen sollten vor der Ausgabe an den Nutzer mit Spezialfarben versiegelt werden. Dies ermöglicht eine Erkennung von Manipulationen.	IN	Vgl. [BSI08a, 115]
TM 28	**Keine mobilen Endgeräte mit austauschbaren Zierschalen einsetzen:** Der Verzicht auf mobile Endgeräte mit austauschbaren Zierschalen erschwert den Zugang zur Gerätehardware. Das Durchführen von Manipulationen wird somit erschwert. Ist ein Verzicht auf Endgeräte mit austauschbaren Zierschalen nicht möglich, sollten die Zierschalen nach der Maßnahme TM 27 behandelt werden.	IN	Vgl. [BSI08a, 116]
TM 29	**Synchronisationsschnittstelle deaktivieren oder schützen:** Wird die Synchronisationsschnittstelle nicht benötigt, so empfiehlt sich eine dauerhafte Deaktivierung, ohne die Möglichkeit, dass der Nutzer diese selbst aktivieren kann. Ist es nicht möglich, die dauerhafte Deaktivierung mit technischen Mitteln sicherzustellen, so sollte dies mittels der Maßnahmen OM 5, OM 6 und vor allem mittels der Maßnahme OM 7 sichergestellt werden. Muss die Synchronisationsschnittstelle genutzt werden, so ist diese Schnittstelle unbedingt mit Authentifizierungsmechanismen zu schützen. Dies kann mittels PIN, Passwortabfrage oder SmartCards geschehen. Dabei sollten die Authentifizierungsinformationen nicht auf dem zu synchronisierenden Arbeitsplatzrechner abgespeichert sein.	VT, IN, VF, AU	Vgl. [BSI08a, 116]
TM 30	**Kommunikationsschnittstellen bei Nichtbenutzung ausschalten:** Kommunikationsschnittstellen (BT, WLAN, IrDA) können potentielle Angriffsmöglichkeiten für Dritte sein. Werden diese nicht nach Gebrauch wieder deaktiviert, können Angreifer Geräte auf Schwachstellen analysieren bzw. unbefugt Zugriff auf diese erlangen. Sind diese Schnittstellen nur für kurze Zeit aktiviert, reduziert dies die Zeit für Analysen des Endgerätes. Dies sollte ebenfalls für die Synchronisationsschnittstelle zutreffen. Wird diese nur selten genutzt, so ist sie für den Zeitraum der Nichtnutzung zu deaktivieren.	VF, AN	Vgl. [BSI06, 28]
TM 31	**Übernahme von OTA-Provisioning-Daten nur mit Zustimmung des Benutzers erlauben:** Gegen OTA-Provisioning, SIM-Toolkit und verwandte Techniken besteht hinsichtlich des Nutzers kaum eine Schutzmöglichkeit. Lediglich die Provider wären in der Lage, entsprechende SMS-Nachrichten mit Provisioning-Inhalten, die nicht von ihnen selbst stammen, herauszufiltern. Sollte es technisch möglich sein, muss ein mobiles Endgerät so konfiguriert werden, dass Konfigurationsänderungen mittels OTA-Provisoning nur auf ausdrückliche Nutzerinteraktion zugelassen werden.	IN, VF, VB	Vgl. [BSI08a, 124]
	Sonstige technische Sicherheitsmaßnahmen		
TM32	**Sicherheitsmanagementsysteme etablieren:** Zur Durchsetzung der Sicherheitspolicy eines Unternehmens existieren Programme oder betriebssysteminterne Mechanismen, die vorgegebene Sicherheitsrichtlinien auf mobilen Endgeräten durchsetzen. Dabei existieren Lösungen, die sowohl einfaches Policy- und Schlüsselmanagement realisieren, aber auch die zentrale Verwaltung von Sicherheitsprofilen und Benutzern ermöglichen. Weiterhin existieren Produkte, die einen Mehrbenutzerbetrieb für mobile Endgeräte ermöglichen. Diese Maßnahme soll technisch die für das Unternehmen erstellte Sicherheitspolicy durchsetzen.	VT, IN, VF, AU, AN	Vgl. [BSI06, 29] Bsp.: CORISECIO Mobile Suite - Enterprise, certgate Mobile SmartCard Solution, NEXERA Device Management
TM33	**Fernlöschsoftware für mobile Endgeräte einsetzen:** Im Falle des Verlustes des Endgerätes sollte es die Möglichkeit geben, das Endgerät zu Sperren oder seinen Speicher zu löschen. Existiert keine bereits integrierte Funktion, sollte eine solche mit Zusatzsoftware realisiert werden. (Oftmals wird die Funktion der Fernlöschung von den in der Maßnahme "Einsatz von Fernwartungssoftware für mobile Endgeräte" erwähnten Fernwartungssystemen ebenfalls realisiert.)	VT, AU, VB, AN	Vgl. [BSI08a, 96] Bsp.: Microsoft System Center Mobile Device Manage, NEXERA Device Management
TM 34	**Fernwartungssoftware für mobile Endgeräte einsetzen:** Verschiedene Hersteller bieten Lösungen an, die in der Lage sind, mobile Endgeräte (verschiedener Plattformen) zentral zu verwalten. Dies stellt sicher, dass alle Geräte auf dem gleichen Stand sind und dass Administratoren für die Wartung (Updates, Anwendungssoftwareinstallation) nicht warten müssen, bis ein Mitarbeiter wieder in das Unternehmen zurückkehrt.	VF	Bsp.: NEXERA Device Management
TM 35	**Sicherheits-Updates für Synchronisations- und Fernwartungssoftware regelmäßig einspielen:** Die durch den Hersteller zur Verfügung gestellten Updates für Desktop-Synchronisationssoftware, Server-Synchronisationssoftware und Fernwartungssoftware, die eventuell von Schadsoftware genutzte Sicherheitslücken schließen, müssen unverzüglich installiert werden.	VF	

TM 36	**Sicherheits-Updates für PC-Systeme, die Verbindungen mit mobilen Endgeräten eingehen, regelmäßig einspielen:** Betriebssysteme und Anwendungssoftware der PC-Systeme (Arbeitsplatzrechner, Server), die mit den mobilen Endgeräten Verbindungen aufbauen können, sind ebenfalls durch Sicherheits-Updates auf dem aktuellen Stand zu halten, um Angriffspunkte zu schließen bzw. zu minimieren.	VF	
TM 37	**Demilitarisierter Zonen einrichten:** Demilitarisierte Zonen können den Zugriff von mobilen Endgeräten auf lokale Unternehmensnetze stark reglementieren. Ist ein mobiles Endgerät kompromittiert, so kann der dadurch entstehende Schaden begrenzt werden.	VT, IN, AU	
	Organisatorische Sicherheitsmaßnahmen		
OM 1	**Mobile Endgeräte in die Erstellung der Sicherheitspolicy des Unternehmens einbeziehen:** mobile Endgeräte dürfen in ihrem Bedrohungspotential für die Sicherheit der Unternehmensdaten nicht unterschätzt und somit außen vor gelassen werden. Mobile Endgeräte sind in die Erstellung der Sicherheitspolicy des Unternehmens mit einzubeziehen.	VT, IN, VF, AU, VB, AN	
OM 2	**Administratoren für die Besonderheiten mobiler Endgeräte schulen:** Administratoren sollten bezüglich der Besonderheiten, die es bei den mobilen Endgeräten zu beachten gilt, geschult werden. Dies gilt sowohl für den Umgang bzw. die Administration der mobilen Endgeräte als auch für die speziellen Bedrohungen für mobile Endgeräte bzw. durch mobile Endgeräte.	VF	Vgl. [Fisc06, 100]
OM3	**Nutzer im sorgsamen Umgang mit Systemen und Anwendungen schulen:** Jede Kurzmitteilung, MMS oder E-Mail sollte objektiv auf den Wahrheitsgehalt von Absender und Inhalt geprüft werden. Bestehen Zweifel, so ist eine Rückfrage beim vermeintlichen Absender durchzuführen. Die Rückfrage sollte allerdings über Telefonnummern erfolgen, die dem Empfänger vom Absender bekannt sind und nicht durch Rückrufnummern im Nachrichtentext. Ist der Absender nicht bekannt, so sollten die Nachrichten umgehend gelöscht werden. Besteht die Möglichkeit, OTA-Provisioning-SMS, d. h. Konfigurationseinstellungsnachrichten, beim Empfang zu bestätigen oder abzulehnen, sollte mit dem Mobilfunkprovider Rücksprache gehalten werden, ob eine Änderung der Zugangsdaten veranlasst wurde, andernfalls sind diese Nachrichten zu löschen bzw. der Rückfragedialog, der durch diese Nachrichten ausgelöst wurde, zu verneinen. Besser sollten solche Einstellungen immer abgelehnt werden und stattdessen per Hand nach den Angaben des Mobilfunkproviders im mobilen Endgerät eingetragen werden. Auch bei der Internetnutzung sollte erhöhte Sorgfalt herrschen. Bspw. sollten Internetlinks per Hand eingegeben werden und nicht aus E-Mails kopiert oder angeklickt werden.	VT, IN, VF, AU, AN	Vgl. [BSI08a, 70] Bsp.: Links in HTML-E-Mails sollte man auf das tatsächliche Ziel untersuchen, bevor man einen solchen Link anklickt. (eine solche Möglichkeit bietet bspw. das BlackBerry OS Version 4.6)
OM 4	**Nutzer für Sicherheitsmaßnahmen sensibilisieren:** Die Nutzer müssen für die Wichtigkeit der Sicherheitsmechanismen sensibilisiert werden. Der Nutzer muss verstehen, dass entsprechende Sicherheitsmaßnahmen notwendig sind, um die mitgeführten und versendeten Daten vor der Kenntnisnahme Dritter zu schützen. Kann ein Nutzer nicht technisch dazu gezwungen werden, z. B. eine E-Mail vor dem Versenden zu verschlüsseln, sondern hätte er auch die Möglichkeit, dies ohne Verschlüsselung zu tun, so sollte er dies aus dem Verständnis für die Sicherheitsmaßnahmen heraus dennoch tun.	VF	
OM 5	**Nutzer im Umgang mit den Sicherheitsmaßnahmen schulen:** Die Nutzer müssen mit der Bedienung und den Funktionen der Sicherheitsmechanismen vertraut gemacht werden. Kann ein Nutzer z. B. nicht mit einem VPN-Client umgehen, so wird er diesen auch nicht benutzen, sondern eine unsichere Verbindung aufbauen.	VF	
OM 6	**Nutzer zur Einhaltung und Anwendung von Sicherheitsmaßnahmen verpflichten:** Auch wenn ein Nutzer wie in den Maßnahmen OM 5 und 6 für die Sicherheitsmaßnahmen sensibilisiert und geschult wurde, so kann er dennoch versuchen, gewisse "lästige" Maßnahmen abzuschalten. Daher sollten Mitarbeiter zusätzlich durch organisatorische Regelungen oder durch rechtliche Verpflichtungen (Arbeitsvertrag etc.) dazu angehalten werden, etablierte Sicherheitsmaßnahmen anzuwenden.	VF	
OM 7	**Nutzer für den Umgang mit sensiblen Daten schulen:** Schulung und Sensibilisierung der Nutzer im Umgang mit sensiblen Daten vornehmen; insbesondere bezogen auf das Mitführen sensibler Daten auf mobilen Endgeräten; Es sollten nur immer die Daten das Unternehmen verlassen, die auch wirklich benötigt werden. Mittel- und langfristig nicht benötigte Daten sollten von den mobilen Endgeräten unwiederbringlich gelöscht werden. (In diesem Zusammenhang ist Maßnahme TM 24 zu beachten.) Zum Umgang mit sensiblen Daten zählen nicht nur elektronische Dokumente, sondern auch alle anderen Daten und Informationen das Unternehmen betreffend (bspw. verwendete Hardware, verwendete Software, Zugangsdaten, zyklische Erneuerung von Zugangsdaten etc.).	VT, AU, VB, AN	
OM 8	**Aufmerksamer Umgang mit mobilen Endgeräten in der Öffentlichkeit:** Werden mobile Endgeräte in der Öffentlichkeit benutzt, empfiehlt sich ein sorgsamer Umgang mit sensiblen Daten. Dies betrifft im Besonderen die Eingabe von PIN und Passwörtern, die nur unter Sichtschutz gegenüber anderen Personen eingegeben werden dürfen.	VT, AU, VB, AN	Vgl. [BSI08a, 115]
OM 9	**Transport und Aufbewahrung von mobilen Endgeräten sichern:** Eine sichere Aufbewahrung des mobilen Endgerätes, der SIM-Karte und eventuell eingesetzter SmartCards und Speichermedien (z. B. in verschließbaren Taschen), sowie kein Zurücklassen in unsicheren Räumen bzw. allgemein unbeobachtetes Zurücklassen (z. B. in öffentlich zugänglichen Räumen, Kfzs usw.), ist die wirksamste Maßnahme gegen die Manipulation des Endgerätes und eine Erschleichung einer digitalen Identität.	VT, VB	Vgl. [BSI08a, 115]
OM 10	**Zugang zum mobilen Endgerät beschränken:** Unbefugten Personen ist unter keinen Umständen ein (unbeaufsichtigter) Zugriff auf das mobile Endgerät zu gestatten. Die Gefahr von Manipulationen (z. B. Installation von (kommerzieller) Überwachungssoftware) ist sonst nicht auszuschließen. Dies gilt auch für die Verwendung von Speichermedien bzw. das Verbinden des mobilen Endgerätes mit fremden PC-Systemen.	VT, IN, VF, AU, AN	Vgl. [BSI06, 30]

OM 11	**Mobile Endgeräte nicht verleihen:** Ein mobiles Endgerät sollte nicht an andere Personen ausgeliehen werden. Sollte ein Verleih notwendig sein, sollte dies nur geschehen, wenn man alle sensiblen Daten (bspw. weil sich diese nur auf einer Speicherkarte befinden) und die SIM-Karte vor dem Verleih entnimmt. Außerdem sollte ein Verleih nur an absolut vertrauenswürdige Personen erfolgen.	VT, IN, VF, AU, AN	Vgl. [BSI08a, 115]
OM 12	**Mobile Endgeräte vor dem Zurücklassen absichern:** Muss ein mobiles Endgerät beispielsweise beim Betreten eines fremden Unternehmens abgegeben werden, so sind Speicherkarten und die SIM-Karte zu entnehmen. Außerdem ist das Gerät auszuschalten und eventuell der Akku zu entnehmen.	VT, IN, VF, AU, AN	
OM 13	**Verlorener SIM-Karten melden und umgehend sperren:** Die SIM-Karte ist eine digitale (vertrauenswürdige) Identität des Anwenders gegenüber dem Mobilfunknetz und ggf. gegenüber dem dazugehörigen Unternehmen. Da es möglich ist, SIM-Karten zu klonen (SIM-Cloning, definitiv nachgewiesen für SIM-Karten, die vor 2001 hergestellt wurden), ist auch ein Wiederauffinden einer verloren gegangenen SIM-Karte kein Garant dafür, dass keine Manipulation stattgefunden hat. Der Verlust eines Endgerätes und der damit verbundene Verlust der SIM-Karte ist unverzüglich dem Mobilfunkprovider mitzuteilen, um die SIM-Karte sperren zu lassen.	AU, VB	Vgl. [BSI08a, 26]
OM 14	**Passwörter mit hoher Passwortkomplexität wählen und prüfen:** Passwörter sollten so komplex wie möglich gestaltet werden (Großbuchstaben, Kleinbuchstaben und Sonderzeichen). Auch sollten Passwörter aus so vielen Stellen wie möglich bestehen, (wobei die Praxistauglichkeit nicht außer Acht gelassen werden sollte). Wenn es technisch möglich ist, sollten bei den vom Nutzer zu wählenden Passwörtern mittels Sicherheitsrichtlinien einfache Passwörter (z. B. 1234, AAAA) gar nicht erst akzeptiert werden. Das BlackBerry-Betriebssystem beinhaltet bereits einen Mechanismus, der bei selbst zu wählenden Passwörtern schwache Passwörter ablehnt. In regelmäßigen Abständen ist außerdem zu prüfen, ob die Benutzerpasswörter leicht zu erraten sind. (Dies gilt für die vom Nutzer zu vergebenden oder zu ändernden Passwörter.)	AU	Vgl. [BSI06, 28]
OM 15	**Regelmäßiges Wechseln von Passwörtern:** In regelmäßigen Abständen sollte der Nutzer dazu veranlasst werden, sein Passwort zu ändern.	VT, IN, VB	
OM 16	**Passwörter und SmartCards sicher aufbewahren:** Passwörter sollten niemals notiert werden, oder über unsichere Kommunikationswege unverschlüsselt übertragen werden. Werden Passwörter eingegeben, so ist dies unter Sichtschutz durchzuführen. Werden SmartCards für die Authentisierung verwendet, so sind diese immer getrennt vom mobilen Endgerät aufzubewahren, falls das mobile Endgerät aus den Händen gegeben werden muss.	AU	
OM 17	**Eingabe von Zugangsdaten an untypischen Stellen unterlassen:** Wird der Nutzer dazu aufgefordert, seine Zugangsdaten an anderer Stelle einzugeben als es die Zugangsdaten sonst erfordern, so sollte er diese generell ignorieren. Trifft eine solche Aufforderung aus einer scheinbar vertrauenswürdigen Quelle ein, so ist vom Nutzer die Authentizität der Quelle z. B. mittels eines Kontrollanrufes zu überprüfen und bei Bedarf über einen sicheren (alternativen) Kanal (z. B. ein entsprechend gesichertes Unternehmens-Webportal) zu übermitteln.	AU, AN	Vgl. [BSI08a, 86]
OM 18	**Nachrichten (SMS/MMS/E-Mail) nur von vertrauenswürdigen Absendern annehmen:** Der Nutzer sollte ausschließlich von absolut vertrauenswürdigen Absendern erhaltene Nachrichten abspeichern bzw. öffnen und somit deren Inhalte ausführen. Außerdem muss die Vertrauenswürdigkeit des Dienstanbieters gegeben sein, da ein Innentäter durchaus die Möglichkeit hätte, Schadsoftware zu übermitteln. Da ein Restrisiko grundsätzlich gegeben ist, empfiehlt sich bspw. gemäß Maßnahme TM 6 die Deaktivierung des MMS-Empfangs.	VT, IN, VF, AN	Vgl. [BSI08a, 127]
OM 19	**Verschlüsselung von Daten auf dem mobilen Endgerät anordnen (org):** Die vom Nutzer auf dem mobilen Endgerät abgelegten Daten (z. B. Dokumente, E-Mails, Passwörter etc.) sollten sowohl auf dem internen als auch auf dem externen Speicher nur stark verschlüsselt abgelegt werden. Der Nutzer sollte für die Notwendigkeit der eventuell zeitaufwendigeren Ablage von Daten mittels Verschlüsselung sensibilisiert werden. Sollte zur Ver- bzw. Entschlüsselung nicht nur ein Passwort, sondern auch ein Security-Token oder RSA-Schlüssel (z. B. auf einer SmartCard) verwendet werden, so ist dieser getrennt vom Endgerät aufzubewahren.	VT, VB	Vgl. [BSI06, 27, 29]
OM 20	**Nutzung von Speicherkarten unterlassen bzw. einschränken:** Speicherkarten lassen sich oft einfacher entwenden als das ganze mobile Endgerät. Daher kann ein kompletter Verzicht auf Speicherkarten eine Lösung sein. Ist ein Verzicht auf Speicherkarten nicht möglich, empfiehlt es sich darauf zu verzichten sensible Daten auf Speicherkarten abzuspeichern. (Diese Maßnahme steht im Widerspruch zur Maßnahme OM 26. Es ist also abzuwägen, welche Maßnahme anzuwenden ist.)	VT, AN	Vgl. [BSI08a, 116]
OM 21	**Speicherkarten als Datenspeicher für sensible Daten nutzen:** Ist es technisch möglich und lässt es die Anwendungssoftware zu, so sollten sensible Daten auf entfernbaren Speicherkarten abgelegt werden. Muss das Gerät beispielsweise beim Betreten eines fremden Unternehmens abgegeben werden, so können zumindest die sensiblen Daten aus dem Gerät entfernt werden. (Diese Maßnahme steht im Widerspruch zur Maßnahme OM 25. Es ist daher abzuwägen, welche Maßnahme anzuwenden ist.)	VT, IN, AN	Vgl. [BSI06, 30]
OM 22	**Prepaid-Karten zur Anonymisierung nutzen**: Ein Kartentausch, der Erwerb von bereits registrierten SIM-Karten oder der Erwerb von Prepaid-SIM-Karten ohne Ausweisprüfung kann zur Vermeidung der Identifikation beim Mobilfunkbetreiber genutzt werden. Diese Maßnahme verschleiert die Identität eines Mobilfunkteilnehmers wirksam.	VT, AN	Vgl. [BSI08a, 27]

OM 23	**SIM-Karten und Endgeräte regelmäßig wechseln:** Um es Angreifern zu erschweren, ein ganz bestimmtes mobiles Endgerät abzuhören bzw. Datenübertragungen abzufangen, zu verändern oder aufzuzeichnen, empfiehlt sich ein häufiger Wechsel von mobilem Endgerät und SIM-Karte. Dies erschwert die Identifikation des Endgerätes bzw. des Nutzers anhand der IMSI-Nummer und der IMEI-Nummer. Das häufige Wechseln der SIM-Karte geht jedoch mit einer ständig wechselnden Telefonnummer einher, was nicht immer praktikabel ist.	VT, AN	Vgl. [BSI08a, 25]
OM 24	**Verwendung von komplexen Bluetooth-PIN anordnen/vereinbaren:** Die für den Bluetooth-Verbindungsaufbau erforderliche PIN muss so komplex wie möglich gewählt werden. Je nach Geräteherstelle r können dabei nicht nur Zahlen gewählt werden. Daher müssen, wenn möglich, bei der Bluetooth-PIN-Erstellung Zahlen, Großbuchstaben, Kleinbuchstaben und Sonderzeichen genutzt werden.	AU, VB	Vgl. [BSI08a, 119]
OM 25	**Geeignete mobile Endgeräte auswählen:** Beim Auswahlprozess für mobile Endgeräte müssen sowohl die funktionalen Anforderungen der Benutzer beachtet werden, als auch dass sich das mobile Endgerät in die bestehende Unternehmenspolicy ohne umfangreiche Änderungen einbinden lässt. Die Sicherheitsmechanismen des mobilen Endgerätes, sowie das Betriebssystem müssen bei der erforderlichen Anwendungssoftware entsprechende Sicherheit bieten. Die Hersteller und Lieferanten der mobilen Endgeräte müssen vertrauenswürdig sein. Auch den Mobilfunkprovidern muss vertraut werden können, da sie häufig zusätzliche Software auf das Gerät aufbringen.	IN, VF	Vgl. [BSI06, 26]
OM 26	**Endgerätevielfalt beschränken:** Eingesetzte Varianten von mobilen Endgeräten sollten auf ein notwendiges Minimum reduziert werden. So ist es möglich, ohne jede weitere Maßnahme die Zahl der Sicherheitsrisiken zu begrenzen.	IN, VF	
OM 27	**Sicherheitszertifizierungen einfordern:** Vor der Auswahl einer bestimmten Anwendungssoftware sollten vom Hersteller entsprechende Sicherheitszertifizierungen eingeholt werden. Auch entsprechende Studien können eine korrekte Implementierung belegen. Ist beides nicht verfügbar, sollte alternative Anwendungssoftware geprüft werden. Ist alternative Anwendungssoftware nicht verfügbar, sollten bekannte Sicherheitsmängel evaluiert werden und eventuell von einem Einsatz der Anwendungssoftware ganz abgesehen werden.	VT, IN, VF	Vgl. [BSI08a, 125]
OM 28	**Anwendungssoftwarevielfalt beschränken:** Eingesetzte Anwendungssoftware sollten auf ein notwendiges Minimum reduziert werden. So ist es möglich, ohne jede weitere Maßnahme die Zahl der Sicherheitsrisiken zu begrenzen.	VT, IN, VF	Vgl. [BSI08a, 126]
OM 29	**Anwendungssoftware ausschließlich aus vertrauenswürdigen Quellen installieren:** Anwendungssoftware, -updates und Firmware-/Betriebssystem-Updates dürfen nur aus absolut vertrauenswürdigen Quellen bezogen werden, da sonst das Risiko besteht, manipulierte Software einzuspielen. Dennoch bleibt ein gewisses Restrisiko, da auch der Hersteller versteckte Schnittstellen etc. eingebaut haben könnte (z. B. aus Gründen der Zusammenarbeit mit Behörden). Darüber hinaus sollte in Erwägung gezogen werden, dass ausschließlich der für mobile Endgeräte zuständige Administrator Anwendungssoftware installieren darf.	IN, VF	
OM 30	**Untersuchung auf Hardwaremanipulation regelmäßig durchführen:** Auch bei nicht als gestohlen gemeldeten mobilen Endgeräten sollte eine regelmäßige Kontrolle auf Hardwaremanipulationen durchgeführt werden, da ein mobiles Endgerät dem Nutzer auch unbemerkt entwendet und wieder untergeschoben werden kann. Hier kann die Hardware mittels Röntgenprüfgeräten berührungsfrei auf Manipulationen untersucht werden.	IN, VF	Vgl. [BSI08a, 116]
OM 31	**Verlust/Wiederauffinden von Geräte melden:** Ist es zum Verlust eines mobilen Endgerätes gekommen, muss dies umgehend einem Administrator gemeldet werden. Um eventuellen Missbrauch durch die auf dem mobilen Endgerät gespeicherten Passwörter bzw. Zugangsdaten zu verhindern, müssen sofort nach der Verlustmeldung die Zugangsberechtigungen entzogen werden und eventuell vorhandene Löschdienste (Löschbefehle über ein Mobilfunknetz) ausgelöst werden. Wurde ein verlorenes Endgerät wiedergefunden, so bedeutet dies den Verlust der Vertraulichkeit, der Anonymität und der Integrität der auf dem Gerät gespeicherten Daten. Insbesondere kann einem wiedergefundenen Gerät nicht mehr vertraut werden, da die Gefahr besteht, dass es manipuliert wurde. Das Gerät muss vor der ersten Wiederverwendung durch einen Techniker auf Manipulationen jeglicher Art untersucht werden. Vor der ersten Wiederverwendung ist eine umfassende Bereinigung des Gerätes vorzunehmen, um es wieder in den Auslieferungszustand zurückzuversetzen. Erst danach darf es wieder an einen Nutzer ausgegeben werden.	VT, IN, VB, AU, AN	Vgl. [BSI06, 28]
OM 32	**Konfiguration der Endgeräte regelmäßig kontrollieren (org.):** Um die Bedrohungen durch OTA-Provisioning und ähnlichen Techniken zu minimieren, sollte die Konfiguration, besonders die Konfiguration von (Internet-) Zugangsprofilen regelmäßig kontrolliert werden. Ist eine Kontrolle über Fernwartungssysteme nicht möglich, so muss diese Aufgabe der Nutzer in regelmäßigen Abständen durchführen.	VF, VB	
OM 33	**Benutzungsspuren entfernen:** Benutzungsspuren (z. B. Kratzer auf dem Display), die auf dem mobilen Endgerät durch häufige PIN- oder Passworteingaben entstehen, sollten vermieden werden oder müssen regelmäßig entfernt werden.	VT, AU, AN	Vgl. [BSI06, 28] Verwendung von Displayschutzfolien, die regelmäßig gewechselt werden

Tab. 5-2: Sicherheitsmaßnahmenkatalog

A.4 Kreuzreferenztabellen

Legende:

OM Organisatorische Maßnahme, TM Technische Maßnahme

Bedrohungen	Technische Sicherheitsmaßnahmen																																						
	TM 1	TM 2	TM 3	TM 4	TM 5	TM 6	TM 7	TM 8	TM 9	TM 10	TM 11	TM 12	TM 13	TM 14	TM 15	TM 16	TM 17	TM 18	TM 19	TM 20	TM 21	TM 22	TM 23	TM 24	TM 25	TM 26	TM 27	TM 28	TM 29	TM 30	TM 31	TM 32	TM 33	TM 34	TM 35	TM 36	TM 37
1																																					
2																																					
3																																					
4																																					
5																																					
6																																					
7																																					
8																																					
9																																					
10																																					
11																																					
12																																					
13	X																																				
14																																					
15	X																																				
16																																					
17	X																																				
18																																					
19																																					
20																																					
21		X	X	X							X															X												
22		X	X	X							X															X												
23		X	X	X							X															X												
24		X	X	X							X															X												
25	X	X	X	X							X															X												
26		X	X	X							X															X												
27																																					
28																																					
29																																					
30																																					
31																																					
32																																					
33																																					
34	X																																				
35																																					
36							X										X	X	X	X	X	X	X			X								X				
37							X										X	X	X	X	X	X	X			X								X				
38							X										X	X	X	X	X	X	X			X								X				
39							X										X	X	X	X	X	X	X			X								X				

	40																																								
	41																							X	X	X														X			
	42																																								
	43																																								
	44																																								
	45																																								
	46																																								
	47	X				X																																		
	48																																								
	49																																								
	50																																								
	51	X				X																																		
	52																																								
	53																																								
	54																																								
	55	X				X																																		
	56																																								
	57																																								
	58																																								
	59																																								
	60																																								
	61		X	X	X							X															X													
	62	X	X	X	X	X						X															X													
	63		X	X	X							X															X													
	64																																								
	65																																								
	66																																								
	67																																								
	68																																								
	69																																								
	70																																								
	71																							X	X	X													X			
	72							X										X	X	X	X	X	X	X			X												X			
	73							X										X	X	X	X	X	X	X			X												X			
	74							X										X	X	X	X	X	X	X			X												X			
	75							X										X	X	X	X	X	X	X			X												X			
	76	X				X																																			
	77																																								
	78																																								
	79																																								
	80																																								
	81																																								
	82			X																																				
	83																																								
	84																																								
	85			X																																				
	86						X									X																								
	87																																								
	88						X			X																										X				
	89						X			X																										X				
	90						X	X								X		X	X	X	X		X	X													X			

91						X	X								X		X	X	X	X		X	X											X			
92						X			X																							X							
93																																								
94																																							
95						X	X								X		X	X	X	X		X	X											X			
96		X									X															X												
97																																							
98																																							
99																										X												
100							X	X							X		X	X	X	X	X	X	X											X			
101							X																															
102																																				X	X	
103																																				X	X	
104																																				X	X	
105																																				X	X	
106							X		X																	X					X						
107							X																															
108							X										X	X	X	X	X	X	X			X								X			
109							X										X	X	X	X	X	X	X			X								X			
110							X										X	X	X	X	X	X	X			X								X			
111							X										X	X	X	X	X	X	X			X								X			
112																																							
113		X									X																											
114																																				X	X	
115																																				X	X	
116																																							
117																																				X	X	
118																																				X	X	
119																																							
120																					X	X	X																
121																																				X	X	
122																																				X	X	
123																																							
124																																							
125																																							
126																																							
127																																							
128																																							
129										X																				X							
130										X																				X							
131												X																		X							
132												X																		X							
133																					X																
134																					X																
135																																							
136																									X	X												
137										X		X																		X							
138															X		X	X	X	X	X	X	X		X	X			X					X			
139																																							
140													X										X			X								X			
141																																							

142																																							
143																																							
144																																							
145																																							
146																																							
147													X									X	X	X												X				
148																																							
149																																							
150																																							
151																																							
152		X								X	X											X	X	X							X				X				
153												X										X	X	X							X				X				
154													X									X	X	X												X				
155		X		X							X											X																	
156		X	X	X							X		X																										
157		X																																					
158																																							
159																									X	X	X			X				X					
160																									X	X	X			X				X					
161																									X	X	X			X				X					
162										X												X		X							X				X				
163										X												X	X	X							X				X				
164													X									X	X	X												X				
165																						X	X	X												X				
166													X									X	X	X												X				
167																						X	X	X												X				
168																										X	X												
169																																							
170																																						X			
171													X	X	X	X							X			X	X	X	X	X			X						
172														X														X	X										
173														X														X	X										
174													X										X	X		X	X			X			X		X				
175													X		X																								
176																																							
177													X										X	X		X	X			X			X		X				
178																																							
179																																							
180													X													X				X								
181													X		X					X			X	X		X	X			X					X				
182													X											X	X		X			X									
183													X													X	X	X	X	X									
184																																							
185																																							
186													X														X												
187																																							
188																																							
189																																							
190																																							
191													X		X												X			X						X	X		
192																																							

	193						X			X																					X							
	194						X			X																					X							
	195										X														X			X								X			
	196												X												X	X	X									X			
	197															X								X		X	X									X	X			
	198																																							
	199																																							
	200																																							
	201																																							
	202																																							
	203																																							
	204																																							
	205																																							
	206																																							
	207																																							
	208																																							
	209																																							
	210																																							
	211																																							
	212																																							
	213																											X												
	214																																							
	215																																							
	216																																							
	217																																							
	218																												X	X										X
	219																												X	x										X
	220																												X	X										X
	221																												X	X										X

Tab. 5-3: Kreuzreferenztabelle (Technische Sicherheitsmaßnahmen)

Legende:

OM Organisatorische Maßnahme, TM Technische Maßnahme

		Organisatorische Sicherheitsmaßnahmen																																		
		OM 1	OM 2	OM 3	OM 4	OM 5	OM 6	OM 7	OM 8	OM 9	OM 10	OM 11	OM 12	OM 13	OM 14	OM 15	OM 16	OM 17	OM 18	OM 19	OM 20	OM 21	OM 22	OM 23	OM 24	OM 25	OM 26	OM 27	OM 28	OM 29	OM 30	OM 31	OM 32	OM 33
Bedrohungen	1	X	X																															
	2	X	X																															
	3	X	X																															
	4	X	X																															
	5	X	X																															
	6	X	X																															
	7	X	X																															
	8																																	
	9																																	
	10																																	
	11																																	
	12																						X	X										
	13																																	
	14																						X	X										
	15																																	
	16																						X	X										
	17																																	
	18																						X	X										
	19																						X	X										
	20																						X	X										
	21				X	X	X																											
	22				X	X	X																											
	23				X	X	X																											
	24				X	X	X																											
	25				X	X	X																											
	26				X	X	X																											
	27																																	
	28																																	
	29																																	
	30																																	
	31																																	
	32																						X	X										
	33																						X	X										
	34																						X	X										
	35																																	
	36			X	X	X	X											X				X		X										
	37			X	X	X	X											X				X		X										
	38			X	X	X	X											X				X		X										
	39			X	X	X	X											X				X		X										
	40																																	
	41				X	X	X																											
	42																																	
	43																																	

44																																			
45																																			
46																							X	X											
47																																			
48																							X	X											
49																							X	X											
50																							X	X											
51																																			
52																							X	X											
53																							X	X											
54																							X	X											
55																																			
56																							X	X											
57																							X	X											
58																							X	X											
59																							X	X											
60																							X	X											
61				X	X	X																													
62				X	X	X																													
63				X	X	X																													
64																																			
65																																			
66																																			
67																																			
68																																			
69																							X	X											
70																																			
71				X	X	X																													
72			X	X	X	X												X				X		X											
73			X	X	X	X												X				X		X											
74			X	X	X	X												X				X		X											
75			X	X	X	X												X				X		X											
76																							X	X											
77																																			
78																																			
79																																			
80																																			
81																																			
82				X	X	X																													
83																																			
84																																			
85				X	X	X																													
86																				X													X		
87																																			
88			X																	X															
89			X																	X															
90			X	X	X	X													X													X			
91			X	X	X	X													X													X			
92			X																	X															
93																																			
94																																			

95			X	X	X	X												X											X					
96				X	X	X																												
97																																		
98																																		
99																																		
100			X	X	X	X											X	X			X								X					
101																																	X	
102																																		
103																																		
104																																		
105																																		
106																		X															X	
107																																		
108			X	X	X	X											X				X		X											
109			X	X	X	X											X				X		X											
110			X	X	X	X											X				X		X											
111			X	X	X	X											X				X		X											
112																																		
113																																		
114																																		
115																																		
116																																		
117																																		
118																																		
119																																		
120				X	X	X																												
121																																		
122																																		
123																																		
124																																		
125																																		
126																																		
127																																		
128																							X	X										
129				X		X																												
130				X		X																												
131				X		X																												
132				X		X																												
133				X		X																												
134				X		X																												
135																																		
136									X	X	X	X	X																		X			
137																							X	X										
138			X	X	X	X			X	X	X	X		X						X													
139							X	X																										
140							X	X						X	X	X	X	X	X	X														
141														X	X	X																		
142							X	X																										
143								X						X																				
144														X	X	X																		
145														X	X	X																		

146														X	X	X																		
147				X	X	X														X	X	X	X						X					
148																																		
149																				X														
150																																		
151																																		
152				X	X	X																												
153				X	X	X													X															
154				X	X	X																								X				
155				X	X	X																												
156				X	X	X																												
157				X	X	X													X															
158																																		
159				X	X	X	X							X		X				X												X		
160				X	X	X	X							X		X				X												X		
161				X	X	X	X							X		X				X												X		
162				X	X	X																												
163				X	X	X													X															
164				X	X	X																								X				
165				X	X	X																												
166				X	X	X														X		X	X						X					
167				X	X	X																												
168									X	X	X	X	X																		X			
169																																		
170				X																											X			
171				X	X	X								X		X			X	X														
172																															X	X		
173																															X	X		
174	X			X	X	X								X						X														
175				X	X		X												X															
176																																		
177	X			X	X	X								X				X	X				X										
178																																		
179																																		
180				X	X	X								X					X	X														
181				X	X	X								X					X	X														
182				X	X	X	X	X						X	X	X		X	X	X														
183				X	X	X		X	X	X	X	X		X		X			X															
184																																		
185																																		
186																			X															
187																																		
188																																		
189																																		
190																																		
191				X	X	X													X															
192																																		
193																			X															
194																			X															
195				X	X	X																									X			
196				X	X	X													X												X			

197				X	X	X																	X						X				
198						X				X																							
199						X				X																							
200				X		X																									X		
201																																	
202				X	X	X								X				X															
203				X	X	X	X	X									X																
204				X		X	X																										
205																																	
206				X		X	X																										
207				X		X	X																										
208				X		X	X																										
209				X		X	X																										
210																																	
211				X		X	X																										
212				X		X	X																										
213				X		X	X																										
214				X	X	X																											
215																																	
216				X	X	X																											
217				X	X	X																											
218				X					X		X	X	X									X									X		
219				X					X		X	X	X									X									X		
220				X					X		X	X	X									X									X		
221				X					X		X	X	X									X									X		

Tab. 5-4: Kreuzreferenztabelle (Organisatorische Sicherheitsmaßnahmen)