DSGVo: Handling von Mobiltelefonen – Smartphones – Tablets – PDAs anhand der IT-Grundschutzkataloge des BSI

Dieses Paper ist eine Zusammenfassung aller Datenschutz- und Informationssicherheitsthemen zu Mobiltelefonen, Smartphones, Tablets und PDAs.

Es basiert auf den zutreffenden Bausteinkatalogen, den Gefährungskatalogen und den Maßnahmenkatalogen aus dem Dokument „IT-Grundschutz-Kataloge“ in der Version 15. Ergänzungslieferung – 2016 (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/download/download.html bzw. https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf).

Inhalt

Bausteinkataloge

B 3.404 Mobiltelefon
B 3.405 Smartphones, Tablets und PDAs
B 4.8 Bluetooth
B 5.14 Mobile Datenträger

Gefährdungskataloge

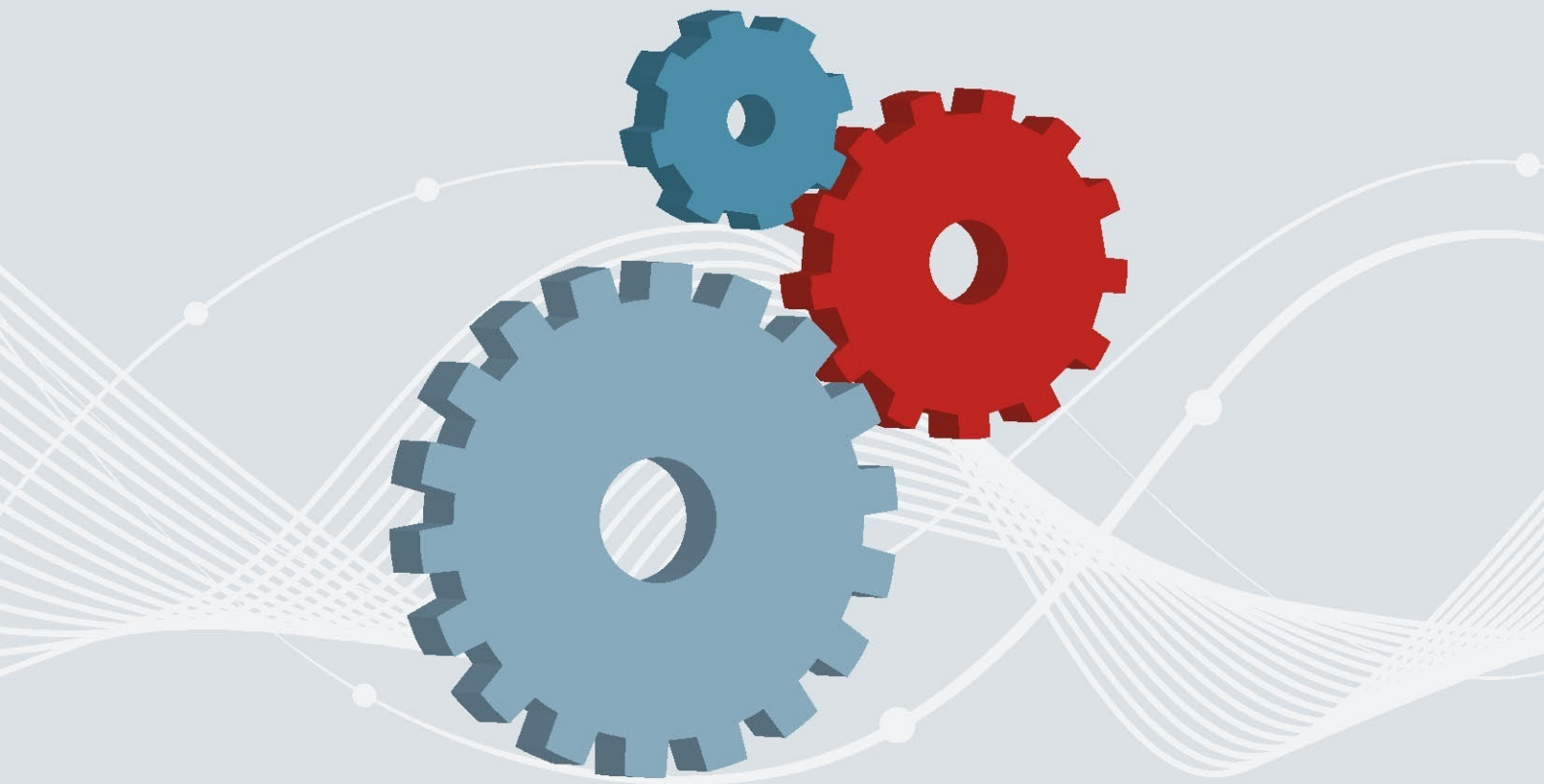
G 0.19 Offenlegung schützenswerter Informationen
G 0.45 Datenverlust
G 1.15 Beeinträchtigung durch wechselnde Einsatzumgebung
G 2.2 Unzureichende Kenntnis über Regelungen
G 2.4 Unzureichende Kontrolle der Sicherheitsmaßnahmen
G 2.139 Mangelhafte Berücksichtigung von mobilen Endgeräten beim Patch- und Änderungsmanagement
G 2.200 Unzureichende Planung bei der Anschaffung von Mobiltelefonen, Smartphones, Tablets oder PDAs
G 3.1 Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten
G 3.3 Nichtbeachtung von Sicherheitsmaßnahmen
G 3.44 Sorglosigkeit im Umgang mit Informationen
G 3.76 Fehler bei der Synchronisation mobiler Endgeräte
G 3.77 Mangelhafte Akzeptanz von Informationssicherheit
G 3.106 Ungeeignetes Verhalten bei der Internet-Nutzung
G 3.123 Unerlaubte private Nutzung des dienstlichen Mobiltelefons, Smartphones, Tablets oder PDAs
G 4.42 Ausfall des Mobiltelefons, Smartphones, Tablets oder PDAs
G 4.51 Unzureichende Sicherheitsmechanismen bei Smartphones, Tablets oder PDAs
G 4.52 Datenverlust bei mobilem Einsatz
G 4.79 Schwachstellen in der Bluetooth-Implementierung
G 4.84 Unzureichende Validierung von Ein- und Ausgabedaten bei Webanwendungen und Web-Services
G 5.2 Manipulation an Informationen oder Software
G 5.4 Diebstahl
G 5.13 Abhören von Räumen über TK-Endgeräte
G 5.94 Missbrauch von SIM-Karten
G 5.95 Abhören von Raumgesprächen über Mobiltelefone
G 5.96 Manipulation von Mobiltelefonen
G 5.97 Unberechtigte Datenweitergabe über Mobiltelefone
G 5.99 Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefonen
G 5.123 Abhören von Raumgesprächen über mobile Endgeräte
G 5.124 Missbrauch der Informationen von mobilen Endgeräten
G 5.125 Datendiebstahl mithilfe mobiler Endgeräte
G 5.126 Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten
G 5.141 Datendiebstahl über mobile Datenträger
G 5.160 Missbrauch der Bluetooth-Profile

G 5.177 Missbrauch von Kurz-URLs oder QR-Codes
G 5.193 Unzureichender Schutz vor Schadprogrammen auf Smartphones, Tablets und PDAs
G 5.194 Einschleusen von GSM-Codes in Endgeräte mit Telefonfunktion

Maßnahmenkataloge

M 1.33 Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
M 1.34 Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz
M 2.9 Nutzungsverbot nicht freigegebener Hard- und Software
M 2.163 Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte
M 2.188 Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
M 2.189 Sperrung des Mobiltelefons bei Verlust
M 2.207 Sicherheitskonzeption für Lotus Notes/Domino
M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten
M 2.303 Festlegung einer Strategie für den Einsatz von Smartphones, Tablets oder PDAs
M 2.304 Sicherheitsrichtlinien und Regelungen für die Nutzung von Smartphones, Tablets und PDAs
M 2.305 Geeignete Auswahl von Smartphones, Tablets oder PDAs
M 2.306 Verlustmeldung
M 2.312 Konzeption eines Schulungs- und Sensibilisierungsprogramms zur Informationssicherheit
M 2.390 Außerbetriebnahme von WLAN-Komponenten
M 2.430 Sicherheitsrichtlinien und Regelungen für den Informationsschutz unterwegs
M 2.442 Einsatz von Client-Betriebssytemen ab Windows Vista auf mobilen Systemen
M 2.461 Planung des sicheren Bluetooth-Einsatzes
M 2.558 Sensibilisierung der Mitarbeiter zur Informationssicherheit bei Mobiltelefonen, Smartphones, Tablets und PDAs
M 3.87 Einführung in Lotus Notes/Domino
M 4.3 Einsatz von Viren-Schutzprogrammen
M 4.114 Nutzung der Sicherheitsmechanismen von Mobiltelefonen
M 4.128 Sicherer Betrieb der Lotus Notes/Domino-Umgebung
M 4.228 Nutzung der Sicherheitsmechanismen von Smartphones, Tablets und PDAs
M 4.229 Sicherer Betrieb von Smartphones, Tablets und PDAs
M 4.230 Zentrale Administration von Smartphones, Tablets und PDAs
M 4.231 Einsatz zusätzlicher Sicherheitswerkzeuge für Smartphones, Tablets oder PDAs
M 4.234 Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern
M 4.323 Synchronisierung innerhalb des Patch- und Änderungsmanagements
M 4.465 Aussonderung von Mobiltelefonen, Smartphones, Tablets und PDAs
M 4.466 Einsatz von Viren-Schutzprogrammen bei Smartphones, Tablets und PDAs
M 4.467 Auswahl von Applikationen für Smartphones, Tablets und PDAs
M 4.468 Trennung von privatem und dienstlichem Bereich auf Smartphones, Tablets und PDAs
M 4.469 Abwehr von eingeschleusten GSM-Codes auf Endgeräten mit Telefonfunktion
M 4.484 Speicherschutz bei eingebetteten Systemen
M 5.78 Schutz vor Erstellen von Bewegungsprofilen bei der Mobiltelefon-Nutzung
M 5.79 Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung
M 5.80 Schutz vor Abhören der Raumgespräche über Mobiltelefone
M 5.81 Sichere Datenübertragung über Mobiltelefone
M 5.121 Sichere Kommunikation von unterwegs
M 5.173 Nutzung von Kurz-URLs und QR-Codes
M 5.176 Sichere Anbindung von Smartphones, Tablets und PDAs an das Netz der Institution
M 6.72 Ausfallvorsorge bei Mobiltelefonen
M 6.95 Ausfallvorsorge und Datensicherung bei Smartphones, Tablets und PDAs
M 6.159 Vorsorge vor Verlust und Diebstahl von Smartphones, Tablets und PDAs

Bundesamt
für Sicherheit in der
Informationstechnik



IT-Grundschutz-Kataloge

15. Ergänzungslieferung - 2016

B 3.404 Mobiltelefon

Beschreibung

In diesem Baustein werden digitale Mobiltelefone nach dem GSM-Standard (Global System for Mobile communication, D- und E-Netze), UMTS (Universal Mobile Telecommunications System) und LTE (Long Term Evolution) betrachtet. Bei LTE werden Telefonate über Datenpakete abgewickelt, sodass dann zusätzlich Baustein B 4.7 *VoIP* zu betrachten ist. Handelt es sich beim Mobiltelefon um ein Smartphone, ist auch Baustein B 3.405 *Smartphones, Tablets und PDAs* und gegebenenfalls Baustein B 3.203 *Laptop* umzusetzen. Verwendet das Mobiltelefon VPN-Techniken, um sich beispielsweise mit dem Netz der Institution zu verbinden, sollte außerdem Baustein B 4.4 *VPN* betrachtet werden.

Um ein Mobiltelefon mit einem Mobilfunknetz zu verbinden, braucht es eine SIM-Karte (SIM - Subscriber Identity Module). Damit kann in den Mobilfunknetzen zwischen Benutzer und Gerät unterschieden werden.

Ein Mobiltelefon ist durch seine international eindeutige Seriennummer (IMEI - International Mobile Equipment Identity) gekennzeichnet. Der Benutzer wird durch seine auf der SIM-Karte gespeicherte Kundennummer (IMSI - International Mobile Subscriber Identity) identifiziert. Sie wird dem Teilnehmer beim Vertragsabschluss vom Mobilfunkanbieter zugeteilt. Sie ist zu unterscheiden von den ihm zugewiesenen Telefonnummern (MSISDN) (mindestens eine) . Durch diese Trennung ist es möglich, dass ein Teilnehmer mit seiner SIM-Karte verschiedene Mobiltelefone nutzen kann

Auf der SIM-Karte wird unter anderem die teilnehmerbezogene Rufnummer (MSISDN) gespeichert. Ebenso sind dort die kryptografischen Algorithmen für die Authentisierung und Nutzdatenverschlüsselung (zwischen Mobiltelefon und Basisstation) implementiert.

Gefährdungslage

Für den IT-Grundschutz werden im Zusammenhang mit Mobiltelefonen folgende typische Gefährdungen angenommen:

Organisatorische Mängel

- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.200 *Unzureichende Planung bei der Anschaffung von Mobiltelefonen, Smartphones, Tablets oder PDAs*

Menschliche Fehlhandlungen

- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.43 *Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen*
- G 3.44 *Sorglosigkeit im Umgang mit Informationen*
- G 3.45 *Unzureichende Identifikationsprüfung von Kommunikationspartnern*
- G 3.77 *Mangelhafte Akzeptanz von Informationssicherheit*
- G 3.123 *Unerlaubte private Nutzung des dienstlichen Mobiltelefons, Smartphones, Tablets oder PDAs*

Technisches Versagen

- G 4.32 *Nichtzustellung einer Nachricht*
- G 4.41 *Nicht-Verfügbarkeit des Mobilfunknetzes*
- G 4.42 *Ausfall des Mobiltelefons, Smartphones, Tablets oder PDAs*

Vorsätzliche Handlungen

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.4 *Diebstahl*

- G 5.27 *Nichtanerkennung einer Nachricht*
- G 5.94 *Missbrauch von SIM-Karten*
- G 5.95 *Abhören von Raumgesprächen über Mobiltelefone*
- G 5.96 *Manipulation von Mobiltelefonen*
- G 5.97 *Unberechtigte Datenweitergabe über Mobiltelefone*
- G 5.98 *Abhören von Mobiltelefonaten*
- G 5.99 *Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefonen*
- G 5.126 *Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten*
- G 5.192 *Vortäuschen falscher Anrufer-Telefonnummern oder SMS-Absender*

Maßnahmenempfehlungen

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz. Für Mobiltelefone sind eine Reihe von Maßnahmen erforderlich, beginnend mit der Planung über den Betrieb bis zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Es sollte eine Sicherheitsrichtlinie erstellt werden, die umzusetzende Maßnahmen zum sicheren Umgang mit Mobiltelefonen beschreibt (siehe M 2.188 *Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung*). Bei häufigem und wechselndem dienstlichen Gebrauch von Mobiltelefonen, die vom Unternehmen oder der Behörde zur Verfügung gestellt werden, kann es sinnvoll sein, diese Telefone in einer Sammelaufbewahrung zu halten (siehe M 2.190 *Einrichtung eines Mobiltelefon-Pools*).

Umsetzung

Es gibt verschiedene Sicherheitsmechanismen bei Mobiltelefonen, abhängig vom eingesetzten Mobiltelefon, von der SIM-Karte und vom gewählten Netzbetreiber. M 4.114 *Nutzung der Sicherheitsmechanismen von Mobiltelefonen* gibt einen Überblick über die wichtigsten Sicherheitsfunktionen dieser Geräte und beschreibt, wie diese genutzt werden könnten.

Betrieb

Damit Mobiltelefone geordnet und zuverlässig genutzt werden können, müssen einige Maßnahmen umgesetzt werden, zu denen die Sicherstellung der Energieversorgung und bei Bedarf auch der Schutz vor Rufnummernermittlung gehören (siehe M 4.115 *Sicherstellung der Energieversorgung von Mobiltelefonen* und M 5.79 *Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung*) Falls mit dem Gerät Daten übertragen werden, sind ebenfalls einige spezifische Maßnahmen zu beachten, um einerseits eine zuverlässige Funktionsweise zu gewährleisten und andererseits gegen Missbrauch geschützt zu sein (siehe M 5.81 *Sichere Datenübertragung über Mobiltelefone*). Wird das Telefon verloren, sollte die SIM-Karte dieses Telefons unverzüglich gesperrt werden, um Missbrauch und unnötige Kosten zu verhindern (siehe M 2.189 *Sperrung des Mobiltelefons bei Verlust*). Für die speziellen Gefährdungen der Informationssicherheit durch Mobiltelefone müssen die betreffenden Mitarbeiter besonders sensibilisiert werden (siehe M 2.558 *Sensibilisierung der Mitarbeiter zur Informationssicherheit bei Mobiltelefonen, Smartphones, Tablets und PDAs*).

Aussonderung

Da sich auf Mobiltelefonen in der Regel vertrauliche Daten befinden, muss geregelt werden, wie die Geräte auszusondern sind. In Maßnahme M 4.465 *Aussonderung von Mobiltelefonen, Smartphones, Tablets und PDAs* werden Empfehlungen gegeben. Falls die Geräte herausnehmbare Speicherkarten besitzen, ist für diese Karten Maßnahme M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln* anzuwenden, die beschreibt, wie die herausnehmbaren Speicherkarten entsorgt werden.

Notfallvorsorge

In der Maßnahme M 6.72 *Ausfallvorsorge bei Mobiltelefonen* werden wichtige Vorkehrungen beschrieben, durch die sich der Benutzer vor Ausfall und bei Verlust eines Mobiltelefons schützen kann.

Nachfolgend wird das Maßnahmenbündel für den Einsatz von Mobiltelefonen vorgestellt.

Planung und Konzeption
- M 2.188 (A) *Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung*
- M 2.190 (Z) *Einrichtung eines Mobiltelefon-Pools*

Umsetzung
- M 4.114 (A) *Nutzung der Sicherheitsmechanismen von Mobiltelefonen*

Betrieb
- M 2.189 (A) *Sperrung des Mobiltelefons bei Verlust*
- M 2.558 (A) *Sensibilisierung der Mitarbeiter zur Informationssicherheit bei Mobiltelefonen, Smartphones, Tablets und PDAs*
- M 4.115 (B) *Sicherstellung der Energieversorgung von Mobiltelefonen*
- M 4.255 (A) *Nutzung von IrDA-Schnittstellen*
- M 5.78 (Z) *Schutz vor Erstellen von Bewegungsprofilen bei der Mobiltelefon-Nutzung*
- M 5.79 (Z) *Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung*
- M 5.80 (Z) *Schutz vor Abhören der Raumgespräche über Mobiltelefone*
- M 5.81 (B) *Sichere Datenübertragung über Mobiltelefone*

Aussonderung
- M 2.13 (A) *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln*
- M 4.465 (A) *Aussonderung von Mobiltelefonen, Smartphones, Tablets und PDAs*

Notfallvorsorge
- M 6.72 (C) *Ausfallvorsorge bei Mobiltelefonen*

B 3.405 Smartphones, Tablets und PDAs

Beschreibung

Dieser Baustein beschäftigt sich mit mobilen Endgeräten zur Datenerfassung, -bearbeitung und -kommunikation. Diese gibt es in verschiedenen Geräteklassen, die sich nach Abmessungen und Leistungsmerkmalen unterscheiden. Dazu gehören unter anderem:

- Organizer, um Adressen und Termine zu verwalten.
- PDAs mit und ohne eigene Tastatur, bei denen die Dateneingabe über das Display oder die Tastatur erfolgt. Der primäre Einsatzzweck ist das Erfassen und Bearbeiten von Terminen, E-Mails, Adressen und kleinen Notizen.
- Smartphones, also Mobiltelefone mit Computer-Funktionen und eingebauter Schnittstelle zur Datenübertragung. Beim Einsatz von Smartphones ist zusätzlich Baustein B 3.404 *Mobiltelefon* und gegebenenfalls Baustein B 3.203 *Laptop* umzusetzen.
- Tablets, bei denen es sich in der Regel um große Smartphones mit oder ohne Telefonfunktion handelt. Geräte, die größer als übliche Smartphones, aber noch kleiner als übliche Tablets sind, werden auch Smartlets oder Phablets genannt. Der Einsatzbereich ist identisch mit Smartphones, nur dass hier komfortabler Daten verarbeitet, Dokumente gelesen und im Internet gesurft werden kann. Beim Einsatz von Tablets mit Telefonfunktion ist zusätzlich Baustein B 3.404 *Mobiltelefon* umzusetzen.
- Den Übergang zu "echten" Notebooks stellen sogenannte Sub-Notebooks (Netbooks, Ultrabooks, etc.) dar, die wesentlich kleiner als normale Notebooks sind und daher beispielsweise weniger Peripheriegeräte und Anschlussmöglichkeiten bieten, die aber unter anderem für die Vorführung von Präsentationen geeignet sind. Viele Tablets lassen sich auch um eine Tastatur erweitern und sind dann wie ein Laptop zu benutzen. Beim Einsatz von Sub-Notebooks oder Tablets ist zusätzlich der Baustein B 3.203 *Laptop* umzusetzen.

Die Übergänge zwischen den verschiedenen Gerätetypen sind fließend und außerdem dem ständigen Wandel der Technik unterworfen. Eine typische Anforderung an Smartphones, Tablets und PDAs ist die Nutzung von Standard-Office-Anwendungen auch unterwegs. Hierfür werden angepasste Varianten von Textverarbeitungs-, Tabellenkalkulations-, E-Mail- bzw. Kalenderprogrammen angeboten. Die Geräte werden aber auch zunehmend für sicherheitskritische Applikationen eingesetzt, wie beispielsweise die Nutzung als Authentisierungstoken für Zugriffe auf Unternehmensnetze (z. B. Generierung von Einmalpasswörtern), Speicherung von Patientendaten oder die Führung von Kundenkarteien.

In diesem Baustein werden diejenigen Sicherheitseigenschaften von Smartphones, Tablets und PDAs betrachtet, die für die Anwender bei der Nutzung relevant sind. Es soll ein systematischer Weg aufgezeigt werden, wie Smartphones, Tablets und PDAs sicher in Institutionen eingesetzt werden können, wie Sicherheitskonzepte für diese Endgeräte erstellt und fortentwickelt werden sollten und wie auf diese Weise Smartphones, Tablets und PDAs sicher in einem Informationsverbund eingebettet werden können.

Gefährdungslage

Für den IT-Grundschutz werden im Rahmen der Nutzung von Smartphones, Tablets und PDAs folgende typische Gefährdungen angenommen:

Höhere Gewalt

- G 1.15 *Beeinträchtigung durch wechselnde Einsatzumgebung*

Organisatorische Mängel

- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*
- G 2.7 *Unerlaubte Ausübung von Rechten*

- G 2.200 *Unzureichende Planung bei der Anschaffung von Mobiltelefonen, Smartphones, Tablets oder PDAs*

Menschliche Fehlhandlungen

- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.43 *Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen*
- G 3.44 *Sorglosigkeit im Umgang mit Informationen*
- G 3.45 *Unzureichende Identifikationsprüfung von Kommunikationspartnern*
- G 3.76 *Fehler bei der Synchronisation mobiler Endgeräte*
- G 3.123 *Unerlaubte private Nutzung des dienstlichen Mobiltelefons, Smartphones, Tablets oder PDAs*

Technisches Versagen

- G 4.42 *Ausfall des Mobiltelefons, Smartphones, Tablets oder PDAs*
- G 4.51 *Unzureichende Sicherheitsmechanismen bei Smartphones, Tablets oder PDAs*
- G 4.52 *Datenverlust bei mobilem Einsatz*

Vorsätzliche Handlungen

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.22 *Diebstahl bei mobiler Nutzung des IT-Systems*
- G 5.23 *Schadprogramme*
- G 5.123 *Abhören von Raumgesprächen über mobile Endgeräte*
- G 5.124 *Missbrauch der Informationen von mobilen Endgeräten*
- G 5.125 *Datendiebstahl mithilfe mobiler Endgeräte*
- G 5.126 *Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten*
- G 5.177 *Missbrauch von Kurz-URLs oder QR-Codes*
- G 5.193 *Unzureichender Schutz vor Schadprogrammen auf Smartphones, Tablets und PDAs*
- G 5.194 *Einschleusen von GSM-Codes in Endgeräte mit Telefonfunktion*

Maßnahmenempfehlungen

Maßnahmenempfehlungen

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für Smartphones, Tablets und PDAs sind eine Reihe von Maßnahmen erforderlich, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb. Die Phasen, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Phasen beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Um Smartphones, Tablets und PDAs sicher und effektiv in Behörden oder Unternehmen einsetzen zu können, sollte ein Konzept erstellt werden, das auf den Sicherheitsanforderungen für die bereits vorhandenen IT-Systeme sowie den Anforderungen aus den geplanten Einsatzszenarien beruht (siehe M 2.303 *Festlegung einer Strategie für den Einsatz von Smartphones, Tablets oder PDAs*). Darauf aufbauend ist die Nutzung von Smartphones, Tablets und PDAs zu regeln und es sind Sicherheitsrichtlinien dafür zu erarbeiten (siehe M 2.304 *Sicherheitsrichtlinien und Regelungen für die Nutzung von Smartphones, Tablets und PDAs*). Auf Smartphones, Tablets und PDAs können verschiedene Applikationen (Apps) installiert werden. Die Anwendungen müssen ausgewählt und sicher ausgeführt werden (siehe M 4.467 *Auswahl von Applikationen für Smartphones, Tablets und PDAs*).

Beschaffung

Für die Beschaffung von Smartphones, Tablets und PDAs müssen die aus dem Konzept resultierenden Anforderungen an die jeweiligen Produkte formuliert und basierend darauf geeignete Geräte ausgewählt werden (siehe M 4.305 *Einsatz von Speicherbeschränkungen (Quotas)*). Auch muss geprüft werden, ob zusätzliche Sicherheitswerkzeuge anzuschaffen sind, die die Sicherheit von Smartphones, Tablets und

PDAs bis zu einem gewissen Grad erhöhen können (siehe M 4.231 *Einsatz zusätzlicher Sicherheitswerkzeuge für Smartphones, Tablets oder PDAs*).

Umsetzung

Über mobile Endgeräte wie Laptops, Smartphones, Tablets oder PDAs soll auch häufig unterwegs auf Daten aus dem Internet oder dem internen Netz einer Institution zugegriffen werden. Dafür sollten zusätzliche Aspekte zum Schutz der Informationen berücksichtigt werden (siehe M 5.121 *Sichere Kommunikation von unterwegs*).

Betrieb

Je nach Sicherheitsanforderungen müssen die beteiligten Software-Komponenten (Smartphones/Tablets/PDA, Synchronisationssoftware, Software zum zentralen Geräte-Management) unterschiedlich konfiguriert werden. Dies betrifft vor allem die Endgeräte selber (siehe M 4.228 *Nutzung der Sicherheitsmechanismen von Smartphones, Tablets und PDAs*), die Synchronisationsumgebung (siehe M 4.229 *Sicherer Betrieb von Smartphones, Tablets und PDAs*) und spezielle Software zum zentralen Geräte-Management (siehe M 4.230 *Zentrale Administration von Smartphones, Tablets und PDAs*). Damit Smartphones, Tablets und PDAs sicher eingesetzt werden können, müssen auch damit gekoppelte Arbeitsplatz-Rechner und hier vor allem die Synchronisationsschnittstelle sicher konfiguriert sein. Geeignete Sicherheitsempfehlungen für Standard-Arbeitsplatz-PCs sind in den Client-Bausteinen der Schicht 3 beschrieben.

Aussonderung

Bei Ausfall, Defekt, Zerstörung oder Diebstahl eines Smartphones, Tablets oder PDAs, sollte es in jeder Organisation klare Meldewege und Ansprechpartner geben (siehe M 2.306 *Verlustmeldung*). Zudem ist organisatorisch sicherzustellen, dass Smartphones, Tablets und PDAs auf geeignete Weise ausgesondert werden (siehe M 4.465 *Aussonderung von Mobiltelefonen, Smartphones, Tablets und PDAs*).

Notfallvorsorge

Ein Smartphone, Tablet oder PDA kann aus verschiedenen Gründen ausfallen oder in seiner Funktionsfähigkeit gestört sein. Daher sollten entsprechende Vorkehrungen getroffen werden, um einem Ausfall vorzubeugen bzw. die Probleme zu minimieren (siehe M 6.95 *Ausfallvorsorge und Datensicherung bei Smartphones, Tablets und PDAs*). Ebenso müssen entsprechende Empfehlungen umgesetzt werden, damit bei einem Diebstahl oder Verlust nicht alle Daten auf dem Endgerät verloren gehen oder in fremde Hänge gelangen (siehe M 6.159 *Vorsorge vor Verlust und Diebstahl von Smartphones, Tablets und PDAs*).

Nachfolgend wird das Maßnahmenbündel für den Einsatz von Smartphones, Tablets und PDAs vorgestellt.

Planung und Konzeption

- M 2.218 (C) *Regelung der Mitnahme von Datenträgern und IT-Komponenten*
- M 2.303 (A) *Festlegung einer Strategie für den Einsatz von Smartphones, Tablets oder PDAs*
- M 2.304 (A) *Sicherheitsrichtlinien und Regelungen für die Nutzung von Smartphones, Tablets und PDAs*
- M 4.467 (B) *Auswahl von Applikationen für Smartphones, Tablets und PDAs*
- M 4.468 (B) *Trennung von privatem und dienstlichem Bereich auf Smartphones, Tablets und PDAs*

Beschaffung

- M 2.305 (B) *Geeignete Auswahl von Smartphones, Tablets oder PDAs*
- M 4.231 (Z) *Einsatz zusätzlicher Sicherheitswerkzeuge für Smartphones, Tablets oder PDAs*

Umsetzung

- M 5.121 (B) *Sichere Kommunikation von unterwegs*

Betrieb

- M 1.33 (A) *Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz*
- M 2.558 (A) *Sensibilisierung der Mitarbeiter zur Informationssicherheit bei Mobiltelefonen, Smartphones, Tablets und PDAs*

- M 4.3 (A) *Einsatz von Viren-Schutzprogrammen*
- M 4.31 (A) *Sicherstellung der Energieversorgung im mobilen Einsatz*
- M 4.228 (A) *Nutzung der Sicherheitsmechanismen von Smartphones, Tablets und PDAs*
- M 4.229 (C) *Sicherer Betrieb von Smartphones, Tablets und PDAs*
- M 4.230 (Z) *Zentrale Administration von Smartphones, Tablets und PDAs*
- M 4.232 (Z) *Sichere Nutzung von Zusatzspeicherkarten*
- M 4.255 (A) *Nutzung von IrDA-Schnittstellen*
- M 4.466 (C) *Einsatz von Viren-Schutzprogrammen bei Smartphones, Tablets und PDAs*
- M 4.469 (A) *Abwehr von eingeschleusten GSM-Codes auf Endgeräten mit Telefonfunktion*
- M 5.173 (Z) *Nutzung von Kurz-URLs und QR-Codes*
- M 5.176 (B) *Sichere Anbindung von Smartphones, Tablets und PDAs an das Netz der Institution*

Aussonderung

- M 2.306 (A) *Verlustmeldung*
- M 4.465 (A) *Aussonderung von Mobiltelefonen, Smartphones, Tablets und PDAs*

Notfallvorsorge

- M 6.95 (C) *Ausfallvorsorge und Datensicherung bei Smartphones, Tablets und PDAs*
- M 6.159 (C) *Vorsorge vor Verlust und Diebstahl von Smartphones, Tablets und PDAs*

B 4.8 Bluetooth

Beschreibung

Bluetooth ist ein offener Industriestandard für ein lizenzfreies Nahbereichsfunkverfahren zur kabellosen Sprach- und Datenkommunikation zwischen IT-Geräten (Kabelersatz und Ad-hoc-Networking). Die Entwicklung von Bluetooth geht auf eine Initiative der Bluetooth Special Interest Group (Bluetooth SIG) im Jahre 1998 zurück, der eine große Zahl von Herstellern angehört.

Mit Bluetooth können mobile Endgeräte über eine Funkschnittstelle schnell und einfach miteinander verbunden werden. Verschiedene in den Geräten definierte Bluetooth-Profile ermöglichen dann die Übertragung von Daten, Sprachsignalen, Steuerungsinformationen bis hin zur Bereitstellung von Diensten, wie beispielsweise FTP oder Modem- und Netzdiensten. Bluetooth funkt, genauso wie WLAN, im lizenzfreien ISM-Band zwischen 2,402 GHz und 2,480 GHz, hat jedoch nur eine Reichweite von circa 100 m, benötigt aber, im Gegensatz zu Infrarot, keine Sichtverbindung zwischen den einzelnen Endgeräten. Bluetooth wird vornehmlich bei mobilen Endgeräten wie Mobiltelefone, PDAs oder Laptops eingesetzt.

In diesem Baustein soll ein systematischer Weg aufgezeigt werden, wie Bluetooth-fähige Endgeräte einer Institution sicher verwendet werden können.

Gefährdungslage

Für den IT-Grundschutz werden im Rahmen der Nutzung von Bluetooth folgende typische Gefährdungen angenommen:

Höhere Gewalt

- G 1.17 *Ausfall oder Störung eines Funknetzes*

Organisatorische Mängel

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*

Menschliche Fehlhandlungen

- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.38 *Konfigurations- und Bedienungsfehler*
- G 3.43 *Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen*

Technisches Versagen

- G 4.60 *Unkontrollierte Ausbreitung der Funkwellen*
- G 4.79 *Schwachstellen in der Bluetooth-Implementierung*
- G 4.80 *Unzureichende oder fehlende Bluetooth-Sicherheitsmechanismen*

Vorsätzliche Handlungen

- G 5.28 *Verhinderung von Diensten*
- G 5.143 *Man-in-the-Middle-Angriff*
- G 5.159 *Erstellung von Bewegungsprofilen unter Bluetooth*
- G 5.160 *Missbrauch der Bluetooth-Profile*

Maßnahmenempfehlungen

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Damit Bluetooth sicher eingesetzt werden kann, müssen auch damit gekoppelte Clients sicher konfiguriert sein. Geeignete Sicherheitsempfehlungen für Clients sind in den Bausteinen der Schicht 3 beschrieben.

Im Rahmen des Bluetooth-Einsatzes sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Um Bluetooth sicher und effektiv einsetzen zu können, sollte ein Konzept erstellt werden, das auf der Gesamt-Sicherheitsstrategie der Institution sowie den Anforderungen aus den geplanten Einsatzszenarien beruht. Darauf aufbauend ist die Bluetooth-Nutzung in der Behörde bzw. im Unternehmen zu regeln und eine Sicherheitsrichtlinie dafür zu erarbeiten (siehe M 2.461 *Planung des sicheren Bluetooth-Einsatzes*).

Beschaffung

Für die Beschaffung von Bluetooth-Komponenten müssen die aus dem Konzept resultierenden Anforderungen an die jeweiligen Produkte formuliert und basierend darauf die Auswahl der geeigneten Produkte getroffen werden (siehe M 2.462 *Auswahlkriterien für die Beschaffung von Bluetooth-Geräten*).

Umsetzung

Je nach Sicherheitsanforderungen müssen die Bluetooth-Komponenten unterschiedlich konfiguriert werden (siehe M 4.362 *Sichere Konfiguration von Bluetooth*). Benutzer und Administratoren sind ausreichend zu schulen, um Sicherheitsvorfälle zu minimieren und auf mögliche Gefahren bei einer unsachgemäßen Verwendung von Bluetooth-Komponenten hinzuweisen und zu sensibilisieren (siehe M 3.80 *Sensibilisierung für die Nutzung von Bluetooth*).

Betrieb

Bluetooth-Geräte müssen im Betrieb angemessen abgesichert werden (siehe M 4.363 *Sicherer Betrieb von Bluetooth-Geräten*).

Aussonderung

Werden Bluetooth-Geräte außer Betrieb genommen, so sind alle sensiblen Informationen wie Zugangsinformationen zu löschen (siehe M 4.364 *Regelungen für die Aussonderung von Bluetooth-Geräten*).

Nachfolgend wird das Maßnahmenbündel für den Einsatz von Bluetooth vorgestellt.

Planung und Konzeption
- M 2.461 (A) *Planung des sicheren Bluetooth-Einsatzes*
- M 3.79 (W) *Einführung in Grundbegriffe und Funktionsweisen von Bluetooth*

Beschaffung
- M 2.462 (Z) *Auswahlkriterien für die Beschaffung von Bluetooth-Geräten*

Umsetzung
- M 3.80 (A) *Sensibilisierung für die Nutzung von Bluetooth*
- M 4.362 (A) *Sichere Konfiguration von Bluetooth*

Betrieb
- M 2.463 (Z) *Nutzung eines zentralen Pools an Bluetooth-Peripheriegeräten*
- M 4.363 (A) *Sicherer Betrieb von Bluetooth-Geräten*

Aussonderung
- M 4.364 (A) *Regelungen für die Aussonderung von Bluetooth-Geräten*

B 5.14 Mobile Datenträger

Beschreibung

In diesem Baustein werden die grundsätzlichen Sicherheitseigenschaften mobiler Datenträger betrachtet. Mobile Datenträger können eingesetzt werden für

- den Datenaustausch (siehe Baustein B 5.2 *Datenträgeraustausch*),
- den Datentransport zwischen IT-Systemen, die nicht miteinander vernetzt sind, oder zwischen verschiedenen Lokationen (siehe z. B. B 5.8 *Telearbeit*),
- die Archivierung oder Speicherung von Sicherheitskopien (Backup), falls andere automatisierte Verfahren nicht zweckmäßig sind (siehe Bausteine B 1.4 *Datensicherungskonzept* und B 1.12 *Archivierung*),
- die Speicherung von Daten, die zu sensitiv sind, um sie auf Arbeitsplatzrechnern oder Servern zu speichern,
- die mobile Datennutzung oder Datenerzeugung (z. B. MP3-Player, Digitalkamera, etc.).

Es gibt eine Vielzahl verschiedener Varianten von mobilen Datenträgern, hierzu gehören unter anderem Disketten, Wechselplatten (magnetisch, magneto-optisch), CD-ROMs, DVDs, Magnetbänder, Kassetten, USB-Festplatten und auch Flash-Speicher wie USB-Sticks. Durch diese Vielzahl an Formen und Einsatzgebieten werden nicht immer alle erforderlichen Sicherheitsbetrachtungen vorgenommen.

Datenträger können danach klassifiziert werden, ob sie nur lesbar, einmalig beschreibbar oder wiederbeschreibbar sind. Sie können auch nach weiteren Kriterien unterteilt werden, beispielsweise

- nach der Art der Datenspeicherung: analoge oder digitale Datenträger
- wie sie bearbeitet werden können: ohne technische Hilfsmittel, wie z. B. Papier, oder nur mit technischen Hilfsmitteln, wie z. B. Mikrofilme oder Tonbänder
- nach ihrer Bauform: auswechselbare Datenträger, externe Datenspeicher oder Datenträger, die in andere Geräte integriert sind.

Auswechselbare Datenträger, teilweise auch als Wechselmedien bezeichnet, werden in ein Laufwerk eingelegt. Beispiele hierfür sind Disketten, CD-ROMs, DVDs, Magnetbänder und Kassetten. Externe Datenspeicher, wie beispielsweise USB-Sticks und externe Festplatten, können hingegen direkt an ein IT-System angeschlossen werden. Beispiele für Datenträger, die in anderen Geräten integriert sind, sind die Speicherkomponenten in Mobiltelefonen, MP3-Playern und Digitalkameras.

Neben den digitalen Datenträgern sind auch Informationen auf Papier, Mikrofilmen oder anderen analogen Datenträgern bei der Sicherheitskonzeption zu berücksichtigen. Dies betrifft insbesondere das Drucken, Kopieren und Einscannen von Dokumenten sowie die Nutzung von Fax-Diensten. Weitere Hinweise hierzu finden sich in den Bausteinen B 3.406 *Drucker, Kopierer und Multifunktionsgeräte* und B 3.402 *Faxgerät*.

In diesem Baustein wird einerseits aufgezeigt, wie die auf mobilen Datenträgern gespeicherten Informationen sicher genutzt werden können und andererseits wie einer unbefugten Weitergabe von Informationen über mobile Datenträger vorgebeugt werden sollte.

Gefährdungslage

Für den IT-Grundschutz bei der Nutzung von mobilen Datenträgern werden folgende typische Gefährdungen angenommen:

Höhere Gewalt

- G 1.9 *Datenverlust durch starke Magnetfelder*
- G 1.15 *Beeinträchtigung durch wechselnde Einsatzumgebung*

Organisatorische Mängel

- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.10 *Nicht fristgerecht verfügbare Datenträger*

Menschliche Fehlhandlungen

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.44 *Sorglosigkeit im Umgang mit Informationen*

Technisches Versagen

- G 4.7 *Defekte Datenträger*
- G 4.52 *Datenverlust bei mobilem Einsatz*

Vorsätzliche Handlungen

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.4 *Diebstahl*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.23 *Schadprogramme*
- G 5.141 *Datendiebstahl über mobile Datenträger*
- G 5.142 *Verbreitung von Schadprogrammen über mobile Datenträger*

Maßnahmenempfehlungen

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den sicheren Umgang mit mobilen Datenträgern sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung und Konzeption über die Beschaffung bis hin zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Es sollte ein Konzept für den sicheren Umgang mit mobilen Datenträgern erstellt werden, in dem für die verschiedenen Arten von mobilen Datenträgern Risiken und Sicherheitsmaßnahmen aufgezeigt werden (siehe M 2.401 *Umgang mit mobilen Datenträgern und Geräten*).

Beschaffung

Die Auswahl geeigneter Datenträger ist abzustimmen. Für die Entscheidung, welche Arten von Datenträgern eingesetzt werden, sollte M 4.169 *Verwendung geeigneter Archivmedien* berücksichtigt werden.

Betrieb

Basierend auf den jeweiligen Sicherheitsanforderungen sollten anhand von Einsatzszenarien Sicherheitshinweise für alle Mitarbeiter erstellt werden (siehe M 3.60 *Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern und Geräten*).

Die Laufwerke und die Schnittstellen der IT-Systeme sollten gemäß den Sicherheitsvorgaben abgesichert werden (siehe M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*).

Aussonderung

Wenn Datenträger weitergegeben werden, sollten sie vor ihrer erneuten Verwendung oder Aussonderung physikalisch gelöscht werden, damit keine sensiblen Informationen in die falschen Hände geraten (siehe M 4.32 *Physikalisches Löschen der Datenträger vor und nach Verwendung*).

Notfallvorsorge

Wichtige Informationen, die auf mobilen Datenträgern gespeichert sind, sollten noch an einer anderen Stelle gespeichert sein, um einem Verlust vorzubeugen.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Mobile Datenträger" vorgestellt.

Planung und Konzeption
- M 2.3 (B) *Datenträgerverwaltung*
- M 2.218 (C) *Regelung der Mitnahme von Datenträgern und IT-Komponenten*
- M 2.401 (C) *Umgang mit mobilen Datenträgern und Geräten*
- M 4.34 (Z) *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*

Umsetzung
- M 4.32 (B) *Physikalisches Löschen der Datenträger vor und nach Verwendung*

Betrieb
- M 3.60 (C) *Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern und Geräten*
- M 4.4 (C) *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*
- M 4.200 (Z) *Umgang mit USB-Speichermedien*
- M 4.232 (Z) *Sichere Nutzung von Zusatzspeicherkarten*

Aussonderung
- M 2.306 (A) *Verlustmeldung*

Notfallvorsorge
- M 6.38 (A) *Sicherungskopie der übermittelten Daten*

G 0.19 Offenlegung schützenswerter Informationen

Vertrauliche Daten und Informationen dürfen nur den zur Kenntnisnahme berechtigten Personen zugänglich sein. Neben der Integrität und der Verfügbarkeit gehört die Vertraulichkeit zu den Grundwerten der Informationssicherheit. Für vertrauliche Informationen (wie Passwörter, personenbezogene Daten, Firmen- oder Amtsgeheimnisse, Entwicklungsdaten) besteht die inhärente Gefahr, dass diese durch technisches Versagen, Unachtsamkeit oder auch durch vorsätzliche Handlungen offengelegt werden.

Dabei kann auf diese vertraulichen Informationen an unterschiedlichen Stellen zugegriffen werden, beispielsweise

- auf Speichermedien innerhalb von Rechnern (Festplatten),
- auf austauschbaren Speichermedien (USB-Sticks, CDs oder DVDs),
- in gedruckter Form auf Papier (Ausdrucke, Akten) und
- auf Übertragungswegen während der Datenübertragung.

Auch die Art und Weise, wie Informationen offengelegt werden, kann sehr unterschiedlich sein, zum Beispiel:

- unbefugtes Auslesen von Dateien,
- unbedachte Weitergabe, z. B. im Zuge von Reparaturaufträgen,
- unzureichende Löschung oder Vernichtung von Datenträgern,
- Diebstahl des Datenträgers und anschließendes Auswerten,
- Abhören von Übertragungsleitungen,
- Infektion von IT-Systemen mit Schadprogrammen,
- Mitlesen am Bildschirm oder Abhören von Gesprächen.

Werden schützenswerte Informationen offengelegt, kann dies schwerwiegende Folgen für eine Institution haben. Unter anderem kann der Verlust der Vertraulichkeit zu folgenden negativen Auswirkungen für eine Institution führen:

- Verstoß gegen Gesetze, zum Beispiel Datenschutz, Bankgeheimnis,
- Negative Innenwirkung, zum Beispiel Demoralisierung der Mitarbeiter,
- Negative Außenwirkung, zum Beispiel Beeinträchtigung der Beziehungen zu Geschäftspartnern, verlorenes Vertrauen von Kunden,
- Finanzielle Auswirkungen, zum Beispiel Schadensersatzansprüche, Bußgelder, Prozesskosten,
- Beeinträchtigung des informationellen Selbstbestimmungsrechtes.

Ein Verlust der Vertraulichkeit wird nicht immer sofort bemerkt. Oft stellt sich erst später heraus, z. B. durch Presseanfragen, dass Unbefugte sich Zugang zu vertraulichen Informationen verschafft haben.

Beispiel:

- Käufer von gebrauchten Rechnern, Festplatten, Mobiltelefonen oder ähnlichen Geräten finden darauf immer wieder höchst vertrauliche Informationen wie Patientendaten oder Kontonummern.

G 0.45 Datenverlust

Ein Datenverlust ist ein Ereignis, das dazu führt, dass ein Datenbestand nicht mehr wie erforderlich genutzt werden kann (Verlust der Verfügbarkeit). Eine häufige Form des Datenverlustes ist, dass Daten unbeabsichtigt oder unerlaubt gelöscht werden, zum Beispiel durch Fehlbedienung, Fehlfunktionen, Stromausfälle, Verschmutzung oder Schadsoftware.

Ein Datenverlust kann jedoch auch durch Beschädigung, Verlust oder Diebstahl von Geräten oder Datenträgern entstehen. Dieses Risiko ist bei mobilen Endgeräten und mobilen Datenträgern häufig besonders hoch.

Weiterhin ist zu beachten, dass viele mobile IT-Systeme nicht immer online sind. Die auf diesen Systemen gespeicherten Daten befinden sich daher nicht immer auf dem aktuellsten Stand. Wenn Datenbestände zwischen mobilen IT-Systemen und stationären IT-Systemen synchronisiert werden, kann es durch Unachtsamkeit oder Fehlfunktion zu Datenverlusten kommen.

Beispiele:

- Der PDA fällt aus der Hemdtasche und zerschellt auf den Fliesen, ein Mobiltelefon wird statt der Zeitung vom Hund apportiert, leider mit Folgen. Solche und ähnliche Ereignisse sind die Ursachen von vielen Totalverlusten der Daten mobiler Endgeräte.
- Es gibt Schadprogramme, die gezielt Daten auf infizierten IT-Systemen löschen. Bei einigen Schädlingen wird die Löschfunktion nicht sofort bei der Infektion ausgeführt, sondern erst, wenn ein definiertes Ereignis eintritt, zum Beispiel wenn die Systemuhr ein bestimmtes Datum erreicht.
- Viele Internet-Dienste können genutzt werden, um online Informationen zu speichern. Wenn das Passwort vergessen wird und nicht hinterlegt ist, kann es passieren, dass auf die gespeicherten Informationen nicht mehr zugegriffen werden kann, sofern der Dienstleister kein geeignetes Verfahren zum Zurücksetzen des Passwortes anbietet.
- Festplatten und andere Massenspeichermedien haben nur eine begrenzte Lebensdauer. Wenn keine geeigneten Redundanzmaßnahmen getroffen sind, kann es durch technische Defekte zu Datenverlusten kommen.

G 1.15 Beeinträchtigung durch wechselnde Einsatzumgebung

Mobile Datenträger und Geräte werden in sehr unterschiedlichen Umgebungen eingesetzt und sind dadurch einer Vielzahl von Gefährdungen ausgesetzt. Dazu gehören beispielsweise schädigende Umwelteinflüsse wie zu hohe oder zu niedrige Temperaturen, ebenso wie Staub oder Feuchtigkeit. Zu anderen Problemen, die durch die Mobilität der Geräte entstehen, gehören beispielsweise Transportschäden.

Ein weiterer wichtiger Aspekt bei mobilen Datenträgern und Geräten ist, dass sie oft in Bereichen mit unterschiedlichem Sicherheitsniveau benutzt werden. Bei einigen Umgebungen ist das Sicherheitsniveau den Benutzern bekannt, bei anderen nicht. Besonders Smartphones, Tablets, PDAs, Laptops und ähnliche mobile Endgeräte sind nicht nur beweglich, sondern können auch einfach mit anderen IT-Systemen kommunizieren. Daher müssen auch die Probleme betrachtet werden, die durch diese Interaktion ausgelöst werden. Innerhalb der eigenen Institution können Mitarbeiter die Vertrauenswürdigkeit von IT-Systemen weitgehend einschätzen, in fremden Umgebungen ist das jedoch schwierig. Die Kommunikation mit unbekannten IT-Systemen und Netzen birgt immer ein Gefährdungspotenzial für das eigene mobile Endgerät. So können bei der Kontaktaufnahme mit anderen IT-Systemen beispielsweise auch Schadprogramme mit übertragen oder sensible Informationen kopiert werden.

Daher muss nach der Rückkehr von mobilen Datenträgern und IT-Systemen immer kritisch hinterfragt werden, wo dieser USB-Stick, PDA oder Laptop schon überall gewesen ist, um dann die entsprechenden Vorsichtsmaßnahmen einzuleiten.

Ein weiteres Problem bei der Nutzung von fremden Infrastrukturen, wie z. B. beim Herunterladen von Informationsangeboten auf Messen, ist die häufig unzureichende Transparenz der angebotenen Dienste. Viele Diensteanbieter sammeln Kundendaten, um Profile zu erstellen, die sie zu Werbezwecken verwenden oder an Dritte weiterverkaufen. Solche Profile enthalten beispielsweise Informationen über Aufenthaltsorte und das Kommunikationsverhalten des Benutzers (welche Dienste, wann, wie oft, mit wem). Auch Anwendungen, die vollständig auf dem eigenen mobilen Endgerät ablaufen, sammeln unter Umständen Daten (z. B. über Nutzungshäufigkeit und -art) und geben sie weiter, sobald das Gerät online geht.

Immer wieder werden mobile Datenträger und Geräte verloren oder gestohlen. Je kleiner und begehrter solche Geräte sind, wie beispielsweise Smartphones, Tablets oder PDAs, desto höher ist dieses Risiko. Neben dem materiellen Verlust kann dabei durch den Verlust bzw. die Offenlegung wichtiger Daten weiterer Schaden entstehen.

G 2.2 Unzureichende Kenntnis über Regelungen

Regelungen lediglich festzulegen sichert noch nicht, dass sie beachtet werden und der Betrieb störungsfrei ist. Allen Mitarbeitern müssen die geltenden Regelungen auch bekannt sein, vor allem den Funktionsträgern. Ein Schaden, der entsteht, weil bestehende Regelungen nicht bekannt sind, darf sich nicht mit den Aussagen entschuldigen lassen: "Ich habe nicht gewusst, dass ich dafür zuständig bin." oder "Ich habe nicht gewusst, wie ich zu verfahren hatte."

Beispiele:

- Werden Mitarbeiter nicht darüber unterrichtet, wie sie korrekt mit mobilen Datenträgern und E-Mails umzugehen haben, besteht die Gefahr, dass hierüber Schadprogramme im Unternehmen bzw. in der Behörde verbreitet werden. Durch falsches Verhalten könnten auch vertrauliche Daten versehentlich in die Hände Unbefugter geraten.
- In einer Bundesbehörde wurden farblich unterschiedliche Papierkörbe aufgestellt, von denen eine Farbe für die Entsorgung zu vernichtender Unterlagen bestimmt war. Die meisten Mitarbeiter waren über diese Regelung nicht unterrichtet.
- In einer Bundesbehörde gab es eine Vielzahl von Regelungen zur Durchführung von Datensicherungen, die nach und nach mündlich zwischen dem IT-Sicherheitsbeauftragten und dem IT-Referat vereinbart worden waren. Eine Nachfrage ergab, dass die betroffenen Mitarbeiter die getroffenen "Vereinbarungen" nicht kannten und auch nicht wussten, wer ihr Ansprechpartner für Fragen der Datensicherung war. Die Regelungen waren auch nicht dokumentiert. Viele Benutzer haben darum z. B. von den lokalen Daten ihres Arbeitsplatzrechners keine Datensicherung angefertigt, obwohl nur auf den Servern kontinuierliche Datensicherungen zentral durchgeführt wurden.
- In einem Rechenzentrum wurde als neue Regelung festgelegt, dass wegen Problemen mit der Einbruch- und Brandmeldeanlage die Pförtnerloge auch nachts besetzt werden sollte. Der Pförtnerdienst war jedoch über diese Regelung vom Sicherheitsverantwortlichen nicht informiert worden. Als Folge war das Rechenzentrum für mehrere Wochen nachts unzureichend geschützt.
- In einer Institution existiert die Regelung, dass der Verlust eines Mobiltelefons sofort einer Leitstelle gemeldet werden muss, damit die SIM-Karte gesperrt werden kann. Einem Mitarbeiter war diese Regelung nicht bekannt. Er gab den Verlust erst Tage später nach seiner Rückkehr von einer Dienstreise an. In der Zwischenzeit wurden mit dem verlorenen Mobiltelefon jedoch diverse Premium-Dienste angerufen und Kurzmitteilungen an diese Dienste geschickt. Dadurch entstand ein erheblicher wirtschaftlicher Schaden.

G 2.4 Unzureichende Kontrolle der Sicherheitsmaßnahmen

Werden bereits eingeführte Sicherheitsmaßnahmen (z. B. Klassifizierung von Informationen, Datensicherung, Zutrittskontrolle, Vorgaben für Verhalten bei Notfällen) nicht konsequent umgesetzt und regelmäßig kontrolliert, kann es sein, dass sie nicht wirksam sind oder missachtet werden. Mängel, die bei einer Kontrolle festgestellt werden, lassen sich meist ohne Schaden abstellen. Wenn Verstöße erst anlässlich eines Schadensfalls auffallen, kann oft nicht mehr rechtzeitig und der jeweiligen Situation angemessen reagiert werden.

Darüber hinaus gibt es Sicherheitsmaßnahmen, die nur wirksam sind, wenn Verantwortliche sie kontrollieren. Hierzu zählen beispielsweise Protokollierungsfunktionen, deren Sicherheitseigenschaften erst zum Tragen kommen, wenn die Protokolldaten ausgewertet werden.

Beispiele:

- Zur Vorbereitung von Straftaten kommt es vor, dass Schließzylinder in Außentüren und Toren von nicht autorisierten Personen ausgetauscht werden. Gerade wenn es sich um Zugänge handelt, die selten genutzt werden oder lediglich als Notausgänge vorgesehen sind, werden diese bei Streifengängen nur in Panikrichtung geprüft. Die Funktionalität der Schließzylinder wird dabei oft vernachlässigt. Zur Vorbereitung von Straftaten kommt es vor, dass Schließzylinder in Außentüren und Toren von nicht autorisierten Personen ausgetauscht werden. Gerade wenn es sich um Zugänge handelt, die selten genutzt werden oder lediglich als Notausgänge vorgesehen sind, werden diese bei Streifengängen nur in Panikrichtung geprüft. Die Funktionalität der Schließzylinder wird dabei oft vernachlässigt.
- Die Sicherheitsleitlinie einer Institution schreibt vor, dass die eingesetzten Smartphones nicht "gerootet" werden dürfen bzw. dass kein "Jailbreak" durchgeführt werden darf, da so die Sicherheitseigenschaften des Betriebssystems umgangen werden können. Solche modifizierten Smartphones sind innerhalb einer Institution nicht mehr sicher einsetzbar. Wird diese Vorgabe nicht überprüft, ist es möglich, dass Mitarbeiter mit einem unsicheren Smartphone auf das Netz oder schützenswerte Informationen der Institution zugreifen.
- In einer Behörde werden einige Unix-Server zur externen Datenkommunikation eingesetzt. Aufgrund der zentralen Bedeutung dieser IT-Systeme sieht das Sicherheitskonzept vor, dass die Unix-Server wöchentlich einer Integritätsprüfung unterworfen werden. Da nicht regelmäßig kontrolliert wird, ob diese Überprüfungen tatsächlich stattfinden, fällt erst bei der Klärung eines Sicherheitsvorfalls auf, dass die IT-Abteilung auf solche Integritätsprüfungen verzichtet hat. Als Grund wurde die mangelhafte personelle Ausstattung der Abteilung genannt.
- In einem Unternehmen wurde die Rolle des z/OS-Security-Auditors nicht besetzt. Dies hatte zur Folge, dass die Einstellungen im RACF im Laufe der Zeit nicht mehr den Sicherheitsvorgaben des Unternehmens entsprachen. Erst nach einem Produktionsausfall wurde bemerkt, dass einige Anwender mehr Rechte hatten, als sie für ihre Tätigkeit benötigten. Eine für die Produktion wichtige Anwendung war von ihnen versehentlich gestoppt worden. In einem Unternehmen wurde die Rolle des z/OS-Security-Auditors nicht besetzt. Dies hatte zur Folge, dass die Einstellungen im RACF im Laufe der Zeit nicht mehr den Sicherheitsvorgaben des Unternehmens entsprachen. Erst nach einem Produktionsausfall wurde bemerkt, dass einige Anwender mehr Rechte hatten, als sie für ihre Tätigkeit benötigten.

Eine für die Produktion wichtige Anwendung war von ihnen versehentlich gestoppt worden.

G 2.139 Mangelhafte Berücksichtigung von mobilen Endgeräten beim Patch- und Änderungsmanagement

Die wachsende Mobilität von Endgeräten ist eine der besonderen Herausforderungen für das Patch- und Änderungsmanagement. Mobile Systeme sind durch ihren wechselnden Einsatzort und ihre Anbindung an bestehenden Netze durch Funktechnologien nicht immer in die automatisierte Verteilung von Patches und Änderungen eingebunden.

Zusätzlich ist bei mobilen Endgeräten üblicherweise nicht die gleiche Bandbreite und Stabilität bei der Datenübertragung wie bei stationären Systemen in einem LAN gewährleistet. Das Anlegen von Sicherheitskopien sowie Wiederherstellungspunkten dauert im Vergleich länger und funktioniert weniger zuverlässig.

Werden mobile Systeme bei der Planung von Patches und Änderungen nicht gesondert berücksichtigt, kann die Verteilung nur unvollständig durchgeführt werden, nimmt mehr Zeit in Anspruch als geplant und bedeutet auch immer ein Sicherheitsrisiko.

Beispiel:

- Die von einem Unternehmen beschafften Mobiltelefone lassen sich nur via Verbindung an einen Rechner aktualisieren. Dazu müssen die Benutzer die mobilen Geräte an die IT-Abteilung des Unternehmens übergeben. Nachdem eine gravierende Schwachstelle in der Bluetooth-Implementierung entdeckt und ein Sicherheitspatch veröffentlich wurde, konnten Angreifer von einigen Geräten wichtige Informationen auslesen, da die entsprechenden Mitarbeiter ihre Geräte nicht zeitnah zur Aktualisierung abgegeben hatten.

G 2.200 Unzureichende Planung bei der Anschaffung von Mobiltelefonen, Smartphones, Tablets oder PDAs

Durch Mobiltelefone, Smartphones, Tablets und PDAs treten Probleme für die Informationssicherheit auf, wenn

- relevante Eigenschaften der anzuschaffenden Geräte nicht während der Planungsphase erhoben werden,
- der Funktionsumfang der Geräte nicht dem Einsatzzweck entspricht oder
- sonstige Randbedingungen zum sicheren Betrieb der Geräte nicht berücksichtigt wurden.

Zwar ist der Funktionsumfang von Mobiltelefonen, Smartphones, Tablets und PDAs verschiedener Anbieter sehr ähnlich, an mitunter relevanten Stellen, wie beispielsweise dem Gerätemanagement, gibt es jedoch große Unterschiede. So kann es sein, dass

- ein Smartphone sich nicht auf gewünschte Weise (zum Beispiel mit IPSec) mit dem Netz der Institution verbinden lässt,
- das Gerät keine vollständige Verschlüsselung aller gespeicherten Daten unterstützt,
- auf dem Gerät keine selbst erstellten oder angepassten Applikationen verwendet werden können sollte dies notwendig sein,
- der auf dem Gerät befindliche E-Mail-Client Zugangspasswörter nur im Klartext speichert,
- die eingesetzte Software zum Management für mobile Endgeräte nicht mit der Betriebssystemversion des Smartphones kompatibel ist und deswegen relevante Anforderungen aus dem Sicherheitskonzept (zum Beispiel Erzwingen eines langen Passwortes) nicht umsetzbar sind oder
- ein Mitarbeiter hauptsächlich außerhalb geschlossener Räume arbeitet und daher statt eines handelsüblichen Smartphones ein witterungsbeständiges und stoßfestes Gerät mit längerer Akkukapazität benötigt.

Werden diese und ähnliche Aspekte in der Planungsphase nicht ausreichend berücksichtigt, können Gefährdungen für die Informationssicherheit der Institution entstehen.

G 3.1 Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten

Durch Fehlverhalten von Personen aller Art kann der Vertraulichkeits- bzw. Integritätsverlust von Informationen und Daten herbeiführt bzw. ermöglicht werden. Die Folgeschäden ergeben sich aus der Schutzbedürftigkeit der Daten. Beispiele für ein solches Fehlverhalten sind:

- Mitarbeiter holen versehentlich Ausdrucke mit personenbezogenen Daten wqnicht am Netzdrucker ab.
- Vertrauliche Informationen werden in Hörweite fremder Personen diskutiert, beispielsweise in Pausengesprächen von Besprechungen oder über Mobiltelefonate in öffentlichen Umgebungen.
- Es werden Datenträger versandt, ohne dass die vorher darauf gespeicherten Daten in geeigneter Weise gelöscht wurden.
- Dokumente werden auf einem Webserver veröffentlicht, ohne dass geprüft wurde, ob diese tatsächlich zur Veröffentlichung vorgesehen und freigegeben sind.
- Aufgrund von fehlerhaft administrierten Zugriffsrechten vermag ein Mitarbeiter Daten zu ändern, ohne die Brisanz dieser Integritätsverletzung einschätzen zu können.
- Neue Software wird mit nicht anonymisierten Daten getestet. Nicht befugte Mitarbeiter erhalten somit Einblick in geschützte Dateien bzw. vertrauliche Informationen. Möglicherweise erlangen überdies auch Dritte Kenntnis von diesen Informationen, weil die Entsorgung von "Testausdrucken" nicht entsprechend geregelt ist.
- Beim Ausbau, Verleih, Einsendung zur Reparatur oder Ausmusterung von Festplatten können Daten auf zum Teil noch intakten Dateisystemen in unbefugte Hände gelangen, wenn diese zuvor nicht irreversibel gelöscht wurden.
- Betreut ein Outsourcing-Dienstleister mehrere Mandanten, so können Daten einer auslagernden Organisation durch menschliches Versagen anderen Mandanten des Outsourcing-Dienstleisters zugänglich werden. Mögliche Ursachen können beispielsweise folgende sein:
  - Auswahl einer falschen E-Mail-Adresse aus dem Adressbuch.
  - Unbedachtes "copy - paste" (z. B. von Konfigurationsdateien von Systemen verschiedener Auftraggeber).
  - Postversand (z. B. von Backup-Medien, Verträgen) an die falsche Adresse.

G 3.3 Nichtbeachtung von Sicherheitsmaßnahmen

Aufgrund von Nachlässigkeit und fehlenden Kontrollen kommt es immer wieder vor, dass Personen die ihnen empfohlenen oder angeordneten Sicherheitsmaßnahmen nicht oder nicht im vollen Umfang durchführen. Es können Schäden entstehen, die sonst verhindert oder zumindest vermindert worden wären. Je nach der Funktion der Person und der Bedeutung der missachteten Maßnahme können sogar gravierende Schäden eintreten. Vielfach werden Sicherheitsmaßnahmen aus einem mangelnden Sicherheitsbewusstsein heraus nicht beachtet. Ein typisches Indiz dafür ist, dass wiederkehrende Fehlermeldungen nach einer gewissen Gewöhnungszeit ignoriert werden.

- Ein verschlossener Schreibtisch bietet zur Aufbewahrung von Dokumenten, DVDs, USB-Sticks oder anderen Informationsträgern keinen hinreichenden Schutz gegen unbefugten Zugriff, wenn der Schlüssel im selbern Büro aufbewahrt wird, z. B. auf dem Schrank oder unter der Tastatur.
- Obwohl die schadensmindernde Eigenschaft von Datensicherungen hinreichend bekannt ist, treten immer wieder Schäden auf, wenn Daten unvorhergesehen gelöscht werden und aufgrund fehlender Datensicherung die Wiederherstellung unmöglich ist. Dies zeigen insbesondere die dem BSI gemeldeten Schäden, die z. B. aufgrund von Schadsoftware entstehen.
- Der Zutritt zu einem Rechenzentrum sollte ausschließlich durch die mit einem Zutrittskontrollsystem (z. B. Authentikation über Chipkartenleser, PIN-Eingabe oder biometrische Verfahren) gesicherte Tür erfolgen. Die Fluchttür wird jedoch, obwohl sie nur im Notfall geöffnet werden darf, als zusätzlicher Ein- und Ausgang ohne besondere Sicherheitsvorrichtungen genutzt.
- In einem z/OS-System liefen täglich Batch-Jobs für die RACF-Datenbank-Sicherungen. Die korrekte Ausführung dieser Abläufe sollte täglich von den zuständigen Administratoren geprüft werden. Da die Sicherungen jedoch über mehrere Monate ohne Probleme durchgeführt wurden, kontrollierte niemand mehr den Ablauf. Erst nachdem die RACF-Datenbanken des Produktionssyfstems defekt waren und die Sicherungen zurückgespielt werden sollten, wurde festgestellt, dass die Batch-Jobs seit mehreren Tagen nicht mehr gelaufen waren. Dies führte dazu, dass keine aktuellen Sicherungen vorhanden waren und die Änderungen der letzten Tage von Hand nachgetragen werden mussten. Neben einem erheblichen zusätzlichen Administrationsaufwand ergab sich dadurch ein Unsicherheitsfaktor, da nicht alle Definitionen sicher rekonstruiert werden konnten.
- In einer Institution ist es verboten, fremde USB-Geräte an die IT-Infrastruktur der Institution anzuschließen. Ein Mitarbeiter findet gerade keinen dienstlichen USB-Stick und verbindet stattdessen sein Smartphone mit dem PC. Diese mobile IT war jedoch mit einer Schadsoftware infiziert, wodurch es zu einem unberechtigten Datenabfluss kam.

G 3.44 Sorglosigkeit im Umgang mit Informationen

Häufig ist zu beobachten, dass in Institutionen zwar eine Vielzahl von organisatorischen und technischen Sicherheitsverfahren vorhanden sind, diese jedoch durch den sorglosen Umgang mit den Vorgaben und der Technik wieder ausgehebelt werden. Ein typisches Beispiel hierfür sind die fast schon sprichwörtlichen Zettel am Monitor, auf denen Zugangspasswörter notiert sind. Auch andere Beispiele für Nachlässigkeit, Pflichtvergessenheit oder Leichtsinn im Umgang mit schützenswerten Informationen finden sich in großer Menge.

Beispiele:

- In der Bahn oder im Restaurant geben Mitarbeiter oft intimste Unternehmensdetails über ihr Mobiltelefon weiter. Dabei informieren sie jedoch nicht nur den Gesprächspartner, sondern auch die Umgebung. Beispiele für besonders interessante Interna sind,
  - warum der Vertrag mit einer anderen Firma nicht zustande kam oder
  - wie viele Millionen der Planungsfehler in der Strategie-Abteilung gekostet hat und wie das die Aktienkurse des Unternehmens drücken könnte, wenn irgendjemand davon erführe.
- Häufig ist es bei Dienstreisen erforderlich, ein Notebook, einen Organizer oder andere mobile Datenträger mitzunehmen. Immer wieder ist zu beobachten, dass diese während Pausen unbeaufsichtigt im Besprechungsraum, im Zugabteil oder im Auto zurückgelassen werden. Bei mobilen IT-Systemen sind die damit erfassten Daten oftmals nicht an anderer Stelle gesichert. Werden die IT-Systeme gestohlen, sind die Daten ebenfalls verloren. Dazu kommt, dass sich brisante Informationen auch gewinnbringend weiter veräußern lassen, wenn der Dieb aufgrund fehlender Verschlüsselung oder eines nur unzureichenden Zugriffsschutzes einfach darauf zugreifen kann.
- Ein Grund, ein Notebook oder Akten auf Dienstreisen mitzunehmen, ist auch, die Fahrzeiten produktiv nutzen zu können. Hierbei bieten sich Mitreisenden oft interessante Einblicke, da es in der Bahn oder im Flugzeug kaum zu vermeiden ist, dass Sitznachbarn in den Unterlagen oder auf dem Bildschirm mitlesen können.
  Öffentliche Räumlichkeiten, z. B. Hotel-Foyer, Hotel-Business-Center, Zug-Abteil, bieten in der Regel nur wenig Sichtschutz. Gibt der Benutzer Passwörter ein oder muss Veränderungen an den Konfigurationen vornehmen, so kann ein Angreifer ohne größeren Aufwand an diese Informationen gelangen und sie missbräuchlich nutzen.
- In jüngerer Zeit werden E-Mails häufig von einem Mobiltelefon oder Smartphone abgerufen, da die Zeit, um das Notebook zu starten, als zu lang empfunden wird oder weil in einem vollen Zug gerade kein Platz für das Notebook ist. Mobiltelefone und Smartphones besitzen jedoch viel seltener Sichtschutzfolien, sodass vertrauliche E-Mails von Personen in der Umgebung unbemerkt mitgelesen werden können.
- Immer wieder sind in der Presse Artikel über Behörden und Unternehmen zu finden, in deren Hinterhöfen sich hochbrisante Papiere im Altpapiercontainer fanden. Bekannt wurden auf diese Weise beispielsweise die Gehaltszahlen aller Mitarbeiter eines Unternehmens und die geheimen Telefonnummern von Unternehmensvorständen.
- Wenn IT-Systeme Defekte aufweisen, werden diese schnell zur Reparatur gegeben. Meist besteht bei einem Defekt auch keine Möglichkeit mehr, die auf dem betroffenen IT-System gespeicherten Daten zuverlässig zu löschen. Gelegentlich bieten Fachhändler ein funktionsfähiges Austausch-

gerät an. Es hat allerdings diverse Fälle gegeben, bei denen der Kundendienst den Fehler bei einer anschließenden Überprüfung schnell beheben konnte und der nächste Kunde ebenso kulant das jetzt reparierte Gerät erhielt inklusive aller vom ersten Kunden erfassten Daten.

G 3.77 Mangelhafte Akzeptanz von Informationssicherheit

Verschiedene Umstände können dazu führen, dass in einer Institution oder auch in Teilen einer Institution die Informationssicherheit nicht akzeptiert wird und damit auch keine Einsicht in die Notwendigkeit besteht, Sicherheitsmaßnahmen umzusetzen. Dies kann beispielsweise bedingt sein durch

- die Behörden- oder Unternehmenskultur (nach dem Motto: "Das war schon immer so!", "Unseren Mitarbeitern können wir vertrauen, hier muss nichts weggeschlossen werden.", "Was soll hier schon passieren?", "Diese Sicherheitsmaßnahmen stören doch nur die Arbeitsabläufe."),
- fehlende Vorbilder, wenn beispielsweise die Vorgesetzten nicht mit gutem Beispiel vorangehen, oder
- ein anderes soziales Umfeld oder einen anderen kulturellen Hintergrund ("andere Länder, andere Sitten"). Typische Probleme können dadurch entstehen, dass bestimmte Benutzerrechte oder auch die Ausstattung mit Hard- oder Software als Statussymbol gesehen werden. Einschränkungen in diesen Bereichen können auf großen Widerstand stoßen.

Beispiele:

- Im militärischen Umfeld gehen Vorgesetzte häufig davon aus, dass die Umsetzung von Sicherheitsmaßnahmen befohlen werden kann. Allerdings zeigt auch hier die Erfahrung, dass Mitarbeiter, die nicht über Sinn und Zweck von Sicherheitsmaßnahmen informiert sind, diese umgehen, wenn sie diese nur als Behinderung ihrer eigentlichen Aufgabe ansehen.
- Ein Befehl, nur sichere Passwörter zu verwenden, führte bei einem militärischen IT-System dazu, dass ein Passwort-Generator implementiert wurde. Dieser erzeugte 16-stellige zufällige Passwörter, die einmalig 10 Sekunden am Bildschirm angezeigt wurden. Diese Zeitspanne reichte aus, um die Passwörter aufzuschreiben. Da es vielen Leuten schwer fällt, sich Passwörter der Form "aN§3bGP?tz1BuH89" zu merken, wurden diese Zettel entgegen der Anweisungen nicht vernichtet, sondern häufig in der Nähe der Rechner aufbewahrt.
- Gerade Smartphones oder Tablets werden als Statussymbol angesehen, wodurch die Bereitschaft sinkt, Anweisungen zur Informationssicherheit zu befolgen, wie beispielsweise die Geräte nicht für private Zwecke zu benutzen. So gibt es Fälle, in denen Mitarbeiter die Sicherungsmaßnahmen der IT-Abteilung durch "rooten" beziehungsweise "jailbreaking" aktiv umgingen, um gesperrte Applikationen zu installieren. Diese hatten dann allerdings das Recht, das Telefonbuch auszulesen, wodurch die dort gespeicherten Kundendaten in unbefugte Hände gerieten.

G 3.106 Ungeeignetes Verhalten bei der Internet-Nutzung

Falsches Verhalten der unterschiedlichsten Art kann bei der Nutzung von Internet-Diensten negative Auswirkungen haben. Typische Beispiele für ein unpassende Handlungsweise und daraus resultierende unerwünschte Wirkungen sind im Folgenden aufgeführt.

Unzureichende Reaktionsgeschwindigkeit

Die Erwartung von Kommunikationspartner an die Reaktionsgeschwindigkeit ihrer Ansprechpartner ist bei Internet-Anwendungen und E-Mail hoch. Wenn diese Erwartungen nicht erfüllt werden, z. B. weil kein angepasster Bearbeitungsprozess vorhanden ist, kann das zu Umsatzeinbußen, Frustration von Kunden und Mitarbeitern etc. führen.

Kontrollverlust

Durch die Publikation von Informationen in Internet-Diensten oder die Weitergabe per E-Mail ist nicht mehr durch den Verfasser steuerbar, wer diese Informationen erhält und was mit ihnen geschieht. Dadurch kann es zu unerwünschter oder missbräuchlicher Verwendung dieser Informationen kommen.

Vermischung privater und beruflicher Sphäre

Da viele IT-Systeme (z. B. Mobiltelefone, PDAs), Anwendungen und Dienste (z. B. soziale Netzwerke, Web-Mail) sowohl beruflich als auch privat genutzt werden, ist es schwierig, die dort verwendeten Informationen sauber zwischen privater und beruflicher Sphäre zu trennen. Dies kann dann problematisch sein, wenn Angreifer so eine Vielzahl von Daten zusammentragen und für gezielte Angriffe auf einzelne Personen oder Institutionen auswerten, wie z. B. beim Social Engineering.

Vertraulichkeitsverlust

Häufig wird die Sicherheit von Internet-Anwendungen falsch eingeschätzt oder ungeeignete Maßnahmen zur Absicherung von Informationen benutzt, z. B. wenn Informationen verschleiert statt verschlüsselt werden. Dadurch werden vertrauliche Informationen ungewollt einer breiten Öffentlichkeit zugänglich gemacht.

Beispiel:

- Um Daten einfach auszutauschen, hatten zwei Vertragspartner Dateien auf einem Webserver abgelegt. Die URL wurde nur den vertrauenswürdigen Personen der entsprechenden Institutionen per E-Mail mitgeteilt. Die Partner gingen davon aus, dass es nicht möglich ist, diese Dateien über Suchmaschinen zu finden. Doch aufgrund von Webserver-Statistiken, die die meistbesuchten Dateien oder Dateien, die den meisten Datenverkehr (Traffic) verursachten, auflisten, kann es passieren, dass genau diese versteckten Dateien samt genauem Link in der Statistik aufgeführt werden und damit auch für nicht befugte Personen erreichbar sind.

G 3.123 Unerlaubte private Nutzung des dienstlichen Mobiltelefons, Smartphones, Tablets oder PDAs

Wird ein dienstliches Mobiltelefon, Smartphone, Tablet oder ein PDA unerlaubt privat benutzt, kann dies zu folgenden Problemen führen. Beispiele sind:

- Durch private Anrufe oder Nutzung von Datendiensten entstehen Kosten für die Institution.
- Nutzt der Anwender eine grafisch aufwendige Applikation (z. B. ein Spiel), entleert sich der Akku schneller. Dadurch kann das Gerät für die nachfolgende dienstliche Nutzung gegebenenfalls nicht mehr zur Verfügung stehen.
- Verbietet die Institution die private Nutzung von Mobiltelefonen, Smartphones, Tablets und PDAs nicht explizit bzw. kontrolliert ein solches Verbot nicht wirksam, kann dies z. B. datenschutzrechtliche Folgen haben, was das Informationssicherheitsmanagementsystem der Institution behindern kann.
- Werden auf dem Gerät auch private personenbezogene Daten gespeichert, erhöht sich dadurch die Gefahr, dass die Institution Datenschutzgesetze verletzt, beispielsweise wenn die Daten vom Telefon automatisiert durch die Institution gesichert werden.
- Wird auf einem dienstlichen Mobiltelefon, Smartphone, Tablets oder PDA eine private und nicht von der Institution freigegebene Anwendung installiert und betrieben, kann dadurch Schadsoftware auf das Gerät gelangen, Daten, wie z. B. das dienstliche Telefonbuch, können an unbefugte Stellen abfließen oder die Integrität der Daten auf dem Gerät kann durch Fehler in der Anwendung beeinträchtigt werden.

G 4.42 Ausfall des Mobiltelefons, Smartphones, Tablets oder PDAs

Die Benutzung eines Mobiltelefons, Smartphones, Tablets oder PDAs kann durch verschiedene Faktoren negativ beeinträchtigt werden:

- Der Akku kann leer sein, weil vergessen wurde, ihn aufzuladen oder weil das Gerät stark genutzt wurde. Der Akku kann leer sein, weil vergessen wurde, ihn aufzuladen.
- Der Akku kann seine Fähigkeit, Energie zu speichern, verloren haben.
- Der Benutzer hat das Zugangspasswort bzw. die PIN vergessen und kann deswegen das Gerät nicht mehr benutzen oder es wird gelöscht, nachdem das Zugangspasswort bzw. die PIN wiederholt falsch eingegeben wurde.
- Komponenten wie Display, Tasten oder SIM-Karte können defekt sein.

Wenn ein Mobiltelefon, Smartphone, Tablet oder PDA schädigenden Umwelteinflüssen ausgesetzt wird, kann seine Funktionsfähigkeit beeinträchtigt werden. So können die Geräte beispielsweise sowohl unter zu hohen als auch zu niedrigen Temperaturen leiden, ebenso unter Staub oder Feuchtigkeit. Wenn ein Mobiltelefon oder PDA schädigenden Umwelteinflüssen ausgesetzt wird, kann seine Funktionsfähigkeit beeinträchtigt werden. Mobiltelefone und PDAs können sowohl unter zu hohen als auch zu niedrigen Temperaturen leiden, ebenso unter Staub oder Feuchtigkeit.

Beispiele:

- Auf einer längeren Zugfahrt bearbeitete ein Mitarbeiter auf seinem Smartphone eine Präsentation. Um inhaltliche Details zu klären, wurde diese zwischen ihm und einem Kollegen in der Firma mehrmals per E-Mail hin und her geschickt. Da jedoch die Akkulaufzeit stark von der Nutzung abhängig ist und insbesondere Datendienste viel Akkuleistung benötigen, war der Akku unbemerkt nahezu leer geworden. Bei einem späteren wichtigen Telefonat schaltete sich das Gerät automatisch ab und konnte erst Stunden später im Hotelzimmer wieder in Betrieb genommen werden.
- Ein Tablet wird in einem geparkten Auto zurückgelassen. Dies erhöht nicht nur die Diebstahlgefahr, sondern es wird auch eventuell schädigenden Umwelteinflüssen ausgesetzt. Durch direkte Sonneneinstrahlung können im Sommer hinter einer Glasscheibe Temperaturen von über 60°C entstehen. Ein ähnliches Problem besteht im Winter, wo im geparkten Auto Temperaturen deutlich unter dem Gefrierpunkt herrschen können. Durch solche extremen Temperaturen kann der Akku oder auch das Display beschädigt werden.
- Auf einer Dienstreise ist einem älteren PDA zwischendurch der Strom ausgegangen, weil die Ersatzbatterien zu spät eingesetzt wurden. Nach dem Wiedereinschalten sind allerdings viele Konfigurationseinstellungen verloren gegangen, da diese vom Betriebssystem nicht automatisch gesichert wurden. Dadurch laufen anschließend einige Anwendungen wie E-Mail und Internetzugriff nicht mehr korrekt. Auf einer Dienstreise ist dem PDA zwischendurch der Strom ausgegangen, weil die Ersatzbatterien zu spät eingesetzt wurden. Nach dem Wiedereinschalten sind allerdings viele Konfigurationseinstellungen verloren gegangen, da diese vom Betriebssystem nicht automatisch gesichert wurden. Dadurch laufen anschließend einige Anwendungen wie E-Mail und Internetzugriff nicht mehr korrekt.

G 4.51 Unzureichende Sicherheitsmechanismen bei Smartphones, Tablets oder PDAs

Ein IT-System, das sich im mobilen Einsatz befindet, kann über ein VPN an ein LAN angeschlossen sein, so dass die Kommunikationsverbindung sehr gut geschützt ist. Wenn allerdings dieses IT-System selber ungenügend gegen unbefugten Zugriff geschützt ist, besteht die Gefahr, dass ein Unbefugter dieses als "Gateway" missbraucht, um auf das interne Netz zuzugreifen.

Typische Endgeräte für den mobilen Einsatz sind Handys oder PDAs, bei denen meistens keine Benutzertrennung möglich ist. Dadurch kann jeder, der Zugriff auf das IT-System hat, auf alle Daten und Programme zugreifen, auch auf interne Daten der Organisation oder sehr persönliche Daten des Eigentümers.

Andere leider sehr typische Schwachstellen bei mobilen Komponenten wie PDAs sind:

- unzureichende Zugriffschutz- und Authentisierungsmechanismen
- keine oder unzureichende Möglichkeiten zur Verschlüsselung von Daten
- ungesicherte Synchronisation
- keine oder unzureichende Protokollierungsmöglichkeiten

Es gibt eine Vielzahl verschiedener PDA-Modelle mit den unterschiedlichsten Betriebssystemen. Die Sicherheitseigenschaften der verschiedenen PDA-Plattformen sind unterschiedlich, einen sicheren Schutz gegen Manipulationen bietet aber derzeit keines der kommerziell gebräuchlichen Systeme.

Beispiel:

Bei Palm OS 3.5.2 und allen Vorgängerversionen kann über eine Tastenkombination wahlweise in den sogenannten "Console Mode" oder den "Debug Mode" gewechselt werden. Beide Modi erlauben, an allen Sicherheitsmechanismen des Betriebssystems vorbei, den direkten Zugriff auf Systemdaten. Dabei ist es völlig gleichgültig, ob der PDA-Zugriff über ein Passwort geschützt ist oder nicht: beide Modi können unter Umgehung des Zugriffsschutzes aktiviert werden.

G 4.52 Datenverlust bei mobilem Einsatz

Bei mobilen Endgeräten und mobilen Datenträgern ist das Risiko von Datenverlusten höher als bei stationären Systemen. Ursache können Diebstahl oder Geräteverlust sein, aber auch technische Probleme oder schlichter Strommangel.

Mobile Datenträger und Geräte werden oft gestohlen, da sie klein und universell einsetzbar sind. Teilweise haben es die Täter auf die Geräte abgesehen, teilweise aber auch auf die dort gespeicherten Informationen.

Noch häufiger sind Datenverluste ohne kriminelle Absichten von Außenstehenden. In Umfragen hat sich gezeigt, dass jeder zweite Befragte schon einmal einen USB-Stick, eine Speicherkarte oder einen anderen mobilen Datenträger verlegt, vergessen oder verloren hat. Dadurch können schützenswerte Daten in fremde Hände gelangen.

Mobile IT-Endgeräte sind nicht immer online. Daher befinden sich die auf diesen Systemen gespeicherten Daten nicht immer auf dem aktuellsten Stand. Dies betrifft sowohl Kalendereinträge als auch allgemeine Informationen, kann aber unter Umständen auch sicherheitsrelevante Auswirkungen haben. Während der Zeit, in der keine Verbindung zu den organisationseigenen IT-Systemen und Informationsquellen besteht, können beispielsweise keine Informationen über aktuelle Sicherheitsprobleme eingeholt und Virenscanner nicht aktualisiert werden.

Beispiele:

- Das neue Smartphone fällt aus der Hemdtasche und zerschellt oder ein Handheld wird statt der Zeitung vom Hund apportiert. Vor allem Transportschäden führen häufig zu Datenverlusten und Geräte- oder Komponentenausfällen. Staub, Verschmutzung, Feuchtigkeit und Stürze, kurz "unsachgemäße Behandlung", sind die Ursachen von vielen Totalverlusten der Daten mobiler Endgeräte.
- Die Daten eines mobilen Gerätes können temporär nicht verfügbar sein, weil der Akku leer ist, da vergessen wurde, ihn aufzuladen. Sie können unter Umständen, wie z.B. bei älteren Geräten, aber auch vollständig vernichtet sein, wenn neben dem Akku auch die eventuell vorhandene Sicherungsbatterie leer ist und damit alle nicht bereits synchronisierten Daten verloren sind.
- Auch bei der Synchronisation von mobilen Datenträgern und Geräten mit anderen IT-Systemen können Daten zerstört werden. Im Allgemeinen muss vor einer Synchronisation eingestellt werden, wie mit Konflikten beim Datenabgleich umzugehen ist: ob beispielsweise bei gleichlautenden Dateien
  - die des mobilen Endgerätes oder des anderen Endgerätes ungefragt übernommen werden,
  - die neueste Datei übernommen wird oder ob
  - eine Abfrage erfolgt.

Dies wurde häufig bei Inbetriebnahme der Dockingstation einmal konfiguriert und gerät danach wieder in Vergessenheit. Werden dann aber Daten in einer anderen Reihenfolge geändert als ursprünglich einmal gedacht, gehen dabei schnell wichtige Informationen verloren. Zu diesem unangenehmen Nebeneffekt kann es auch kommen, wenn mehrere Benutzer ihre mobilen Endgeräte

mit demselben Endgerät synchronisieren, ohne daran zu denken, dass gleichnamige Dateien dabei überschrieben werden können.

G 4.79 Schwachstellen in der Bluetooth-Implementierung

Die Bluetooth-Spezifikationen enthalten viele Freiheiten, die dort beschriebenen Funktionen umzusetzen. Bereits in den Bluetooth-Spezifikationen finden sich diverse Schwachstellen, durch die jeweiligen Implementierungen der Bluetooth-Geräte können weitere Schwachstellen hinzukommen.

Um die Schwachstellen der Bluetooth-Implementierungen in Endgeräten bzw. der Bluetooth-Spezifikationen auszunutzen, sind diverse Angriffsverfahren bekannt. Im Folgenden sind einige der wesentlichen Angriffsverfahren dargestellt:

Bluejacking

Mit Bluejacking wird ein Übergriff bezeichnet, bei dem von einem Bluetooth-Endgerät, z. B. einem Handy oder PDA, per Bluetooth eine Nachricht auf ein fremdes Bluetooth-fähiges Gerät übertragen wird. Ziel ist es dabei in den meisten Fällen, dadurch beim Empfänger Befremden auszulösen. Als typische Nachrichten finden sich dann solche wie "Deine rote Hose gefällt mir sehr gut.", "Auf der Cebit sollten Sie auf Ihr Handy besser aufpassen." oder einfach "Hello, you've been bluejacked". Hierdurch wird vermittelt, dass einerseits ein tatsächlicher Angriff sehr leicht möglich wäre und dass man andererseits unter Beobachtung steht. Da Bluetooth allerdings nur im Nahbereich funktioniert, ist dies nicht weiter erstaunlich.

Die Nachricht, die hier übertragen wird, ist dabei nicht anderes als der Name des sendenden Bluetooth-Gerätes, der zu einer "Nachricht" ausgebaut wurde. Bei einer Verbindungsanfrage wird der Name des anfragenden Bluetooth-Geräts normalerweise auf dem Display des anderen Gerätes angezeigt. Der Name eines Bluetooth-Geräts ist frei wählbar und kann bis zu 248 Zeichen lang sein. Daher kann dieser auch dazu missbraucht werden, kurze Nachrichten zu übertragen, die den Benutzer verwirren sollen.

Blueprint

Mit dem Blueprint-Verfahren ist es möglich, die Kennung (ID) eines Bluetooth-Endgerätes auszulesen. Aufgrund dieser ID ist es möglich zu ermitteln, um welches Modell es sich bei dem Endgerät handelt. Wenn danach frei verfügbare Informationen, welche Schwachstellen bei dem Modell vorherrschen, ausgewertet werden, kann dann ein gezielter Angriff erfolgen.

Bluesnarfing

Bluesnarfing bezeichnet das Ausspionieren von Informationen aus Bluetooth-Mobiltelefonen wie Adressbüchern und Kalendereinträgen, ohne dass der Handybenutzer darauf aufmerksam wird. Bluesnarfing nützt eine Sicherheitslücke bei Bluetooth-Handys aus. Bei einigen Modellen besteht freier Zugriff auf gespeicherte Daten, wenn Bluetooth eingeschaltet und das Telefon auf "sichtbar" geschaltet ist.

Bei Bluesnarfing wird, ähnlich wie bei Bluejacking, ein fehlerhaft implementiertes Object Exchange Profil in Endgeräten ausgenutzt. Durch den Angriff ist es möglich, mit einem Bluetooth-Endgerät eine direkte Verbindung aufzubauen und beliebige Daten auszulesen, die auf dem Endgerät gespeichert sind. Dadurch können beispielsweise Informationen wie wie Adressbücher aus Mobiltelefonen ausspioniert werden, ohne dass deren Benutzer dies merken. Bei

Mobiltelefonen und Smartphones ist es dadurch auch möglich, die International Mobile Equipment Identity (IMEI) des Endgerätes auszulesen. Diese IMEI ist für jedes Endgerät eindeutig und ein Angreifer kann beispielsweise eingehende Gespräche auf ein Endgerät unter seiner Kontrolle umleiten, indem er dieses dazu bringt, vorzugeben das angerufene Endgerät zu sein. Mit dem Bluesnarfing++-Verfahren besteht zusätzlich die Möglichkeit, schreibend auf das Endgerät zuzugreifen.

Bluebugging

Durch das Bluebugging wird eine fehlerhafte Bluetooth-Implementierung in manchen älteren Endgeräten ausgenutzt, um einen Zugriff auf das Endgerät direkt bzw. die Kontrolle über das Endgerät zu erlangen. Hierbei werden beim Bluetooth-Protokoll RFCOMM (Radio Frequency Communication), welches dazu dient, serielle Schnittstellen zu emulieren, die Kanäle 16 und 17 ausgenutzt, um Daten auszulesen oder Einstellungen an dem Bluetooth-Endgerät vorzunehmen. Darüber hinaus können über Bluebugging ausgehende Telefongespräche initiiert und damit Kosten verursacht bzw. vom Benutzer geführte Telefongespräche überwacht werden. Über Bluebugging können auch andere Dienste beeinträchtigt werden, die das Endgerät anbietet. Bei älteren Endgeräten erhält der Benutzer keinerlei Hinweis darauf, dass sein Endgerät attackiert wird. Bei neueren Endgeräten wird meist eine Sicherheitsabfrage angezeigt, dass ein anderes Endgerät versucht, eine Verbindung zu dem eigenen Endgerät aufzunehmen.

Bluesniping

Als Bluesniping werden Angriffe bezeichnet, bei denen über größere Entfernungen mittels Richtfunkantennen gezielt Bluetooth-Geräte angegriffen werden. In Laborumgebungen wurden hierbei bereits Entfernungen von bis zu zwei Kilometern erreicht. Durch Bluesniping können die verschiedenen Bluetooth-Angriffsverfahren auf eine größere Umgebung ausgeweitet werden.

Denial of Service / BlueSmacking

Denial-of-Service-Angriffe zielen bei Bluetooth in der Regel darauf ab, durch Kompromittierung der Bluetooth-Schnittstelle entweder das Endgerät nicht nutzbar zu machen, beispielsweise weil ständig Pairing-Anfragen beantwortet werden müssen, oder die Batterie des Endgerätes schnell leer zu bekommen.Ein typischer Denial-of-Service-Angriff im Bluetooth-Umfeld ist BlueSmacking. Hierbei werden L2CAP-Anfragen missbraucht, um alle in Empfangsreichweite befindlichen Bluetooth-Geräte gleichzeitig zu stören. Die L2CAP-Anfrage "Echo Request" dient grundsätzlich dazu, ähnlich wie mit einem Ping-Kommando die Empfangsbereitschaft und die Verbindungsgeschwindigkeit zu testen.

G 4.84 Unzureichende Validierung von Ein- und Ausgabedaten bei Webanwendungen und Web-Services

Webanwendungen werden im Allgemeinen von generischen Clients (Web-Browsern) verwendet, sodass Benutzer beliebige Eingabedaten an den Server übermitteln können. Auf Web-Services wird dagegen durch andere Anwendungen oder Dienste zugegriffen (beispielsweise Smartphone-Apps). Eingabedaten können aber auch hier oft modifiziert werden, beispielsweise durch den Einsatz eines Proxys oder durch Manipulation der Clients. Werden schadhafte Eingaben eines Angreifers von der Webanwendung beziehungsweise dem Web-Service verarbeitet, können möglicherweise Schutzmechanismen umgangen werden.

Beispiele für Angriffe, die auf einer unzureichenden Validierung von Eingabedaten beruhen, sind SQL-Injection (siehe G 5.131 *SQL-Injection*), Path Traversal (siehe G 5.172 *Umgehung der Autorisierung bei Webanwendungen und Web-Services*) und Remote File Inclusion. Diese Angriffe können Unbefugten Zugriff auf das Betriebssystem oder auf Hintergrundsysteme ermöglichen. Bei einem erfolgreichen Angriff können schützenswerte Daten unautorisiert ausgelesen oder manipuliert werden.

Nachdem die Webanwendung beziehungsweise der Web-Service die Eingabedaten erfolgreich verarbeitet hat, werden üblicherweise wieder Daten ausgegeben. Die Ausgabedaten werden entweder direkt an den Browser des Benutzers (zum Beispiel Statusmeldungen oder ein neuer Eintrag im Gästebuch) oder die aufrufende Anwendung übermittelt oder an nachgelagerte Systeme weitergereicht. Werden die Daten vor der Ausgabe nicht ausreichend validiert, könnten die Ausgaben Schadcode enthalten, der auf den Zielsystemen interpretiert oder ausgeführt wird.

Die folgenden Beispiele beschreiben mögliche Auswirkungen einer unzureichenden Validierung von Ein- und Ausgaben:

- Eine Webanwendung beziehungsweise ein Web-Service verwendet Eingabedaten ungefiltert zur Erzeugung von Datenbankabfragen. Dies kann ein Angreifer ausnutzen und eine Anfrage formulieren, die neben den regulären Eingabedaten zusätzliche Befehle für die Datenbank enthält. Durch das ungefilterte Einbetten der Eingabedaten in die Datenbankabfrage werden die Befehle von der Datenbank ausgeführt. So kann der Angreifer direkten Zugriff auf die Datenbank erhalten.
- Eine Webanwendung bietet eine Funktion zum Datei-Upload an und schränkt diese auf gewisse Dateitypen ein. Zur Bestimmung des Dateityps überprüft die Webanwendung ausschließlich die Dateiendung und berücksichtigt dabei nicht den Inhalt der Datei. Wird eine erlaubte Dateiendung für den Upload verwendet, können so Dateien mit beliebigem Inhalt zum Server übermittelt werden.
- Werden Eingabedaten durch die Filterkomponente automatisiert geändert und angepasst (Sanitizing), können die Daten durch gezielte Eingaben eines Angreifers von der Filterkomponente in einen Angriffsvektor überführt werden.
- Ein- und Ausgabedaten können in verschiedenen Kodierungen (zum Beispiel UTF-8, ISO 8859-1) und Notationen (zum Beispiel bei UTF-8 ist "." = "2E" = "C0 AE") vorliegen. Abhängig vom angewandten Kodierungssche-

ma kann der gleiche Wert unterschiedlich interpretiert werden. Interpretiert die Filterkomponente die Daten anders als die verarbeitenden Komponenten der Webanwendung oder des Web-Service, so kann ein Angreifer schadhafte Daten (zum Beispiel SQL-Anweisungen) derart codieren, dass sie bei der Filterung nicht erkannt werden. Somit werden die vom Angreifer schadhaften Daten an die verarbeitenden Komponenten weitergereicht und aufgrund der unterschiedlichen Interpretation ausgeführt.

- Die Kommentar-Funktion einer Webanwendung erlaubt eine Formatierung der Texte durch HTML. Die Eingaben werden zum Beispiel nicht auf spezielle HTML-Tags eingeschränkt, sodass ein Angreifer über diese Funktion beliebigen HTML-Code auf der Webanwendung platzieren kann. Dies kann ein Angreifer dazu nutzen, um Elemente der Webseite zu manipulieren oder zu überlagern und Benutzereingaben abzufangen (siehe G 5.175 *Clickjacking*). Derselbe Angriff ist übertragbar auf Web-Services, welche HTML-Code als Eingabe erlauben und diesen ungefiltert in ihre Ausgabe übernehmen.

G 5.2 Manipulation an Informationen oder Software

Informationen oder Software können auf vielfältige Weise manipuliert werden: durch falsches Erfassen von Daten, Änderungen von Zugriffsrechten, inhaltliche Änderung von Abrechnungsdaten oder von Schriftverkehr, Änderungen in der Betriebssystem-Software und vieles mehr. Grundsätzlich betrifft dies nicht nur digitale Informationen, sondern beispielsweise auch Dokumente in Papierform. Ein Täter kann allerdings nur die Informationen und Software-Komponenten manipulieren, auf die er Zugriff hat. Je mehr Zugriffsrechte eine Person auf Dateien und Verzeichnisse von IT-Systemen besitzt bzw. je mehr Zugriffsmöglichkeiten auf Informationen sie hat, desto schwerwiegendere Manipulationen kann sie vornehmen. Falls die Manipulationen nicht frühzeitig erkannt werden, kann der reibungslose Ablauf von Geschäftsprozessen und Fachaufgaben dadurch empfindlich gestört werden.

Die Beweggründe der Täter sind vielfältig und reichen von Rache und mutwilliger Zerstörungslust bis zu Bereicherung oder anderen persönlichen Vorteilen.

Beispiele:

- In einem Schweizer Finanzunternehmen wurde durch einen Mitarbeiter die Einsatzsoftware für bestimmte Finanzdienstleistungen manipuliert. Damit war es ihm möglich, sich illegal größere Geldbeträge zu verschaffen.
- Mitarbeiter, die die Firma verlassen, kopieren vorher Kundendaten, um sie für andere Zwecke gewinnbringend einzusetzen. Solche illegal beschafften Daten von Privatkunden sind beispielsweise benutzt worden, um Vertragsabschlüsse vorzutäuschen. Mitarbeiter, die im Unfrieden eine Behörde oder ein Unternehmen verlassen, könnten auch Informationen oder IT-Systeme mutwillig zerstören oder den Zugriff auf wichtige Informationen oder IT-Systeme verhindern.
- Manipulationen archivierter Dokumente können besonders schwer wiegen, da sie unter Umständen erst nach Jahren bemerkt werden und eine Überprüfung dann oft nicht mehr möglich ist. Archivierte Dokumente stellen meist besonders schützenswerte Informationen dar. Die Manipulation solcher Dokumente ist besonders schwerwiegend, da sie unter Umständen erst nach Jahren bemerkt wird und eine Überprüfung dann oft nicht mehr möglich ist.
- Eine Mitarbeiterin hat sich über die Beförderung ihrer Zimmergenossin in der Buchhaltung dermaßen geärgert, dass sie sich während einer kurzen Abwesenheit der Kollegin unerlaubt Zugang zu deren Rechner verschafft hat. Hier hat sie durch einige Zahlenänderungen in der Monatsbilanz enormen negativen Einfluss auf das veröffentlichte Jahresergebnis des Unternehmens genommen.
- Ein Mitarbeiter ärgert sich darüber, dass sein Vorgesetzter ihm keine Gehaltserhöhung bewilligt hat. Aus Wut sendet er an einige seiner Arbeitskollegen per E-Mail ein Dokument, das einen Computer-Virus enthält und als Geschäftsbrief getarnt ist. Beim Öffnen dieses Dokuments werden unterschiedliche Dateien auf den betroffenen Systemen verändert. Ein Mitarbeiter ärgert sich darüber, dass sein Vorgesetzter ihm keine Gehaltserhöhung gegeben hat. Aus Wut sendet er an einige seiner Arbeitskollegen per E-Mail ein Dokument, das einen Computer-Virus enthält und als Geschäftsbrief getarnt ist. Beim Öffnen dieses Dokuments werden unterschiedliche Dateien auf den betroffenen Systemen verändert.
- Ein Mitarbeiter empfindet die Einschränkungen durch Sicherheitsmaßnahmen bei seinem Smartphone als zu restriktiv und "rootet" sein Smartphone. So gelangt nicht freigegebene Software auf das Gerät, die Schad-

software enthält, vertrauliche Informationen der Institution abgreift und an unbefugte Dritte verschickt. Dadurch entsteht ein großer wirtschaftlicher Schaden.

G 5.4 Diebstahl

Durch den Diebstahl von Datenträgern, IT-Systemen, Zubehör, Software oder Daten entstehen einerseits Kosten für die Wiederbeschaffung sowie für die Wiederherstellung eines arbeitsfähigen Zustandes, andererseits Verluste aufgrund mangelnder Verfügbarkeit. Darüber hinaus können Schäden durch einen Vertraulichkeitsverlust und die daraus resultierenden Konsequenzen entstehen.

Gestohlen werden neben teuren IT-Systemen häufig auch mobile Endgeräte, die unauffällig und leicht zu transportieren sind. Gerade neue Smartphones oder Tablets sind bei Dieben als teure Statussymbole beliebt. Ihr Verlust ist meist schwerwiegend, weil sie für viele Anwendungen benutzt werden (E-Mails, Internet, Präsentationen erstellen) und große Datenmengen speichern können.

Beispiele:

- Im Frühjahr 2000 verschwand ein Notebook aus dem amerikanischen Außenministerium. In einer offiziellen Stellungnahme wurde nicht ausgeschlossen, dass das Gerät vertrauliche Informationen enthalten könnte. Ebenso wenig war bekannt, ob das Gerät kryptografisch oder durch andere Maßnahmen gegen unbefugten Zugriff gesichert war. Bei Sicherheitsuntersuchungen war bereits vor ungenügenden Kontrollen gewarnt worden.
- In einem deutschen Bundesamt wurde mehrfach durch die gleichen ungesicherten Fenster eingebrochen. Neben anderen Wertsachen verschwanden auch mobile IT-Systeme. Das auch Akten kopiert oder manipuliert wurden, konnte nicht zweifelsfrei ausgeschlossen werden.
- In Großbritannien gab es eine Reihe von Datenpannen, bei denen vertrauliche Unterlagen offengelegt wurden, weil Datenträger gestohlen wurden. In einem Fall wurden bei der britischen Luftwaffe Computer-Festplatten gestohlen. Sie enthielten auch sehr persönliche Informationen, die zur Sicherheitsüberprüfung von Mitarbeitern erfasst worden waren.
- Ein Mitarbeiter eines Call-Centers erstellte, kurz bevor er das Unternehmen verlassen musste, Kopien einer großen Menge von vertraulichen Kundendaten. Nach seinem Ausscheiden aus dem Unternehmen hat er diese dann an Wettbewerber verkauft. Da anschließend Details hierüber an die Presse gelangten, verlor das Call-Center viele wichtige Kunden.

G 5.13 Abhören von Räumen über TK-Endgeräte

Über Mikrofone in Endgeräten können grundsätzlich auch Räume abgehört werden. Dabei werden zwei Varianten unterschieden. Bei der ersten Variante geht die Bedrohung von einem Endgerät aus. Hier sind intelligente Endgeräte mit eingebauten Mikrofonen wie Multimedia-PCs, PDAs, Mobiltelefone, aber auch Anrufbeantworter zu nennen. Solche Endgeräte können, wenn entsprechende Funktionalitäten implementiert sind, aus dem öffentlichen Netz oder über das LAN, dazu veranlasst werden, die eingebauten Mikrofone zu aktivieren (siehe auch G 5.40 *Abhören von Räumen mittels Rechner mit Mikrofon und Kamera*). Ein bekanntes Beispiel hierfür ist die so genannte "Baby-Watch-Funktion" von Telefonen oder Anrufbeantwortern.

Bei der zweiten Variante wird die Funktionalität einer TK-Anlage in Verbindung mit entsprechend ausgerüsteten Endgeräten ausgenutzt. Diese Gefährdung entsteht durch die missbräuchliche Verwendung des Leistungsmerkmals "direktes Ansprechen" in Kombination mit der Option "Freisprechen". Die auf diese Weise realisierbare Funktion einer Wechselsprechanlage kann unter gewissen Umständen auch zum Abhören eines Raumes ausgenutzt werden. Im Normalfall wird ein kurzer, einmaliger Warnton bei Aktivierung des Mikrofons abgegeben. Warntöne können aber durch eine entsprechende Konfiguration unterbunden werden. Jeder, der in der Lage ist, eine TK-Anlage zu administrieren, könnte in diesem Fall jeden Raum, in dem ein entsprechend ausgerüstetes Telefon steht, von jedem Endgerät mit Zugriff auf die TK-Anlage oder den Anlagenverbund abhören.

Bei der Nutzung von VoIP-Softphones ergibt sich ein weiteres Gefährdungsszenario. Diese Applikationen ermöglichen die Verwendung eines Multimedia-PCs als Telefon-Endgerät. Der Multimedia-PC wird in der Regel auch für weitere Aufgaben genutzt, beispielsweise um im Internet zu surfen. Da ein Mikrofon für die Sprachübermittlung benötigt wird, könnte es unter Umständen durch Schadsoftware aktiviert und die Umgebung des PCs abgehört werden.

G 5.94 Missbrauch von SIM-Karten

Jeden Tag werden Mobiltelefone verloren oder gestohlen. Neben dem unmittelbaren Verlust kann dabei weiterer finanzieller Schaden entstehen. Gelangt ein Unbefugter mit dem Gerät auch in den Besitz einer SIM-Karte, kann er auf Kosten des rechtmäßigen Karteninhabers telefonieren, sofern:

- ihm die SIM PIN bekannt ist,
- keine SIM PIN gesetzt wurde,
- das Telefon eingeschaltet ist (Standby ohne Display-Password)
- oder die SIM PIN erraten kann.

Mit dem Aufkommen von Datendiensten über Mobilfunk ist zudem das rechtliche Risiko durch Kartenmissbrauch deutlich erhöht worden. Nutzt der Unbefugte die SIM-Karte, beispielsweise um urheberrechtlich geschütztes Material herunterzuladen, Spam-E-Mails zu verschicken oder für Denial-of-Service-Attacken, kann zunächst der Inhaber der SIM-Karte dafür belangt werden.

Daten wie Telefonbuch oder Kurznachrichten, die im Mobiltelefon oder auf der SIM-Karte gespeichert sind, können durchaus einen vertraulichen Charakter haben. Ein Verlust des Mobiltelefons oder der Karte bedeutet dann unter Umständen die Offenlegung dieser gespeicherten Informationen.

Die kryptografischen Sicherheitsmechanismen der SIM-Karten einiger Netzbetreiber waren gegen 1998 schwach ausgelegt. Dadurch war es möglich, SIM-Karten dieser Netzbetreiber zu kopieren. Dazu musste dem Angreifer allerdings die Original-Karte zur Verfügung stehen. Außerdem muss die PIN bekannt sein oder die PIN-Abfrage abgeschaltet sein, damit die IMSI ausgelesen werden kann.

Benutzer können einen solchen Angriff durch Setzen einer schlecht erratbaren SIM PIN nahezu verhindern.

G 5.95 Abhören von Raumgesprächen über Mobiltelefone

Mobiltelefone können dazu benutzt werden, unbemerkt Gespräche aufzuzeichnen oder abzuhören. Im einfachsten Fall wird z. B. bei einer Besprechung ein Mobiltelefon, mit dem eine Verbindung zu einem interessierten Mithörer aufgebaut wurde, unauffällig in einem Raum platziert. Die meisten Mobiltelefone sind mit einer Freisprechfunktion ausgestattet und können problemlos Gespräche im gesamten Raum erfassen. Ferner können die Mobiltelefone so eingestellt werden, dass sie ohne Nutzerinteraktion Anrufe automatisch annehmen, und so in der Nähe stattfindende Gespräche abhören können. Auch wenn die Akkukapazität begrenzt ist, reichen die mehrtägige Bereitschaftszeit und die mehrstündige Gesprächszeit für einen wirkungsvollen Abhörversuch aus.

Mobiltelefone können dazu benutzt werden, unbemerkt Gespräche aufzuzeichnen oder abzuhören. Im einfachsten Fall wird z. B. bei einer Besprechung ein Mobiltelefon, mit dem eine Verbindung zu einem interessierten Mithörer aufgebaut wurde, unauffällig in einem Raum platziert. Die meisten Mobiltelefone sind mit einer Freisprechfunktion ausgestattet und können problemlos Gespräche im gesamten Raum erfassen. Ferner können die Mobiltelefone so eingestellt werden, dass sie ohne Nutzerinteraktion Anrufe automatisch annehmen, und so in der Nähe stattfindende Gespräche abhören können. Auch wenn die Akkukapazität begrenzt ist, reichen die mehrtägige Bereitschaftszeit und die mehrstündige Gesprächszeit für einen wirkungsvollen Abhörversuch aus.

Raumgespräche können auch oft dadurch einfach abgehört werden, in dem ein Mobiltelefon mit aktivierter Diktiergerätefunktion geschickt platziert wird.

Für diesen Zweck können aber auch Mobiltelefone benutzt werden, denen nicht anzusehen ist, dass sie eingeschaltet sind. Das Mobiltelefon dient dabei als Abhöranlage, die über das Telefonnetz von jedem Ort der Welt aktiviert werden kann, ohne dass dies am Mobiltelefon erkennbar wäre. Es waren auch Geräte bekannt, bei denen diese Funktion mittels zusätzlicher Schaltungseinbauten realisiert ist. Diese Manipulation war durch eine Sichtprüfung nach Zerlegen des Gerätes oder durch spezielle Untersuchungsmethoden relativ leicht nachzuweisen. Der Betrieb solcher Geräte ist in Deutschland illegal. Neben diesen technischen Vorkehrungen zum Abhören von Raumgesprächen über Mobiltelefone kann der gleiche Effekt durch geeignete Applikationen (Apps) von Smartphones erzielt werden (siehe G 5.96 *Manipulation von Mobiltelefonen*).

G 5.96 Manipulation von Mobiltelefonen

Der in G 5.95 *Abhören von Raumgesprächen über Mobiltelefone* erwähnte Einbau zusätzlicher elektronischer Schaltungen ist eine typische Hardware-Manipulation. Damit diese Manipulation durchgeführt werden kann, muss sich das zu manipulierende Gerät für eine gewisse Zeit im Besitz des Angreifers befinden.

Täter können Mobiltelefone oder Smartphones aber auch dadurch für Abhörangriffe nutzbar machen, dass sie die geräteinterne Steuersoftware (Firmware) oder eine Applikation manipulieren. Derartige Manipulationen sind meistens weitaus schwerer zu entdecken als Hardware-Manipulationen.

Eine versteckte, nicht dokumentierte Abhörfunktion könnte schon bei der Entwicklung des Gerätes (bewusst oder unbewusst) in die Steuersoftware einprogrammiert sein

Denkbar ist jedoch auch eine nachträgliche Veränderung der Steuersoftware durch einen Dritten, z. B. wenn das Gerät bei einer Reparatur oder aus sonstigen Gründen (Verlust, Entwendung) für den Benutzer (kurzzeitig) nicht kontrollierbar ist. Die Manipulation erfordert aber eingehende Spezialkenntnis, die neben den Firmware-Entwicklern nur wenigen Angreifern zugänglich ist. Für Außenstehende ist diese Manipulation praktisch nicht nachweisbar.

Durch die Erweiterung der Menüfunktionen der Mobiltelefone mittels "SIM-Toolkit" und einer neuen Generation von SIM-Karten, die diese Funktionalität unterstützen, werden Mobiltelefone noch flexibler. Ein so ausgestattetes Mobiltelefon lässt sich per Mobilfunk vom Service-Provider mit neuen Funktionen programmieren. So kann der Kartenanbieter zum Beispiel die Menüstruktur individuell an die Bedürfnisse eines Kunden anpassen.

Dies birgt nun erst recht die Gefahr der Firmware-Manipulation, da Funktionen bereits serienmäßig in der Firmware enthalten sein können, die auch für den Umbau als Lauschsender notwendig sind. Die Wahrscheinlichkeit steigt, dass Funktionen von "außen" aufgerufen werden können, die das Mobiltelefon zu einem Lauschsender umfunktionieren. Denkbar ist auch, dass diese Funktionen ein- und ausschaltbar sind.

Bei Smartphones manipulieren Angreifer eher die Applikationen als die Firmware, da dies deutlich einfacher ist. Denn viele Applikationen haben großzügig eingeräumte Rechte über die Schnittstellen des Smartphones. Sie sind beispielsweise ständig mit dem Internet verbunden und dürfen Umgebungsgeräusche aufnehmen. Ein Angreifer kann unbemerkt über das Internet diese Funktion starten und so nahezu risikolos einen Abhörangriff erfolgreich ausführen. Zudem kann die Abhörfunktion ereignisbasiert eingeschaltet werden, z. B. zu einer gewissen Uhrzeit, wenn sich das Mobiltelefon an einem bestimmten Ort befindet oder wenn ein Telefonat geführt wird. Auch reguläre Applikationen können durch Schwachstellen für Angreifer aus dem Internet gegebenenfalls durch Schwachstellen so manipuliert werden, dass mit ihnen Raumgespräche abgehört und vertrauliche Daten abgeschöpft werden können.

G 5.97 Unberechtigte Datenweitergabe über Mobiltelefone

Mobiltelefone ermöglichen den Datentransport von einem IT-System, z. B. einem PC oder Notebook, zum anderen, ohne dass eine drahtgebundene Verbindung hergestellt werden muss.

Informationen können dort, wo ein offener Zugang zu IT-Systemen möglich ist, unauffällig abgefragt und übermittelt werden. Mithilfe eines Mobiltelefons mit angeschlossenem oder eingebautem Modem können gespeicherte Informationen drahtlos an nahezu jeden beliebigen Ort der Welt übertragen werden. Heutige Smartphones sind nahezu ständig mit dem Internet verbunden. Sie nutzen WLAN und schnelle Datendienste wie HSDPA und LTE und können daher wesentlich einfacher große Datenmengen unberechtigt weitergeben.

Diese Art der unbefugten Datenweitergabe kann sowohl mit einem eigens dafür mitgebrachten oder sogar mit einem internen Mobiltelefon durchgeführt werden. Auf diese Weise lassen sich große Datenbestände unbemerkt nach außen schaffen. Durch neue Technologien wird die Übertragung von großen Datenmengen über Mobiltelefone zunehmend attraktiver. Bei GSM beträgt die maximale Datenübertragungsrate derzeit 14,4 Kbit/s. Neuere Protokolle erreichen wesentlich höhere Bandbreiten. So ist mit GPRS eine Übertragung von 53,6 Kbit/s, mit UMTS eine Übertragung von 384 Kbit/s und mit LTE oder LTE-Advances eine Übertragung von 300 Mbit/s bzw. 900 Mbit/s möglich.

Für eine unberechtigte Datenweitergabe kann ein eigens dafür mitgebrachtes oder sogar ein internes Mobiltelefon eingesetzt werden. Eine nachträgliche Überprüfung ist nicht immer möglich, da die Verbindungsdaten beim Netzbetreiber schon gelöscht sein können.

Beispiele:

- Ein Mitarbeiter eines Unternehmens wird aus einer Besprechung mit einem Externen gerufen, um ein wichtiges Telefonat entgegenzunehmen. Der Externe nutzt die kurze Zeitspanne ohne Beaufsichtigung, um den im Besprechungsraum aufgestellten PC mit seinem GSM-Modem zu verbinden. Anschließend initiiert er eine Datenübertragung zu einem Anschluss seiner Wahl.
- Viele Smartphones können als WLAN-Hotspots (sogenanntes "Tethering") eingesetzt werden. Ein Angreifer könnte in einem Raum (beispielsweise eine Hotelhalle), in dem es regulär einen WLAN-Zugang gibt, mit einem solchen Smartphone das Funksignal des eigentlichen WLANs ersetzen. So kann er alle Datenverbindungen der Teilnehmer in diesem Raum, die nun über dieses Smartphone mit dem Internet verbunden sind, mitschneiden und abhören.

G 5.99 Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefonen

Bei der Mobil-Kommunikation lässt sich auf der Funkstrecke nicht physikalisch verhindern, dass mit entsprechend technischem Aufwand die übertragenen Signale unbefugt mitgehört und aufgezeichnet werden. Darum hätte ein Angreifer nicht das bei leitungsgebundener Kommunikation bekannte Zugriffsproblem.

Ein zweites, generell bei den meisten Funkdiensten auftretendes Problem resultiert daraus, dass die mobilen Kommunikationspartner aus technischen Gründen geortet werden müssen, um erreichbar zu sein.

Sofern sie selbst eine Verbindung aufbauen, geben sie ebenfalls - im Zuge des Verbindungsaufbaus - Informationen über ihren Standort ab. Diese Standort-Informationen könnten durch den Netzbetreiber oder Dienstbetreiber zur Bildung von Bewegungsprofilen verwendet werden.

Die meisten Mobiltelefone und Smartphones haben das sogenannte "Radio Resource Location Services Protocol" (RRLP) umgesetzt, welches der Ortung eines Mobilfunkteilnehmers bei Notrufen dient und das sogar den gegebenenfalls eingebauten GPS-Empfänger zur genaueren Ortung nutzen kann.

In der Regel kann RRLP nicht abgeschaltet werden. Diese Informationen liegen beim Netzbetreiber vor.

G 5.123 Abhören von Raumgesprächen über mobile Endgeräte

Nahezu alle mobilen Endgeräte wie Laptops, Smartphones, Tablets, PDAs und Mobiltelefone werden mit integriertem Mikrofon und/oder eingebauter Kamera ausgeliefert. So können die Geräte dazu benutzt werden, unbemerkt Gespräche aufzuzeichnen oder abzuhören (siehe G 4.95 *Ausfall von Komponenten einer Speicherlösung*). Hierzu genügt ein unauffällig im Raum platziertes Smartphone, zum Beispiel in einer Besprechung.

Beispiel:

- In einer Besprechung haben fast alle Beteiligten ihre Laptops dabei und benutzen diese auch fortwährend. Einer der Teilnehmer hat unauffällig sein Rechnermikrofon aktiviert. Wie bei den meisten mobilen Endgeräten ist auch hier für die anderen Teilnehmer nicht erkennbar, dass das Mikrofon eingeschaltet ist. Er fertigt darüber einen kompletten Mitschnitt der Besprechung an und schneidet daraus kleinere Beiträge heraus. Da diese aus dem Sinnzusammenhang herausgerissen wurden, kann er damit erfolgreich ein anderes Besprechungsergebnis vorspiegeln.

G 5.124 Missbrauch der Informationen von mobilen Endgeräten

Mobile Endgeräte gehen leicht verloren und sind einfach zu stehlen (siehe G 5.22 *Diebstahl bei mobiler Nutzung des IT-Systems*). Je kleiner und begehrter solche Geräte sind, desto höher ist dieses Risiko. Neben dem unmittelbaren Verlust kann dabei durch den Verlust bzw. die Offenlegung wichtiger Daten weiterer Schaden entstehen. Dieser mittelbare Schaden wiegt in vielen Fällen deutlich schwerer als der rein materielle Verlust des Gerätes.

Beispiele:

- Daten wie E-Mails, Notizen von Besprechungen, Adressen oder sonstige Dokumente, die im Smartphone, Tablet oder PDA gespeichert sind, können durchaus einen vertraulichen Charakter haben. Ein Verlust des Geräts bedeutet dann unter Umständen die Offenlegung dieser gespeicherten Informationen.
- Viele mobile Endgeräte haben Sicherheitsmechanismen, die sie vor einem unbefugten Zugriff schützen sollen. Diese Sicherheitsmechanismen sind aber meistens zu schwach ausgelegt, sodass Angreifer sie überwinden können. Selbst wo wirksame Sicherungen vorhanden sind, werden sie häufig aus Bequemlichkeit nicht benutzt, sodass die vertraulichen Daten im Verlustfall überhaupt nicht geschützt sind.
- Oft sind auf mobilen Endgeräten Zugangsdaten für andere IT-Systeme oder für das LAN der Behörde bzw. des Unternehmens gespeichert. Wenn ein Unbefugter in den Besitz eines Laptops oder PDAs mit (statischen) Zugangskennungen gelangt, ist damit ein missbräuchlicher Zugriff auf interne Daten möglich.
- Mit Smartphones und Mobiltelefonen kann ein Dieb auf Kosten des rechtmäßigen Besitzers telefonieren, sofern ihm die PIN bekannt ist oder er sie leicht erraten kann oder wenn die Sicherheitsmechanismen des Gerätes leicht überwunden werden können.
- Mit Smartphones, Tablets oder PDAs mit einer SIM-Karte für den Zugang zum Internet über das Mobilfunknetz kann ein Dieb zum Schaden des rechtmäßigen Besitzers Daten aus dem Internet beziehen. Da innerhalb Deutschlands in der Regel Pauschaltarife angeboten werden, beläuft sich der Schaden lediglich auf die Gebühr, die Karte zu sperren und eine neue Karte in Betrieb zu nehmen. Wenn der Dieb jedoch über die Datenverbindung Spam verschickt oder urheberrechtlich geschütztes Material heruntergeladen hat, sieht sich der Eigentümer des Geräts unter Umständen hohen Schadenersatzforderungen gegenüber. Ihm droht dann zumindest ein hoher Aufwand für rechtliche Auseinandersetzungen.
- Viele Smartphones, Tablets, PDAs und Laptops haben Schnittstellen für den Einsatz austauschbarer Datenspeicher wie z. B. Speicherkarten oder USB-Sticks. Bei einem solchen unbeaufsichtigten mobilen Endgerät mit der entsprechenden Hard- und Software besteht die Möglichkeit, dass über diese Speichermedien große Datenmengen schnell herunterkopiert werden können. Dabei werden nicht einmal Spuren hinterlassen.

G 5.125 Datendiebstahl mithilfe mobiler Endgeräte

Mobile Endgeräte wie Notebooks, Smartphones, Tablets oder PDAs sind größtenteils darauf ausgelegt, einen einfachen Datenaustausch mit anderen IT-Systemen zu ermöglichen. Dies kann über ein Verbindungskabel oder auch drahtlos, z. B. über WLAN, Bluetooth oder eine Mobilfunkverbindung, erfolgen.

Wo ein offener Zugang zu IT-Systemen möglich ist, können Angreifer mithilfe mobiler Endgeräte Informationen unauffällig abfragen, verändern oder mitnehmen. Eine nachträgliche Überprüfung oder gar ein Nachweis sind nicht immer möglich, da häufig die Zugriffe nicht entsprechend protokolliert werden.

Falls das mobile Endgerät über eine drahtlose Kommunikationsschnittstelle verfügt (z. B. WLAN, SIM-Karte oder Bluetooth), können die gespeicherten Informationen auch unmittelbar an jeden Ort der Welt übermittelt werden (siehe G 5.97 *Unberechtigte Datenweitergabe über Mobiltelefone*).

Beispiel:

- Ein Mitarbeiter eines Unternehmens wird aus einer Besprechung mit einem Externen gerufen, um ein wichtiges Telefonat entgegenzunehmen. Der Externe nutzt die kurze Zeitspanne ohne Beaufsichtigung, um den im Besprechungsraum aufgestellten PC mit seinem mobilen Endgerät zu verbinden. Anschließend transferiert er alle zugreifbaren Daten auf sein mobiles Endgerät.
- Ein größeres Unternehmen betreibt ein eigenes drahtloses Netz (WLAN), das jedoch nicht ausreichend abgesichert ist. Ein Angreifer nutzt das aus und verbindet sein Tablet mit dem WLAN. Er kann nun problemlos alle übermittelten Daten "mitschneiden" und hat im schlechtesten Fall Zugriff auf die Dateien im Unternehmensnetz.

G 5.126 Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten

Viele mobile Endgeräte sind inzwischen mit eingebauten Kameras ausgerüstet, zum Beispiel Laptops, Smartphones oder Mobiltelefone. In der Regel ist mit diesen Kameras auch die Aufzeichnung von Filmen möglich. Solche mobilen Endgeräte können leicht dazu benutzt werden, in geschäftskritischen Bereichen (beispielsweise in einer Entwicklungsabteilung) unauffällig Foto- oder Filmaufnahmen anzufertigen. Die Bildqualität reicht meist an die Qualität gewöhnlicher Kleinbildkameras heran.

Wie beim "allgemeinen Datenklau" (siehe G 5.125 *Datendiebstahl mithilfe mobiler Endgeräte*) können die gemachten Bilder unmittelbar nach draußen übertragen und anschließend wieder vom Gerät gelöscht werden. In diesem Fall ist selbst dann, wenn jemand Verdacht schöpft, ein Nachweis ggf. nur mit forensischen Methoden möglich. Sind auf einem Smartphone Applikationen von sozialen Netzen oder Videoportalen wie YouTube installiert, können die gerade erstellten Bilder und Videos im auch Internet veröffentlicht werden. Abgesehen von der Urheberrechtsproblematik können so schützenswerte Daten schnell an Unberechtigte weitergegeben werden. Personen und Institutionen können durch kompromittierende Bilder einen Imageverlust erleiden.

Beispiele:

- In vielen Schwimmbädern und Sportstudios dürfen mittlerweile keine Foto-Handys mehr mitgenommen werden, da es verschiedene Beschwerden über heimlich aufgenommene Fotos aus Umkleidekabinen gab. Unter anderem wurde dies öffentlich, da einige Hobby-Paparazzi ihre Fotos stolz auf Webseiten präsentiert haben.
- Viele Laptop-Modelle haben neben einem integrierten Mikrofon auch eine kleine integrierte Kamera, die je nach Auslegung für Standbilder, Videoaufnahmen oder als Webcam benutzt werden kann. Mit solchen Kameras ist es problemlos möglich, sogar aus den hintersten Reihen in einem Hörsaal nicht nur die Folien lesbar und den Redner hörbar aufzuzeichnen. Sogar Zwischenfragen können damit erstaunlich gut mitgeschnitten werden. Da die Geräte nicht als Kamera wahrgenommen werden, ist es hier schon zu unangenehmen Überraschungen gekommen, als nachträglich ungenehmigte Mitschnitte veröffentlicht wurden.

G 5.141 Datendiebstahl über mobile Datenträger

Viele IT-Systeme haben Schnittstellen für den Einsatz austauschbarer Datenspeicher, wie z. B. Zusatzspeicherkarten oder USB-Speichermedien. Bei einem unbeaufsichtigten IT-System mit der entsprechenden Hard- und Software besteht die Gefahr, dass über diese Datenspeicher große Mengen an Daten unbefugt kopiert werden können. Dieser Vorgang ist in der Regel nach kurzer Zeit abgeschlossen und noch nicht einmal direkt erkennbar.

Natürlich können diese Schnittstellen auch in umgekehrter Weise benutzt werden, um hierüber Schadprogramme auf einem IT-System oder in ein Netz einzuschleusen.

Mobile Datenträger können auch in Geräten mit weiteren Aufzeichnungsfunktionen integriert sein, z. B. in Mobiltelefonen, MP3-Playern oder Digitalkameras. Auch hierüber können unter Umständen sensible Informationen unbefugt aufgenommen werden (siehe G 5.126 *Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten*).

G 5.160 Missbrauch der Bluetooth-Profile

Bluetooth stellt einzelne Profile zur Verfügung, über die standardisiert Daten ausgetauscht, Nachrichten übertragen oder Konfigurationen vorgenommen werden können. Diese Profile können unter Umständen ausgenutzt werden, um auf Bluetooth-Endgeräte zuzugreifen und diese zu manipulieren oder abzuhören bzw. Daten zu entwenden. Einige Gefährdungen, die auf einen Missbrauch dieser Profile zurückzuführen sind, sind im Folgenden beispielhaft beschrieben.

Damit auf ein anderes Bluetooth-Endgerät zugegriffen werden kann, ist normalerweise ein Pairing zwischen den Endgeräten notwendig. Teil des Pairings ist stets auch eine Authentisierung. Allerdings sieht es die Bluetooth-Spezifikation vor, dass bereits vor dem Pairing ohne eine entsprechende Authentisierung ein Zugriff auf das Service Discovery Protocol (SDP) möglich ist. Mit diesem Protokoll tauschen die Bluetooth-Endgeräte die jeweils verfügbaren Profile aus. In der Vergangenheit wurden Bluetooth-Implementierungen bekannt, bei denen Profile vorgesehen waren, die nicht über das SDP angezeigt wurden. Die Hersteller hatten offensichtlich eine Art Hintertür geöffnet. Auf Basis dieser Schwachstelle ließen sich unter anderem einzelne Profile ausnutzen, so dass ohne ein vorheriges Pairing, also ohne Authentisierung, Daten zwischen Bluetooth-Endgeräten ausgetauscht werden konnten.

- Ein Angreifer konnte beispielsweise das OBEX Push Profile nutzen, das für den einfachen Datenaustausch vorgesehen ist, um Kalendereinträge oder Telefonbücher auszulesen. Unterstützt das Endgerät auch einen OBEX-basierenden FTP-Server, so erhält der Angreifer gleichzeitig auch schreibenden Zugriff auf das Endgerät.
- Durch die fehlende Authentisierung kann auch das HID Profil ausgenutzt werden, das für die Eingabe von Eingabegeräten, sprich Maus oder Tastaturen, gedacht ist. Wird auch hier auf die Authentisierung verzichtet und existiert bereits ein erfolgreiches Pairing, beispielsweise zwischen einer Tastatur und einem Rechner, dann kann mit diesen Informationen ein weiteres Eingabegerät simuliert werden und beispielsweise über eine Keylogger-Software Tastatureingaben mitgeschnitten werden.

Problematischer ist der Missbrauch des SIM Access Profils. Mit diesem Profil besteht die Möglichkeit, direkt über Bluetooth auf die SIM-Karten von Mobiltelefonen zuzugreifen. Dieses Profil wird typischerweise bei einem eingebauten Autotelefon angewendet, das mittels Bluetooth auf ein anderes Telefon zugreifen möchte. Durch diesen direkten Zugriff auf die SIM-Karte könnten Manipulationen an der Mobilfunkverbindung vorgenommen werden, ohne dass der Nutzer das mitbekommt. So kann über das SIM Access Profil beispielsweise das SIM Application Toolkit, das in vielen SIM-Karten implementiert ist, dazu verwendet werden, um den für die Verschlüsselung der Mobilfunkverbindung verwendeten Sitzungsschlüssel per SMS zu versenden. Mit diesem Sitzungsschlüssel kann eine aufgezeichnete Kommunikation über die Funkschnittstelle eines Mobiltelefons entschlüsselt und somit ausgespäht werden. Somit entstehen durch die Kombination der beiden Techniken Bluetooth und Mobilfunk Angriffsszenarien, die mit jeder Technik für sich genommen nicht möglich wären.

G 5.177 Missbrauch von Kurz-URLs oder QR-Codes

Webseiten werden üblicherweise über eine URL (Uniform Resource Locator) angesteuert, die daher auch Web-Adresse genannt wird. Die Komplexität vieler Webseiten führt häufig zu relativ langen Web-Adressen, die schwer zu merken sind und vor allem bei mobilen Endgeräten wie Smartphones nicht in einer Zeile dargestellt werden können. Daher haben sich verschiedene Methoden entwickelt, um den Benutzern die Nutzung von Webadressen zu erleichtern. Prominente Vertreter sind Kurz-URLs und QR-Codes.

Kurz-URLs

Kurz-URLs bezeichnen einen weitverbreiteten Dienst im Internet, bei dem lange URLs durch kürzere URLs ersetzt werden. Kurz-URLs erleichtern es, Referenzen und Verweisen in Zeitschriftenartikeln zu folgen. Viele Artikel in papiergebundenen Zeitschriften verweisen auf Quellen aus dem Internet bzw. enthalten Hinweise zu Internetseiten. Anders als bei Online-Artikeln müssen diese per Hand abgetippt werden. Kurz-URLs verringern den Aufwand dafür erheblich. Kurz-URLs haben also einige Vorteile, aber auch einige Risiken:

- Verfügbarkeit: Kurz-URLs werden, ohne dass die Benutzer eingreifen müssen, über die Datenbank eines Dienstleisters in die dort hinterlegte ursprüngliche Web-Adresse aufgelöst. Diese Datenbank mit den Zuordnungen zwischen den kurzen und langen URLs muss verfügbar sein. Große Datenbanken haben Milliarden an Einträgen. Fällt die Datenbank zeitweise oder dauerhaft aus, sind Milliarden von Kurz-URLs unbrauchbar. Ferner kann es sein, dass der bisherige Anbieter eines Dienstes die Nutzungsbedingungen ändert, so dass die darüber generierten Kurz-URLs nicht mehr ohne weiteres genutzt werden können.
- Datenschutz: Durch die Benutzung von Kurz-URLs kann der Anbieter des Dienstes nachvollziehen, welche IP-Adresse wann auf welche Seite zugegriffen hat.
- Integrität: Aus einer Kurz-URL ist nicht ersichtlich, wohin sie verweist. Daher sind Kurz-URLs für alle Formen von Angriffen attraktiv, bei denen Benutzer auf manipulierte Webseiten gelockt werden sollen. So ist beispielsweise bei einer gefälschten E-Mail-Adresse eines eventuell bekannten Absenders, die eine Kurz-URL enthält, die Chance größer, dass der Link wirklich angeklickt wird. Ferner kann die Datenbank des Anbieters der Kurz-URL manipuliert worden sein, so dass die Kurz-URLs gar nicht mehr auf ihr eigentliches Ziel verweisen.

QR-Codes

QR-Codes (Quick Response) sind, ähnlich wie Barcodes, Darstellungen von Daten in maschinenlesbarer Form, in diesem Fall handelt es sich typischerweise um Quadrate, in denen mit Mustern aus kleineren Quadraten Informationen standardisiert gespeichert sind. QR-Codes finden sich oft auf Produkten oder Verbraucherinformationen und dienen dazu, Anwender auf zusätzliche Informationsquellen zu verweisen, die für diese nützlich oder interessant sein könnten. Die Anwender müssen den jeweiligen QR-Code zunächst abfotografieren oder einscannen, z. B. mit ihrem Smartphone. Auf dem Endgerät muss außerdem eine Applikation installiert sein, um die in den QR-Codes enthaltenen Informationen wie beispielsweise URLs, Adressen, Telefonnummern oder WLAN-Zugangsinformationen aufzulösen. Ein häufiges Anwendungsszenario sind QR-Codes auf Prospekten, in denen eine URL codiert ist, aber auch in industriellen Umgebungen und in der Logistik werden sie oft eingesetzt.

QR-Codes sind mit einer hohen Fehlertoleranz maschinenlesbar, lassen sich aber von Menschen nicht ohne weiteres dekodieren. Daher können Benutzer vor dem Einlesen eines QR-Codes nicht erkennen, welche Informationen in diesem kodiert wurden. Die Gefährdungen sind ähnlich wie bei Kurz-URLs. Beispielsweise könnten QR-Codes auf Webseiten mit Schadsoftware oder auf kostenpflichtige Service-Rufnummern verweisen. Außerdem könnten QR-Codes auch Informationen enthalten, über die Schwachstellen im Betriebssystem des auslesenden Endgerätes ausgenutzt werden. Beispielweise könnte ein QR-Code Programmaufrufe beinhalten, die zu einen Buffer Overflow oder zu einem Injection-Angriff führen.

Beispiel:

- Ein Angreifer erstellte einen QR-Code, der auf über eine URL auf eine Webseite verwies, die mit Schadsoftware für ein weitverbreitetes Smartphone-Betriebssystem verseucht war. Diesen druckte er im passenden Format aus und überklebte damit zahlreiche QR-Codes auf Litfaßsäulen und anderen Werbeträgern auf einer gut besuchten Technik-Messe. Zahlreiche Anwender lasen den QR-Code ein, wodurch deren Smartphones mit der Schadsoftware infiziert und kostenpflichtige SMS an einen ausländischen Dienst auf Kosten der Anwender verschickt wurden.

G 5.193 Unzureichender Schutz vor Schadprogrammen auf Smartphones, Tablets und PDAs

Smartphones, Tablets und PDAs besitzen meistens nur ein aktives Benutzerkonto mit eingeschränkten Rechten. Das Administrator-Konto ist in der Regel abgeschaltet. Das heißt, Benutzer können zwar neue Anwendungen installieren oder deinstallieren, jedoch keine tiefen Veränderungen am Betriebssystem selbst vornehmen. Solche administrativen Rechte sind nur durch Manipulationen am Betriebssystem zugänglich ("rooten" oder "jailbreaking").

Anders als bei PCs ist es daher nicht möglich, Programme zur Abwehr von Schadprogrammen mit so hohen Rechten auszustatten, dass sie von diesen nicht manipuliert werden können. So gibt es Schadsoftware, die Schwachstellen im Betriebssystem ausnutzt, um sich administrative Rechte auf dem Endgerät zu verschaffen. Damit verfügt sie dann über höhere Rechte als jedes Schutzprogramm. Solche Schadprogramme sind sehr schwer zu entdecken und können mit normalen Mitteln nicht mehr vom Endgerät entfernt werden.

Eine weitere Hürde für Schutzprogramme ist, dass der Zugriff von einer Anwendung auf eine andere Anwendung in der Regel eingeschränkt und auf manchen Plattformen sogar komplett ausgeschlossen ist. Das erschwert die Arbeit von Schutzprogrammen oder macht sie sogar unmöglich.

Zudem arbeiten Schutzprogramme meistens nur mit Virensignaturen, um Schadsoftware zu erkennen. Weitere Methoden, wie heuristische Analysen der Daten oder eine Verhaltensanalyse, sind in der Regel aufgrund der begrenzten Akku-Kapazität nicht verfügbar. Verfahren, die dieses Problem durch eine externe Datenverkehrsanalyse lösen wollen, werfen jedoch datenschutzrechtliche Fragen und zusätzliche Sicherheitsrisiken auf, da hier der gesamte Datenstrom auf das Gerät mit heuristischer Suche analysiert wird. Dafür müssen verschlüsselte Verbindungen entweder aufgebrochen werden oder können nicht analysiert werden.

G 5.194 Einschleusen von GSM-Codes in Endgeräte mit Telefonfunktion

GSM-Codes (oder auch USSD- oder MMI-Codes) bestehen aus Zahlenkombinationen, die mit Stern, Raute oder beidem beginnen bzw. enden. Sie veranlassen das Endgerät dazu, bestimmte Funktionen auszuführen. Ein bekannter GSM-Code ist **#06#*, der bei allen Endgeräten mit Telefonfunktion dazu führt, dass die international eindeutige Geräteidentifikationsnummer (IMEI-Nummer) im Display angezeigt wird. Im Weiterem können mit GSM-Codes auch die PIN und die PUK geändert werden.

Neben den GSM-Codes gibt es noch herstellerspezifische Codes, die beispielsweise das Gerät in den Werkszustand versetzen oder Servicemenus aufrufen. Eine weitere Klasse von Codes ist abhängig vom Netzbetreiber- bzw. Mobilfunkanbieter z. B. um das Guthabenkonto abzufragen.

Eine Gefährdung für die Informationssicherheit entsteht dadurch, dass diese GSM-Codes nicht nur durch direkte Eingabe am Gerät, sondern auch über andere Schnittstellen an die Endgeräte übergeben werden können. So können entsprechend konfigurierte Internetseiten GSM-Codes über den Browser an das Endgerät übermitteln. Auch QR-Codes (siehe G 5.177 *Missbrauch von Kurz-URLs oder QR-Codes*) können GSM-Codes enthalten und nach dem Einscannen an das Endgerät weitergeben. Zudem ist es möglich, über die "Near-Field-Communication"-Schnittstelle (NFC-Schnittstelle) solche Codes einzuschleusen. Dadurch ist es Angreifern möglich, zum Beispiel Schadsoftware zur Datenspionage auf dem Gerät zu installieren oder die SIM-Karte zu sperren.

Beispiele:

- Auf einer von Angreifern präparierten Internetseite ist der GSM-Code für dreimaliges Ändern der PIN und anschließendes zehnmaliges Ändern der PUK enthalten. Ein Mitarbeiter besucht mit seinem Smartphone die Internetseite und der GSM-Code wird an sein Gerät übermittelt. Danach ist die SIM-Karte so gesperrt, dass es für den Benutzer nicht mehr möglich ist, diese ohne Hilfe der IT-Abteilung zu entsperren.
- Angreifer haben den QR-Code auf einem Werbeplakat mit einem anderen QR-Code überklebt. Dieser enthält nun, statt eines Links zu einer Internetseite mit weiteren Informationen, den GSM-Code für einen Firmware-Reset. . Ein solcher Vorfall gefährdet nicht nur die Informationssicherheit, sondern schädigt auch die öffentliche Reputation der jeweiligen Institution, von der das Poster stammt.

M 1.33 Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Benutzer

Benutzer mobiler IT-Systeme wie Laptops, Mobiltelefone, Smartphones, Tablets oder PDAs müssen darauf achten, dass sie die Geräte auch außerhalb des Unternehmens sicher aufbewahren. Hierfür können nur einige Hinweise gegeben werden, die bei der mobilen Nutzung zu beachten sind:

- Mobile Endgeräte sollten möglichst nicht unbeaufsichtigt bleiben.
- Wird ein Laptop, Smartphone, Tablet oder PDA in einem Kraftfahrzeug aufbewahrt, so sollte das Gerät von außen nicht sichtbar sein. Das Abdecken des Gerätes oder das Einschließen in den Kofferraum bieten Abhilfe. Ein mobiles IT-System kann einen hohen Wert darstellen, der potenzielle Diebe anlockt, zumal tragbare IT-Systeme leicht veräußert werden können.
- Wird das mobile IT-System in fremden Büroräumen benutzt, so ist auch bei kurzzeitigem Verlassen des Raumes dieser zu verschließen oder das Gerät mitzunehmen. Wird der Raum für längere Zeit verlassen, sollte zusätzlich das mobile IT-System ausgeschaltet oder ein Zugriffsschutz aktiviert werden, um eine unerlaubte Nutzung zu verhindern.
- In Hotelräumen sollte das mobile IT-System nicht unbeaufsichtigt herumliegen. Wird das Gerät in einen Schrank eingeschlossen, hält das zumindest Gelegenheitsdiebe ab.
- Einige neuere Geräte können zusätzlich durch ein Schloss gesichert werden. Ein Dieb braucht dann Werkzeug, um es zu stehlen.
- Ein mobiles IT-System sollte nie extremen Temperaturen ausgesetzt werden. Insbesondere der Akku und das Display können anderenfalls beschädigt werden. Auch sollten weder IT-Geräte noch Akkus in geparkten Autos zurückgelassen werden, wenn die Außentemperatur extrem hoch oder niedrig ist.
- Ebenso sollten mobile Endgeräte vor Umwelteinflüssen geschützt werden, die diese schädigen können, also beispielsweise vor Feuchtigkeit durch Regen oder Spritzwasser.
- Mobile Endgeräte sind nicht unzerstörbar, daher sollten sie auch bei kürzeren Transportwegen möglichst stoßgeschützt befördert werden. Bei Laptops sollte beispielsweise das Gerät zusammengeklappt werden, da sowohl die Scharniere als auch der Bildschirm bei einem Sturz leicht beschädigt werden können. Grundsätzlich ist es immer empfehlenswert, für den Transport ein schützendes Behältnis zu verwenden. Beispielsweise haben viele Taschen und Rucksäcke für mobile Endgeräte eigene Fächer mit Polsterungen. Nach Möglichkeit sollten solche Taschen und Rucksäcke bereitgestellt und genutzt werden.

Es ist empfehlenswert, für die Benutzer mobiler IT-Systeme ein Merkblatt zu erstellen, das die wichtigsten Hinweise und Vorsichtsmaßnahmen zur geeigneten Aufbewahrung und zum sicheren Transport der Geräte enthält.

Prüffragen:

- Werden die Benutzer von tragbaren IT-Systemen auf die geeignete Aufbewahrung hingewiesen?

M 1.34 Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Benutzer

Tragbare IT-Systeme wie Laptops, PDAs oder Mobiltelefone sind durch ihre Bauform immer beliebte Ziele für Diebstähle. Daher müssen sie auch dann sicher aufzubewahrt werden, wenn sie sich im vermeintlichen sicheren Büro befinden. Aus diesem Grund sind natürlich die in Baustein B 2.3 *Büroraum / Lokaler Arbeitsplatz* beschriebenen Maßnahmen zu beachten. Da ein tragbares IT-Systeme jedoch besonders leicht zu transportieren und zu verbergen ist, sollte das Gerät außerhalb der Nutzungszeiten weggeschlossen werden, also beispielsweise in einem Schrank oder Schreibtisch verschlossen werden oder angekettet werden.

Prüffragen:

- Werden tragbare IT-Systeme außerhalb der Nutzungszeiten gegen Diebstahl gesichert bzw. verschlossen aufbewahrt?

M 2.9 Nutzungsverbot nicht freigegebener Hard- und Software

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Leiter IT

Es ist durchaus üblich, dass Mitarbeiter eigene Hard- und Software wie beispielsweise private Mobiltelefone, PDAs oder Kameras auch dienstlich oder zumindest in den Diensträumen verwenden. Da die Nutzung von zusätzlicher Hardware über Standardschnittstellen wie USB und weitgehende Plug-and-Play-Funktionalität immer einfacher wird, muss deren Einsatz geregelt werden. Die Informationssicherheit kann dabei beispielsweise durch externe USB-Speichermedien (z. B. Festplatten, Memory-Sticks) oder private PDAs beeinträchtigt werden.

Es muss daher geregelt sein, wie Hard- und Software abgenommen, freigegeben, installiert bzw. benutzt werden darf. Maßnahmen, die zu diesem Zweck umgesetzt werden sollten, sind z. B.: M 2.216 *Genehmigungsverfahren für IT-Komponenten*, M 2.62 *Software-Abnahme- und Freigabe-Verfahren* bzw. Baustein B 1.10 *Standardsoftware* und M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*.

Das Einspielen bzw. Benutzen nicht freigegebener Hard- und Software muss verboten und außerdem durch technische Möglichkeiten soweit möglich verhindert werden. Bei den meisten Betriebssystemen kann dies durch Einschränkung der Benutzerumgebung erreicht werden. Damit soll verhindert werden, dass Programme mit unerwünschten Auswirkungen eingebracht werden. Zusätzlich soll verhindert werden, dass das System über den festgelegten Funktionsumfang hinaus unkontrolliert genutzt wird. Es kann sinnvoll sein (z. B. um Makro-Viren vorzubeugen), dieses Nutzungsverbot auch auf das Einspielen privater Daten auszudehnen.

Bei Software ist zu dokumentieren, welche Versionen ausführbarer Dateien freigegeben wurden (inklusive Erstellungsdatum und Dateigröße). Die freigegebenen Programme sind regelmäßig auf Veränderungen zu überprüfen.

Nutzungsverbote nicht freigegebener Hard- und Software sollten schriftlich fixiert werden, alle Mitarbeiter sind darüber zu unterrichten. Ausnahmeregelungen sollten einen Erlaubnisvorbehalt vorsehen.

Prüffragen:

- Existiert eine Regelung zur Abnahme, Freigabe, Installation und Nutzung von Hard- und Software?
- Wurden alle Mitarbeiter über das Verbot für die Nutzung nicht freigegebener Hard- und Software informiert?
- Wird das Nutzungsverbot allen Mitarbeitern zur Kenntnis gebracht?
- Bei Ausnahmeregelungen: Wird ein Erlaubnisvorbehalt vorgesehen?
- Wird die Nutzung nicht freigegebener Hard- und Software technisch soweit möglich unterbunden?
- Werden freigegebene Programme regelmäßig auf Veränderungen überprüft?

M 2.163 Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter
Verantwortlich für Umsetzung: Administrator, Verantwortliche der einzelnen Anwendungen

Bevor eine Entscheidung getroffen werden kann, welche kryptographischen Verfahren und Produkte eingesetzt werden sollen, müssen eine Reihe von Einflussfaktoren ermittelt werden. Dazu können die Systemadministratoren und die Verantwortlichen der einzelnen IT-Systeme bzw. IT-Anwendungen befragt werden. Die Ergebnisse sind nachvollziehbar zu dokumentieren.

Für sämtliche in M 2.162 *Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte*festgelegten Speicherorte und Übertragungsstrecken sind folgende Einflussfaktoren zu ermitteln:

Sicherheitsaspekte

- Welcher Schutzbedarf besteht bzw. welches Sicherheitsniveau gilt es zu erreichen?
- Welche kryptographischen Funktionen sind dafür notwendig (Verschlüsselung, Integritätsschutz, Authentizität und/oder Nichtabstreitbarkeit)?
- Angreiferpotential: Mit welchen Angreifern wird gerechnet (zeitliche und finanzielle Ressourcen, technische Fähigkeiten)?

Die Antworten auf diese Fragen ergeben sich aus M 2.162 *Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte*.

Technische Aspekte

Der Betrieb von weitverzweigten IT-Infrastrukturen mit ihrer Vielzahl von Einzelkomponenten und Spezialeinrichtungen (Netzknoten, Server, Datenbanken, etc.) macht ein ebenfalls weitverzweigtes Sicherheitssystem mit mehreren Funktionseinheiten (Sicherheitsmanagement, Sicherheitsserver, Sicherheitsanwenderkomponente, etc.) erforderlich. In der Regel müssen dabei Systembetrachtungen angestellt werden, die nicht nur auf die eigentlichen Funktionalitäten abzielen, sondern auch bauliche und organisatorische Aspekte einbeziehen. Auch in Bezug auf die konkrete technische Platzierung von Sicherheitskomponenten sowie deren Integration in Nicht-Sicherheitskomponenten gilt es zu differenzieren, da dies einen unmittelbaren Einfluss auf die Implementierung der Sicherheitsfunktionen, auf die notwendige Unterstützung durch die Betriebssysteme, die Aufwände und den Kostenfaktor und nicht zuletzt auf die erreichbare Sicherheit hat. Ganz entscheidend für die Sicherheitsbewertung ist der Umstand, an welchen geographischen Lokalitäten und in welchen Ebenen des Protokollstacks die jeweiligen Sicherheitsdienste realisiert sind und wie diese in die Prozesse des zu schützenden IT-Systems eingebunden sind. Somit ergeben sich als Fragen:

- Umfeldschutz: Welchen Schutz bietet das Umfeld, beispielsweise durch infrastrukturelle Sicherheitsmaßnahmen wie Zutrittskontrolle, organisatorische, personelle und technische Maßnahmen?
- IT-Systemumfeld: Welche Technik wird eingesetzt, welche Betriebssysteme, etc.?
- Datenvolumen: Welches Datenvolumen ist zu schützen?
- Häufigkeit: Wie häufig besteht Verschlüsselungsbedarf?

- Performance: Wie schnell müssen kryptographische Funktionen arbeiten (Offline, Online-Rate)?

Personelle und organisatorische Aspekte
- Benutzerfreundlichkeit: Benötigen die Benutzer für die Bedienung kryptographische Grundkenntnisse? Behindert der Einsatz eines Kryptoprodukts die Arbeit?
- Zumutbarkeit: Wie viel Belastung durch zusätzliche Arbeit ist für Benutzer zumutbar (Arbeitszeit, Wartezeit)?
- Zuverlässigkeit: Wie zuverlässig werden die Benutzer mit der Kryptotechnik umgehen?
- Schulungsbedarf: Inwieweit müssen die Benutzer geschult werden?
- Personalbedarf: Ist zusätzliches Personal erforderlich, z. B. für Installation, Betrieb, Schlüsselmanagement?
- Verfügbarkeit: Kann durch den Einsatz eines Kryptoprodukts die Verfügbarkeit reduziert werden?

Wirtschaftliche Aspekte
- Finanzielle Randbedingungen: Wie viel darf der kryptographische Schutz kosten? Wie hoch sind die
  - einmaligen Investitionen,
  - laufenden Kosten, inklusive der Personalkosten,
  - Lizenzgebühren?
- Investitionsschutz: Sind die geplanten kryptographischen Verfahren bzw. Produkte konform zu bestehenden Standards? Sind sie interoperabel mit anderen Produkten?

Key-Recovery

Falls die zur Verschlüsselung benutzten Schlüssel verloren gehen, sind auch die damit geschützten Daten verloren, sofern die unverschlüsselten Daten nicht zusätzlich an anderer Stelle vorliegen. Viele Kryptoprodukte bieten daher Funktionen zur Datenwiedergewinnung für solche Fälle an. Bevor solche Funktionen eingesetzt werden, sollte man sich auch deren Risiken klar machen: Wenn dadurch vertrauliche Schlüssel wiederhergestellt werden können, muss sichergestellt sein, dass dies nur Berechtigte können. Wenn es möglich ist, ohne Wissen des Original-Schlüsselbenutzers auf dessen Daten zuzugreifen, hat dieser keine Möglichkeit, böswillige Manipulationen zu beweisen. Der Einsatz von Key-Recovery-Mechanismen führt auch häufig aufgrund des entgegengebrachten Misstrauens zu Vorbehalten innerhalb des eigenen Unternehmens bzw. Behörde, aber auch bei den Kommunikationspartnern. Bei der Datenübertragung sollte daher generell auf Key-Recovery verzichtet werden. Hierfür gibt es auch keine Notwendigkeit, da beim Schlüssel- oder Datenverlust diese einfach noch einmal ausgetauscht werden können. Bei der lokalen Speicherung von Daten sollte der Einsatz sorgfältig überlegt werden (siehe auch M 6.56 *Datensicherung bei Einsatz kryptographischer Verfahren*). Unter den Hilfsmitteln zum IT-Grundschutz befindet sich ein Artikel zu Möglichkeiten und Risiken von Key-Recovery.

Lebensdauer von kryptographischen Verfahren

Kryptographische Verfahren und Produkte müssen regelmäßig daraufhin überprüft werden, ob sie noch dem Stand der Technik entsprechen. Die verwendeten Algorithmen können durch neue technische Entwicklungen, z. B. schnellere, billigere IT-Systeme, oder durch neue mathematische Erkenntnisse zu schwach werden. Die eingesetzten kryptographischen Produkte können Implementierungsfehler aufweisen. Bereits bei der Auswahl kryptographischer Verfahren sollte daher eine zeitliche Grenze für deren Einsatz festgelegt wer-

den. Zu diesem Zeitpunkt sollte noch einmal gründlich überdacht werden, ob die eingesetzten Kryptomodule noch den erwarteten Schutz bieten.

Gesetzliche Rahmenbedingungen

Beim Einsatz kryptographischer Produkte sind diverse gesetzliche Rahmenbedingungen zu beachten. In einigen Ländern dürfen beispielsweise kryptographische Verfahren nicht ohne Genehmigung eingesetzt werden. Daher muss untersucht werden (siehe M 2.165 *Auswahl eines geeigneten kryptographischen Produktes*),

- ob innerhalb der zum Einsatzgebiet gehörenden Länder Einschränkungen beim Einsatz kryptographischer Produkte zu beachten sind (innerhalb Deutschland gibt es keinerlei Einschränkungen) und
- ob für infrage kommende Produkte Exportbeschränkungen beachtet werden müssen.

Es gibt allerdings nicht nur Maximalanforderungen, sondern auch Minimalanforderungen an die verwendeten kryptographischen Algorithmen oder Verfahren. So müssen z. B. bei der Übermittlung von personenbezogenen Daten Verschlüsselungsverfahren mit ausreichender Schlüssellänge eingesetzt werden.

Technische Lösungsbeispiele:

Im Folgenden finden sich einige Anwendungsbeispiele zu den verschiedenen Einsatzfeldern für kryptographische Verfahren.

Beispiel 1: Festplattenverschlüsselung

Die auf einem Speicherbaustein, z. B. einer Festplatte oder einem Flashspeicher eines stationären oder mobilen Clients (wie z. B. ein PDA, Smartphone, Tablet, Laptop oder PC) gespeicherten sensiblen Daten sollen so geschützt werden, dass

- der Computer nur von autorisierten Benutzern gebootet werden kann,
- nur autorisierte Benutzer Zugriff auf die gespeicherten Daten erhalten,
- die gespeicherten Daten bei abgeschaltetem Computer - auch im Falle des Diebstahls - hinreichend vor Kenntnisnahme durch Unberechtigte geschützt sind.

Dabei soll der Computer gegen die folgenden Bedrohungen geschützt werden:

- Unbefugte Kenntnisnahme der gespeicherten Daten
- Manipulation der gespeicherten Daten
- Manipulation des Kryptosystems

Im Vordergrund soll hier der Schutz der Vertraulichkeit stehen.

Bei Diebstahl bzw. Verlust des Computers oder des Speicherbausteins steht dem Angreifer sehr viel Zeit für die unbefugte Kenntnisnahme zur Verfügung. Eine Schutzmaßnahme muss auch bei solchen Langzeitangriffen die Vertraulichkeit der gespeicherten Daten gewährleisten.

Als Schutzmaßnahme soll daher ein Produkt mit Boot-Schutz und Festplattenverschlüsselung eingesetzt werden. Auf dem Markt sind verschiedene Lösungen verfügbar.

Grundsätzlich sollte im eingesetzten Produkt ein etablierter Kryptoalgorithmus (z. B. AES) mit einer hinreichenden Schlüssellänge (128 Bit oder mehr) in einem verlässlichen Betriebsmodus (z. B. CBC, OFB oder GCM, kein XOR) implementiert sein.

Zum Einsatz kann entweder eine Verschlüsselungs-Software (Lösung A), eine Hardware-Verschlüsselungskomponente (Lösung B) oder eine Kombination aus Hardware- und Software-Komponente (Lösung C) kommen. Lösung C wird typischerweise aus einer Verschlüsselungs-Software in Kombination mit einem Hardware-Token, z. B. einer Chipkarte oder einem USB-Stick, zur Zugangskontrolle bestehen. Welche Lösung gewählt werden sollte, hängt von verschiedenen Entscheidungskriterien ab:

- Sicherheit
  Je nachdem, auf welcher Betriebssystem-Plattform Verschlüsselung betrieben wird, stößt eine Software-Lösung (Lösungen A oder C) unweigerlich an Grenzen. Kann kein sicheres Betriebssystem mit strikter Task- und Speicherbereichs-Trennung vorausgesetzt werden (bisher ist das bei keinem Betriebssystem sicher nachgewiesen!), muss der während der Ver- bzw. Entschlüsselung verwendete Schlüssel zumindest kurzzeitig ungeschützt im Arbeitsspeicher des Computers gehalten werden. Die Vertraulichkeit des Schlüssels ist somit möglicherweise nicht mehr sichergestellt. Hardware-Verschlüsselungskomponenten (Lösung B) können eventuell mehr bieten. Der Schlüssel kann in die Hardware-Komponente geladen und dort - gegen Auslesen gesichert - gespeichert werden. Der Schlüssel wird die Hardware-Komponente nicht mehr verlassen und ist vor Ausspähversuchen geschützt. Er kann nur durch berechtigte Benutzer mittels Besitz und Wissen (z. B. Chipkarte und Passwort) aktiviert werden. Wichtig sind weitere Aspekte, wie die Art und Weise der Einbindung in das Computer-System. Die Verschlüsselungs-Hardware sollte idealerweise so eingebunden werden, dass sie die gesamte Festplatte zwangsweise verschlüsselt und durch Angriffe nicht unbemerkt abgeschaltet bzw. umgangen werden kann. Werden im Gegensatz dazu lediglich einzelne Dateien verschlüsselt, besteht die Gefahr, dass die Inhalte dieser Dateien unkontrollierbar zumindest teilweise zusätzlich im Klartext auf die Festplatte geschrieben werden (z. B. in den Auslagerungsdateien verschiedener Betriebssysteme oder in Backup-Dateien).
- Performance (Geschwindigkeit der ausführbaren Programme)
  Software-Verschlüsselung nutzt die Systemressourcen des Computers, belastet also die CPU und benötigt Arbeitsspeicher. Vor allem bei der Verschlüsselung der gesamten Festplatte kann die Performance des Computers sinken. Hardware-Komponenten mit eigenem Prozessor können die Verschlüsselung ohne Belastung der CPU und somit ohne nennenswerten Performanceverlust durchführen. Hier ist je nach Bauart die Durchsatzrate der verwendeten Verschlüsselungs-Hardware mitentscheidend.
- Organisatorischer und personeller Aufwand (Administration, Schlüsselmanagement, Schulung etc.)
  Der organisatorische bzw. personelle Aufwand ist von der Umsetzung der Sicherheitspolitik und dem "Komfort" der Verschlüsselungskomponenten abhängig. Generelle Entscheidungskriterien für oder gegen eine der drei Lösungen können nicht allgemeingültig formuliert werden.
- Wirtschaftlichkeit (Anschaffung, Schulungs-/Administrationskosten, ...)
  Eine allgemeine Aussage zur Wirtschaftlichkeit ist schwierig. Betrachtet man nur die Anschaffungskosten, so werden Software-Lösungen oft preiswerter sein als Hardware-Lösungen. Kalkuliert man dagegen auch die Schäden ein, die durch unzureichenden Schutz auf längere Sicht entstehen können, kann sich im Vergleich die Investition in sicherere und vielleicht teurere Lösungen lohnen. Wirtschaftliche Nachteile können u. U. durch Performanceverlust des Computer-Systems entstehen.
- Restrisiken (Betriebssystem, Kompromittierung des Festplattenschlüssels etc.)

Bei der Auswahl der geeigneten Verschlüsselungskomponente spielt die Restrisikobetrachtung eine wesentliche Rolle. Es stellen sich u. a. die Fragen:

- Welche Restrisiken können in Kauf genommen werden?
- Welche Restrisiken werden durch andere Maßnahmen (z. B. materielle oder organisatorische Maßnahmen) minimiert?

Es können sich durchaus mehrere tragbare Lösungsmöglichkeiten durch die Kombination verschiedener Maßnahmen ergeben.

Beispiel 2: E-Mail-Verschlüsselung

Werden sensible Informationen (z. B. Firmengeheimnisse) per E-Mail über ungesicherte Netze ausgetauscht, sind Mechanismen zum Schutz der Vertraulichkeit und für die Gewähr der Authentizität von Nachrichten erforderlich.

Grundsätzlich bieten sich zwei Möglichkeiten, die sensiblen Daten zu schützen.

1. Die zu schützenden Informationen werden in einer Datei gespeichert, die Datei wird dann mit einem Dateiverschlüsselungsprogramm verschlüsselt und die verschlüsselte Datei wird der E-Mail als Anhang beigefügt. Der eigentliche Text der E-Mail bleibt dabei ungesichert.
2. Die gesamte E-Mail (Text und ggf. Anhänge) wird mithilfe eines speziellen E-Mail-Verschlüsselungsprogramms verschlüsselt.

Möglichkeit 2 setzt voraus, dass beim Benutzer ein E-Mail-Programm (z. B. Outlook, Kontact oder Thunderbird) installiert ist, welches die Einbindung eines E-Mail-Verschlüsselungsprogramms als Plugin ermöglicht. Im Falle, dass der Benutzer einen webbasierten E-Mail-Client verwendet, kommt nur Möglichkeit 1 in Frage.

Voraussetzung ist hierbei natürlich, dass nicht nur der Sender der E-Mail, sondern auch der Empfänger über ein kompatibles Verschlüsselungsprogramm verfügt.

Beide genannten Möglichkeiten bieten Ende-zu-Ende-Sicherheit zwischen Sender und Empfänger. Der Sender entscheidet dabei in der Regel, welche Informationen er für sensibel und schützenswert hält. In vielen Fällen (je nach eingesetztem Verschlüsselungsprogramm) sind Sender und Empfänger auch für das Schlüsselmanagement verantwortlich. Die Entscheidung des Senders, welche Daten er verschlüsselt und das Schlüsselmanagement werden ihm abgenommen, wenn grundsätzlich alle E-Mails, die beispielsweise zwischen den Liegenschaften einer Institution versendet werden, automatisiert vom E-Mail-Server ver- bzw. entschlüsselt werden. Das Schlüsselmanagement beschränkt sich dann personell auf die IT-Administratoren der Institution, und die E-Mails sind lediglich zwischen Sender und E-Mail-Server bzw. E-Mail-Server und Empfänger ungeschützt, also auf Strecken, die im Allgemeinen innerhalb einer Liegenschaft und somit in einem gesicherten Bereich verlaufen.

Selbstverständlich sind beide Methoden (Ende-zu-Ende-Verschlüsselung und automatisierte Verschlüsselung zwischen den E-Mail-Servern) miteinander kombinierbar und erhöhen so die Sicherheit.

Werden die E-Mails mittels eines Datei- oder eines E-Mail-Verschlüsselungsprogramms gesichert, stellt sich die Wahl zwischen einem Programm, welches mit symmetrischen oder mit asymmetrischen Mechanismen arbeitet (siehe M 3.23 *Einführung in kryptographische Grundbegriffe*). In jedem Fall sollte ein Produkt eines namhaften Herstellers verwendet werden, welches mit

etablierten und (auch aus Interoperabilitätsgründen) standardisierten Verfahren arbeitet. Auch Open-Source-Produkte bieten häufig eine gute Alternative. Produkte, die vollmundig mit "beweisbarer hunderprozentiger Sicherheit" werben, sind meist mit Vorsicht zu genießen.

Beide Arten, symmetrisch und asymmetrisch, bieten Vor- und Nachteile.

Verschlüsselungsprogramme mit symmetrischen Mechanismen

Ein symmetrisches Verfahren bietet sich beispielsweise an, wenn sensible Daten innerhalb eines kleinen Arbeitskreises ausgetauscht werden sollen. Der notwendige Schlüssel kann etwa auf einer konstituierenden Sitzung des Arbeitskreises ad hoc erzeugt und an die Mitglieder verteilt werden - ein aufwändiges Schlüsselmanagement oder gar eine Public-Key-Infrastruktur (siehe unten) sind nicht notwendig. Keinesfalls darf ein symmetrischer Schlüssel per E-Mail versendet werden.

Wird der Schlüssel für ein symmetrisches Verfahren selbstständig, d. h. ohne Verwendung eines Zufallszahlengenerators erzeugt, ist zu beachten, dass für den Schlüssel ein wesentlich höheres Sicherheitsniveau als beispielsweise für ein Passwort beim Online-Banking notwendig ist, da es für den Schlüssel keinen Fehlbedienungszähler gibt und ein Angreifer, der in Besitz einer verschlüsselten Datei kommt, beliebig viele Versuche hat, den Schlüssel systematisch und automatisiert zu ermitteln.

Auch einige ZIP-Programme bieten ausreichend sichere Verschlüsselungsoptionen, allerdings gibt es auch ZIP-Programme mit schlecht implementierter oder unzureichender Verschlüsselung. Bevor ZIP-Programme zur Verschlüsselung von vertraulichen Informationen genutzt werden, sollte das Sicherheitsmanagement die Güte der verwendeten Kryptoverfahren überprüfen oder entsprechende Testberichte einholen.

Verschlüsselungsprogramme mit asymmetrischen Mechanismen

Der Vorteil von asymmetrischer gegenüber symmetrischer Verschlüsselung ist, dass der Schlüssel, der zum Verschlüsseln verwendet wird, nicht geheim gehalten zu werden braucht. Deshalb wird ein asymmetrisches Verfahren auch Public-Key-Verfahren und der Schlüssel zum Verschlüsseln auch "öffentlicher Schlüssel" genannt. Die öffentlichen Schlüssel können also ruhigen Gewissens per E-Mail versendet oder in einem Verzeichnis veröffentlicht werden. Auf diese Weise können also sogar persönlich nicht miteinander bekannte Personen vertraulich miteinander per E-Mail kommunizieren.

Allerdings muss sich der Versender einer E-Mail davon überzeugen, dass der Schlüssel, den er zum Verschlüsseln der E-Mail verwendet, tatsächlich der öffentliche Schlüssel des Empfängers ist, der öffentliche Schlüssel also authentisch ist.

Die Authentizität der öffentlichen Schlüssel kann beispielsweise durch eine Public-Key-Infrastruktur (PKI) gewährleistet werden. Bei einer PKI stellt eine vertrauenswürdige Stelle Zertifikate für die öffentlichen Schlüssel der Benutzer aus. Der Versender einer E-Mail würde dem öffentlichen Schlüssel des Empfängers nur dann trauen, wenn er ein gültiges Zertifikat besitzt. Das Ausstellen von Schlüsselzertifikaten durch die vertrauenswürdige Stelle ist unter Umständen mit zusätzlichen Kosten verbunden.

Steht keine PKI zur Verfügung oder gehören Sender und Empfänger unterschiedlichen PKIs an, muss sich der Sender auf andere Weise von der Echtheit des öffentlichen Schlüssels überzeugen. Eine Möglichkeit, dies zu tun, ist,

den Empfänger telefonisch zu kontaktieren und den sogenannten Fingerabdruck des Schlüssels (das ist ein kryptographischer Hashwert des Schlüssels) zu vergleichen. Der Fingerabdruck eines öffentlichen Schlüssels lässt sich mit den gängigen asymmetrischen Verschlüsselungsprogrammen am Bildschirm anzeigen. Hierzu ist es jedoch erforderlich, dass der Sender den Empfänger am Telefon (z. B. anhand der Stimme) eindeutig identifizieren kann.

Weit verbreitet sind folgende (nicht miteinander kompatible) Standards:

- OpenPGP ("Pretty Good Privacy") und
- S/MIME (Secure Multipurpose Internet Mail Extensions).

OpenPGP wird etwa vom kommerziellen Produkt PGP und vom Open-Source-Produkt GnuPG unterstützt.

Authentizität der empfangenen E-Mail

Symmetrische Mechanismen bieten in der Regel eine implizite Gewähr für die Authentizität der empfangenen Informationen, da eine sinnvoll zu entschlüsselnde E-Mail nur von demjenigen erzeugt werden konnte, der in Besitz des Schlüssels ist.

Bei Verwendung eines asymmetrischen Verfahrens hingegen liefert die Tatsache, dass eine E-Mail korrekt entschlüsselt werden konnte, keinen Hinweis auf die Authentizität des Absenders, denn der Schlüssel, den er zum Verschlüsseln verwendet hat, ist wie gesagt öffentlich. Somit kann jeder, der Zugang zum öffentlichen Schlüssel des Empfängers hat, der potenzielle Absender gewesen sein.

Aus diesem Grunde bieten asymmetrische Verfahren dem Sender zusätzlich die Möglichkeit, eine Datei bzw. eine E-Mail elektronisch zu signieren. Um die Signatur zu prüfen, benötigt der Empfänger einen öffentlichen Signaturschlüssel des Senders. (Der öffentliche Signaturschlüssel sollte sich nach Möglichkeit vom öffentlichen Verschlüsselungsschlüssel des Senders unterscheiden. Bei vielen Produkten sind jedoch Signatur- und Verschlüsselungsschlüssel identisch.) Um die Echtheit des Signaturschlüssels zu verifizieren, wird auch hier eine PKI benötigt, oder der Empfänger muss den Fingerabdruck des Signaturschlüssels mit dem Sender abgleichen.

Prüffragen:

- Wurden die Einflussfaktoren für den Einsatz kryptographischer Verfahren und Produkte ermittelt und dokumentiert?

M 2.188 Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: IT-Sicherheitsbeauftragter, Leiter IT

Werden in einer Institution Mobiltelefone verwendet, ist dafür eine Sicherheitsrichtlinie zu erstellen, die alle umzusetzenden Maßnahmen beschreibt. Darüber hinaus sollte es für die Benutzer ein kurzes und übersichtliches Merkblatt für die sichere Nutzung von Mobiltelefonen geben. Falls technisch möglich, sollten die Anleitung für das Mobiltelefon und die Sicherheitshinweise zusätzlich auf dem Mobiltelefon gespeichert sein. Der Mitarbeiter ist auf den Speicherort hinzuweisen.

Anfallende Datenarten

Sobald ein Mobiltelefon eingeschaltet wird, meldet es sich über die nächstgelegene Basisstation beim Netzbetreiber an. Bei diesem werden Daten der SIM-Karte, die Seriennummer des Mobiltelefons und die Kennung der Basisstation, über die die Anmeldung erfolgt ist, protokolliert und gespeichert. Das erfolgt auch dann, wenn kein Gespräch geführt wird. Weiterhin wird jeder Verbindungsversuch, unabhängig vom Zustandekommen der Verbindung, gespeichert.

Die bei der Telekommunikation anfallenden Datenarten lassen sich grob in drei Gruppen untergliedern:

- Bestandsdaten (oder auch Stammdaten) sind diejenigen Daten, die in einem Dienst oder Netz dauerhaft gespeichert und bereit gehalten werden. Hierzu gehören die Rufnummer und gegebenenfalls der Name und die Anschrift des Teilnehmers, Informationen über die Art des Endgerätes, gegebenenfalls für den Anschluss jeweils verfügbare Leistungsmerkmale und Berechtigungen sowie Daten über die Zuordnung zu Teilnehmergruppen.
- Inhaltsdaten sind die eigentlichen "Nutzdaten", d. h. die übertragenen Informationen und Nachrichten.
- Verbindungsdaten geben Auskunft über die näheren Umstände von Kommunikationsvorgängen. Hierzu gehören Angaben über Kommunikationspartner (z. B. Rufnummern des rufenden und des angerufenen Anschlusses), Zeitpunkt und Dauer der Verbindung, in Anspruch genommene Systemleistungen, benutzte Anschlüsse, Leitungen und sonstige technische Einrichtungen, Dienste und - bei mobilen Diensten - die Standortkennungen der mobilen Endgeräte.

Im Folgenden werden Empfehlungen gegeben, wie diese Daten vor Missbrauch geschützt werden können.

Schutz vor Kartenmissbrauch

Das Mobiltelefon und die SIM-Karte müssen stets sicher aufbewahrt werden. Bei Dienstreisen sollten sie nicht unbeaufsichtigt gelassen werden. Insbesondere sollten sie nicht in Fahrzeugen zurückgelassen werden.

Mobiltelefone und dazu angebotene Dienstleistungen können an verschiedenen Stellen durch PINs oder Passwörter abgesichert werden. Dazu gehören:

- der Zugriff auf die SIM-Karte,
- der Zugriff auf das eigentliche Endgerät, also das Mobiltelefon,

- der Zugriff auf bestimmte Funktionen des Mobiltelefons, z. B. das Telefonbuch,
- der Zugriff auf die Mailbox, also die Anrufbeantworterfunktion, oder andere Dienstleistungen des Netzbetreibers,
- der Zugriff auf Daten beim Netzbetreiber (bei Fragen an die Hotline wegen der Abrechnung muss unter Umständen ein Kennwort genannt werden).

Alle diese Sicherheitsmechanismen sollten auch genutzt werden (siehe auch M 4.114 *Nutzung der Sicherheitsmechanismen von Mobiltelefonen*). Am wichtigsten ist dabei sicherlich der Schutz der SIM-Karte, da deren Missbrauch zu hohen finanziellen Schäden führen kann. Die persönliche Geheimzahl (PIN) darf keinesfalls zusammen mit der zum Mobiltelefon gehörigen SIM-Karte aufbewahrt werden ebenso wenig der PUK.

Bei Smartphones ist auch der Schutz des Endgerätes durch PIN oder Passwörter von entscheidender Bedeutung, da hier die Applikationen vertrauliche Daten, wie zum Beispiel Authentisierungstoken oder Passwörter, enthalten können. Daher muss ein solcher Schutz bei allen Geräten eingerichtet sein und darf sich nicht deaktivieren lassen. Ferner muss sich das Gerät automatisch (zum Beispiel nach zehn Minuten Untätigkeit) selbst sperren.

Bei Verlust der SIM-Karte sollte sofort beim Netzbetreiber eine Kartensperre veranlasst werden, um einen eventuellen Missbrauch und damit auch einen finanziellen Schaden abzuwehren (siehe M 2.189 *Sperrung des Mobiltelefons bei Verlust*).

Um die missbräuchliche Benutzung der SIM-Karte rechtzeitig zu bemerken, sollte in jedem Fall der Einzelverbindungsnachweis auf unerklärliche Gebühren und Zielrufnummern geprüft werden.

Einzelverbindungsnachweis

Der Netzbetreiber speichert die Anrufdaten für die Abrechnung. In Deutschland darf er sie nur bis zur Rechnungsstellung speichern, maximal aber 80 Tage gemäß TDSV (Telekommunikationsdienstunternehmen-Datenschutzverordnung - Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen). Es kann aber für den Kunden sinnvoll sein, dem Netzbetreiber zu erlauben, die Anrufdaten länger zu speichern, falls nachträglich Probleme mit der Rechnung auftreten.

Jeder Kunde sollte einen Einzelverbindungsnachweis verlangen, um die Mobiltelefon-Nutzung kontrollieren zu können. In Deutschland haben die Kunden das Recht auf einen kostenlosen Einzelverbindungsnachweis. Aus diesem können z. B. folgende Daten entnommen werden:

- Rechnungsdatum,
- angerufene Rufnummer (vollständig bzw. die letzten Ziffern unkenntlich),
- Beginn, Ende oder Dauer der Verbindung,
- Kosten des Gesprächs.

Alle Mitbenutzer des Telefons müssen darüber informiert werden, dass ein Einzelverbindungsnachweis beantragt wurde und welche Daten dadurch erfasst werden.

Wenn in einer Behörde bzw. einem Unternehmen zur Kostenkontrolle Einzelverbindungsnachweise geführt und ausgewertet werden, ist das Verfahren mit dem Betriebs- bzw. Personalrat und dem Datenschutzbeauftragten abzustimmen und den Benutzern bekannt zu geben.

Immer nach Erhalt der Einzelverbindungsnachweise sollte überprüft werden, ob sie korrekt sind. Hierdurch lässt sich auch ersehen, wo eventuell Kosten reduziert werden können.

Weitergabe der Rufnummer

Es kann gewählt werden, ob und welche Daten zu dem Mobiltelefon-Anschluss in öffentliche Telefonbücher eingetragen werden beziehungsweise für Abfragen über Telefonauskünfte zur Verfügung stehen. Ein solcher Eintrag ist jedoch nicht immer sinnvoll, zum Beispiel bei Mobiltelefonen aus einem Pool oder wenn die Zahl der Anrufer klein gehalten werden soll.

Wenn die Rufnummernanzeige aktiviert ist, können die Gesprächspartner (je nach Ausstattung) sehen, von welcher Telefonnummer sie angerufen werden. Dieser Dienst kann vom Netzbetreiber generell für ein Mobiltelefon an- oder abgeschaltet werden.

Rufnummernunterdrückung

Im Mobilfunk-Netz können den beteiligten Kommunikationspartnern die jeweiligen Rufnummern signalisiert werden. Wenn dies nicht gewünscht ist, sollte M 5.79 *Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung* beachtet werden.

Schutz vor Abhören von Telefonaten

Der einzige wirksame Schutz gegen das Abhören von Telefonaten ist die interoperable, netzübergreifende Ende-zu-Ende-Verschlüsselung. Da diese Verschlüsselung nur bei wenig handelsüblichen Geräten realisiert ist, kann jede Verbindung, ob im Festnetz oder im Mobilfunknetz, potenziell abgehört werden. Die Kommunikation zwischen Mobiltelefon und Basisstation wird aber in Deutschland und den meisten anderen Ländern verschlüsselt. Diese Verschlüsselung in Mobilfunknetzen ist jedoch mit entsprechendem Aufwand zu brechen und bietet daher nur mittelmäßigen Schutz.

Folgende Maßnahmen werden zum Schutz vorm Abhören empfohlen:

- Es sollte nicht immer und überall telefoniert werden. Zum Telefonieren sollte ein ungestörter Bereich aufgesucht werden (dadurch werden auch andere weniger gestört).
- Grundsätzlich sollten keine Telefongespräche mit vertraulichem Inhalt geführt werden.
- Manche Mobiltelefone zeigen auf dem Display an, wenn die Übertragung zwischen Mobiltelefon und Basisstation nicht verschlüsselt wird. Wenn diese Anzeige vorgesehen ist, sollten die Benutzer darüber informiert werden. Ab und zu sollten sie sich durch einen Blick auf das Display davon überzeugen, dass tatsächlich verschlüsselt wird. So gibt es z. B. einige Länder, in denen die Kommunikation zwischen Mobiltelefon und Basisstation nicht verschlüsselt wird.
- Es gibt auch einige wenige und verhältnismäßig teure Mobiltelefone, mit denen die Kommunikation von Ende zu Ende verschlüsselt werden kann. Dafür müssen aber beide Gesprächspartner kompatible Geräte einsetzen. Wenn häufiger hochsensitive Informationen über Mobiltelefon weitergegeben werden sollen, kann dies sinnvoll sein.
- Bei der Datenübertragung zum Beispiel von einem Laptop über ein Mobilfunknetz sollten die übertragenen Daten vorher auf dem Endgerät verschlüsselt werden. Hierzu gibt es eine Vielzahl von Programmen, die dies einfach ermöglichen. Alternativ kann für die Datenübertragung ein verschlüsselter VPN-Tunnel etabliert werden.

- Wenn Mobiltelefone bzw. SIM-Karten gewechselt werden, ist es enorm aufwendig, gezielt Telefonate abzuhören. Dies kann daher bei der Übertragung hochsensitiver Information bzw. Daten zweckmäßig sein.
- Es sollte geprüft werden, ob alle Gesprächsgebühren dem Teilnehmer in Rechnung gestellt wurden. Fehlende Gebühren für bestimmte Verbindungen können darauf hindeuten, dass abgehört wurde ebenso wie Gebühren für nicht bewusst getätigte Verbindungen.

Sensibilisierung der Benutzer

Die Benutzer von Mobiltelefonen sollten regelmäßig für die speziellen Gefährdungen der Informationssicherheit sensibilisiert werden (siehe M 2.558 *Sensibilisierung der Mitarbeiter zur Informationssicherheit bei Mobiltelefonen, Smartphones, Tablets und PDAs*).

Regelungen zur Nutzung privater Mobiltelefone

Werden private Mobiltelefone für dienstliche Zwecke benutzt, sind folgende Aspekte vorher zu regeln:

- Wer bezahlt dienstliche Gespräche und wie werden sie abgerechnet?
- Moderne Mobiltelefone beinhalten Terminkalender, Adressbücher, E Mail-Unterstützung und mehr. Um diese Funktionen sinnvoll einzusetzen, ist im Allgemeinen eine Synchronisation mit einem PC oder einem Internetdienst erforderlich. Daher muss geklärt werden, ob die Installation der dafür benötigten Hard- und Software erlaubt wird, beziehungsweise, ob dienstliche Daten mit diesen Internetdiensten verarbeitet und dort gespeichert werden dürfen.

Regelungen zur Nutzung dienstlicher Mobiltelefone

Notwendige Regeln für die Nutzung von dienstlichen Mobiltelefonen:

- Es muss geklärt werden, ob bzw. in welcher Menge Privatgespräche mit dienstlichen Mobiltelefonen geführt werden dürfen.
- Es sollte überlegt werden, die Nutzung der Mobiltelefone auf bestimmte Kommunikationspartner zu begrenzen, um zum Beispiel unnötigen Kosten vorzubeugen oder auch um die Informationsweitergabe einzuschränken (siehe M 2.42 *Festlegung der möglichen Kommunikationspartner*). Hierzu kann eine organisatorische Vorgabe erfolgen, es kann aber auch technisch geregelt werden, wie weiter unten unter den Stichworten "Anrufsperrungen" und "Geschlossene Benutzergruppe" beschrieben.
- Auch bei dienstlichen Mobiltelefonen sollten die Benutzer über die Tarifstruktur, Roaming-Abkommen und Kosten informiert werden, damit sie beispielsweise im Ausland die günstigsten Netzbetreiber auswählen können, wobei die sichersten Netzbetreiber Priorität haben.
- Die Benutzer sollten darauf hingewiesen werden, wie sie sorgfältig mit den Mobiltelefonen umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen bzw. um eine lange Lebensdauer zu gewährleisten (z. B. Akkupflege, Aufbewahrung außerhalb von Büro- oder Wohnräumen, Empfindlichkeit gegenüber zu hohen oder zu niedrigen Temperaturen).
- Die Verwaltung, Wartung und Weitergabe von Mobiltelefonen sollte geregelt werden. Hierzu empfiehlt sich die Einrichtung eines Mobiltelefon-Pools (siehe M 2.190 *Einrichtung eines Mobiltelefon-Pools*).
- Bei jedem Benutzerwechsel müssen alle benötigten PINs gesichert weitergegeben werden (siehe M 2.22 *Hinterlegen des Passwortes*).

Generelle Regelungen

Unabhängig davon, ob privat oder dienstlich angeschaffte Mobiltelefone genutzt werden, sollte der Arbeitgeber schriftlich regeln,

- dass der Fahrer in dienstlich genutzten Fahrzeugen während der Fahrt nicht ohne Freisprecheinrichtung telefonieren darf, da sonst bei einem Unfall Mithaftung droht,
- welche Daten auf dem Mobiltelefon gespeichert werden dürfen und ob für die Daten eine Datenverschlüsselung einzurichten ist,
- dass Dienstgeheimnisse nicht über das Mobiltelefon weitergegeben werden dürfen, weil Gespräche auch akustisch durch Personen in der unmittelbaren Umgebung mitgehört werden können,
- dass der Benutzer sich von der Identität seiner Gesprächspartner überzeugen sollte.

Für Endgeräte mit Zugriffsschutz sollte es eine Passwortrichtlinie geben, die die Art des Zugriffschutzes (siehe M 4.114 *Nutzung der Sicherheitsmechanismen von Mobiltelefonen*) festlegt und die gegebenenfalls Regelungen zur Ausgestaltung enthält (Länge des Passwortes etc.). Es wird meistens als unkomfortabel empfunden, nach wenigen Minuten Untätigkeit immer wieder ein langes Passwort einzugeben. Daher sollten Institutionen einen angemessenen Kompromiss zwischen Sicherheit und Komfort wählen und nicht lediglich die Passwortrichtlinie für den Arbeitsplatz-PC übernehmen.

Wird das Mobiltelefon in fremden Büroräumen vor Ort benutzt, so sind die Sicherheitsregelungen der besuchten Organisation zu beachten. Ein Mobiltelefon sollte möglichst nicht unbeaufsichtigt bleiben. Falls es in einem Kraftfahrzeug zurückgelassen werden muss, so sollte das Gerät von außen nicht sichtbar sein und ausgeschaltet werden (Power Off). Auch in fremden Räumlichkeiten wie Hotelzimmern sollte ein Mobiltelefon bei Abwesenheit nicht ungeschützt herumliegen. Alle Passwort-Schutzmechanismen sollten spätestens jetzt aktiviert werden., bevor das Gerät ausgeschaltet wird (Power Off) und in den Safe oder zumindest an einen nicht sichtbaren Ort gebracht wird (z. B. Koffer).

Im Übrigen sollten Regelungen bei Verlust des Mobiltelefons (M 2.189 *Sperrung des Mobiltelefons bei Verlust*) getroffen und den Mitarbeitern bekannt gegeben werden. Werden für moderne Mobiltelefone besondere Programme zum Orten, Löschen und Sperren des Endgerätes angeschafft, so sind die Mitarbeiter in der Bedienung dieser Programme zu schulen. Ferner müssen Regelungen geschaffen werden, wie mit zeitweise verlorenen und dann wieder gefundenen Geräten zu verfahren ist, da diese manipuliert sein könnten. Es empfiehlt sich, solche Geräte komplett zu löschen und alle relevanten Daten und Programme neu aufzuspielen.

Benutzungsverbot von Mobiltelefonen

Es sollte überlegt werden, ob es in allen oder bestimmten Bereichen einer Institution verboten werden sollte, Mobiltelefone zu benutzen oder mitzuführen (siehe M 5.80 *Schutz vor Abhören der Raumgespräche über Mobiltelefone* über Mobiltelefone). Dies kann zum Beispiel für Besprechungsräume sinnvoll sein. Wenn die Sicherheitsleitlinie der Institution es nicht zulässt, dass Mobiltelefone mitgebracht werden, muss an allen Eingängen deutlich darauf hingewiesen werden. Dies sollte dann auch regelmäßig kontrolliert werden.

Durch Mobiltelefone können unter Umständen auch andere technische Geräte in ihrer Funktion beeinträchtigt werden. So können beispielsweise empfindliche IT Systeme in Serverräumen oder auch auf Intensivstationen durch Mobil-

telefone gestört werden. Mögliche Störungen sind umso unwahrscheinlicher, je geringer die Sendeleistung des Mobiltelefons ist beziehungsweise je weiter dieses entfernt ist.

Bei IT Systemen, auf denen sensitive Daten verarbeitet werden oder die an ein Rechner-Netz angebunden sind, sollten Verbindungen über ein Mobilfunknetz nur mit VPN-Techniken zugelassen werden (siehe M 5.81 Sichere Datenübertragung über Mobiltelefone).

Telefonbuch

Im Telefonbuch eines Mobiltelefons können Rufnummern und zugehörige Namen oder weitere Details gespeichert werden, und zwar im Endgerät, also dem Mobiltelefon, einer eventuell vorhandenen zusätzlichen Speicherkarte oder auf der SIM-Karte. Das Telefonbuch auf dem Endgerät beziehungsweise der Speicherkarte hat für gewöhnlich eine größere Kapazität und erlaubt mehr Zusatzdaten als der Speicher der SIM-Karte, zum Beispiel Anschrift, Faxnummer, E-Mail-Adresse und weitere Notizen, sodass die Inhalte aus SIM-Karte und Endgerät nicht übereinstimmen müssen. Wo die Telefonnummern bevorzugt gespeichert werden sollen, hängt von verschiedenen Faktoren ab, beispielsweise wie einfach die Daten auf anderen Medien gesichert werden können (siehe M 6.72 *Ausfallvorsorge bei Mobiltelefonen*) oder wie hoch der Schutzbedarf der Informationen ist. Denn je nach Speicherort sind die Daten durch unterschiedliche Mechanismen geschützt: Liegen sie auf der SIM-Karte, kann auf die Informationen nur durch die korrekte PIN zugegriffen werden. Werden die Daten auf dem Endgerät oder einer externen Speicherkarte im Endgerät gespeichert, liegen sie in der Regel im Klartext vor und können nur durch zusätzliche Verschlüsselung geschützt werden. In diesem Fall bietet es sich an, den Passwortschutz für das Endgerät mit einer Verschlüsselung zu kombinieren.

Im Telefonbuch sollten alle wichtigen Rufnummern gespeichert werden, damit diese jederzeit verfügbar sind. Die gespeicherten Rufnummern sollten gelegentlich kontrolliert werden, ob sie noch korrekt beziehungsweise notwendig sind. Alle Rufnummern sollten so gespeichert werden, dass sie weltweit angerufen werden können, das heißt inklusive Landes- und Ortsvorwahl. Da nur der Ländercode international abgestimmt ist, nicht die Null, sollte dazu jede Rufnummer mit einem "+" am Anfang, gefolgt vom Ländercode (zum Beispiel +49 für Deutschland), Ortsvorwahl ohne führende Null und dann Telefonnummer eingegeben werden. Ein Eintrag könnte also wie folgt aussehen: +4922895825369 GS-Hotline.

Wenn das Mobiltelefon von mehreren Benutzern eingesetzt wird, sollte das Telefonbuch vor der Übergabe gelöscht und das Telefonbuch des neuen Benutzers aufgespielt werden. Die Telefonbücher aller Benutzer müssen dafür zentral vom Verwalter des Mobiltelefon-Pools gespeichert werden (siehe M 2.190 *Einrichtung eines Mobiltelefon-Pools*).

Anrufbeantworter

Über die Netzbetreiber kann im Allgemeinen zu einem Mobiltelefon eine Anrufbeantworter-Funktionalität aktiviert werden. Eingehende Anrufe werden dabei beim Netzbetreiber in einer so genannten Mail- oder Mobilbox gespeichert, die vom Benutzer jederzeit abgerufen werden kann. Dies kann sehr sinnvoll sein, verursacht aber in der Regel zusätzliche Kosten.

Der Zugriff auf die Mailbox sollte durch eine PIN geschützt werden. Auch wenn die Mailbox nicht genutzt wird, sollte die voreingestellte PIN schnell geändert werden, um eine Fremdnutzung zu verhindern.

Eingegangene Aufzeichnungen sollten regelmäßig abgehört werden. Alle Benutzer müssen darüber informiert werden, wie dies funktioniert.

Rufumleitung

Mit der Funktion Rufumleitung können eingehende Anrufe auf die Mailbox oder auf eine andere Rufnummer weitergeleitet werden. Dafür gibt es mehrere Varianten:

- Es können alle eingehenden Anrufe weitergeleitet werden.
- Anrufe werden nur dann weitergeleitet, wenn besetzt ist.
- Anrufe werden nur dann weitergeleitet, wenn der Anschluss nicht erreichbar ist, z. B. wegen eines Funklochs oder weil das Mobiltelefon ausgeschaltet ist.
- Es können bestimmte Arten von Anrufen weitergeleitet werden, z. B. Sprach-, Daten- oder Faxanrufe.
- Viele Smartphones gestatten sogar eine telefonnummerngenaue Einrichtung von Weiterleitungen auf andere Anschlüsse oder den Anrufbeantworter.

Dabei sollte allerdings berücksichtigt werden, dass Rufumleitungen auf Festnetzanschlüsse hohe Kosten verursachen können, da der Angerufene die Weiterleitungskosten selbst tragen muss.

Anrufsperrungen

Über Anrufsperrungen können Gespräche zu oder von einer Rufnummer gesperrt werden. Diese Funktionen werden über den Netzbetreiber zur Verfügung gestellt und können über das Mobiltelefon geändert werden. Dafür ist im Allgemeinen ein Passwort erforderlich. Viele Smartphones können Anrufsperrungen ohne Unterstützung des Netzbetreibers durch lokale Software realisieren, die in der Regel viel feinteiliger konfiguriert werden kann.

Anrufsperrungen können sinnvoll sein, wenn das Mobiltelefon an Dritte weitergegeben werden soll. Es gibt verschiedene Möglichkeiten von Anrufsperrungen:

- Sperren aller abgehenden Anrufe (Notrufnummern sind davon ausgenommen)
- Sperren aller abgehenden internationalen Anrufe
- Sperren aller abgehenden internationalen Anrufe außer ins Heimatland
- Sperren aller ankommenden Anrufe
- Sperren aller ankommenden Anrufe bei Aufenthalt im Ausland
- Sperren bestimmter ankommender oder abgehender Anrufe

Ob und welche Art von Anrufsperrungen gewählt werden sollte, hängt von der Einsatzart des jeweiligen Mobiltelefons ab.

Geschlossene Benutzergruppe

Über den Dienst "Geschlossene Benutzergruppe" kann die Kommunikation auf die Mitglieder dieser Gruppe beschränkt werden (siehe auch M 5.47 *Einrichten einer Closed User Group*).

Die Gruppenmitglieder müssen beim Netzbetreiber eingetragen werden. Die Option "Geschlossene Benutzergruppe" kann am Mobiltelefon aktiviert wer-

den. Geschlossene Benutzergruppen sind beispielsweise sinnvoll, um die Datenübertragung über Mobilfunk einzuschränken. Auf vielen Smartphones können solche Benutzergruppen in der Regel auch lokal, ohne Einbindung des Netzbetreibers, umgesetzt werden.

Prüffragen:

- Existiert eine aktuelle Sicherheitsrichtlinie für die Mobiltelefon-Nutzung?
- Wie wird die Einhaltung der Sicherheitsrichtlinie für die Mobiltelefon-Nutzung überprüft?
- Besitzt jeder Mobiltelefon-Benutzer ein Exemplar dieser Mobiltelefon-Richtlinie oder ein Merkblatt mit einem Überblick über die wichtigsten Sicherheitsmechanismen?
- Ist die Sicherheitsrichtlinie für die Mobiltelefon-Nutzung Inhalt der Schulungen zu IT-Sicherheitsmaßnahmen?
- Wurden die Benutzer von Mobiltelefonen auf die Regelungen hingewiesen, die von ihnen einzuhalten sind?
- Werden die Benutzer von Mobiltelefonen auf deren geeignete Aufbewahrung hingewiesen?

M 2.189 Sperrung des Mobiltelefons bei Verlust

Verantwortlich für Initiierung: Benutzer, IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Benutzer

Bei Verlust der SIM-Karte bzw. des Mobiltelefons trägt der Inhaber der SIM-Karte die Kosten für eine missbräuchliche Nutzung des Mobiltelefonanschlusses. Daher sollte die SIM-Karte beim Netzbetreiber sofort gesperrt werden, um einen eventuellen Missbrauch, und damit einen zusätzlichen finanziellen Schaden, abzuwehren.

Darüber hinaus sollte die PIN-Abfrage der SIM-Karte stets aktiviert sein (siehe M 4.114 *Nutzung der Sicherheitsmechanismen von Mobiltelefonen*). Bei einem Diebstahl oder Verlust verhindert dies, dass die SIM-Karte von einem Unbefugten benutzt oder ausgewertet werden kann. Bei deaktivierter SIM PIN kann ein nicht legitimierter Nutzer die SIM PIN aktivieren oder die SIM durch mehrfache Falscheingaben unbrauchbar machen. Die PIN wird allerdings nur abgefragt, wenn das Mobiltelefon eingeschaltet wird (Power On). Wird ein eingeschaltetes Mobiltelefon gestohlen, kann hiermit zumindest solange missbräuchlich telefoniert werden, bis der Akku leer ist.

Für Smartphones gibt es auf dem Markt Software zum Diebstahlschutz, die es erlaubt, das Mobiltelefon per GPS-Empfänger oder Mobilfunkzellen zu orten, die Daten auf dem Gerät zu löschen oder das Gerät vollständig zu sperren. Gegebenenfalls können sogar automatisierte Nachrichten an den IT-Betrieb über die Sperrung oder den Aufenthaltsort eines Gerätes versandt werden, wenn beispielsweise die SIM-Karte ausgetauscht wurde. Viele dieser Programme gestatten es auch Nachrichten an das Telefon zu senden oder aktivieren lediglich eine Displayanzeige, die den Finder bitten, die Telefonnummer des IT-Betriebs anzurufen oder das Gerät an einer bestimmten Adresse abzugeben. Die Anschaffung einer solchen Software kann sich schnell bezahlt machen, wenn ein verloren gegangenes Smartphone schneller zurückgegeben werden kann und die Daten besser vor Dieben geschützt sind. Auf der anderen Seite muss permanent das GPS aktiviert und eine Mobilfunk-Verbindung aufgebaut sein. Dies kann zu einem erhöhen Akkuverbrauch führen, zusätzlichen kann die notwendige Geräteortung durch Dritte missbraucht werden (siehe M 5.78 *Schutz vor Erstellen von Bewegungsprofilen bei der Mobiltelefon-Nutzung* und M 4.115 *Sicherstellung der Energieversorgung von Mobiltelefonen*).

Um rechtzeitig zu bemerken, dass die SIM-Karte womöglich missbräuchlich genutzt wurde, sollte der Einzelverbindungsnachweis immer auf unerklärliche Gebühren und Zielrufnummern überprüft werden.

Alle Daten, die für die Sperrung der SIM-Karte bzw. des Mobiltelefons benötigt werden, sollten griffbereit, aber getrennt vom Mobiltelefon aufbewahrt werden. Das sind

- die Rufnummer des Mobilfunkanschlusses sowie die zugehörige SIM-Kartennummer,
- die Seriennummer des Mobiltelefons (GSM-USSD-Code *#06#),
- die Servicenummer des Netzbetreibers, unter der der Sperrwunsch gemeldet werden kann sowie
- das Servicenummer-Passwort und die Kundennummer, also die Daten, die für die Authentikation gegenüber dem Netzbetreiber benötigt werden.

Prüffragen:

- Ist sichergestellt, dass Mobiltelefone nach einem Verlust zeitnah gesperrt werden?
- Sind alle notwendigen Informationen für die Sperrung eines Mobiltelefons bei einem Verlust jederzeit griffbereit?

M 2.207 Sicherheitskonzeption für Lotus Notes/Domino

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Fachverantwortliche, IT-Sicherheitsbeauftragter

Wie für jedes in einer Institution eingesetzte Software-Produkt muss auch für den Einsatz von Lotus Notes/Domino eine geeignete Sicherheitskonzeption erstellt werden. Abhängig von der Größe, den Ressourcen und der organisatorischen Struktur der Institution kann die Sicherheitskonzeption für Lotus Notes/Domino in ein Ergebnisdokument (z. B. eine Sicherheitsrichtlinie) oder eine Reihe von Ergebnisdokumenten einfließen. Eine modulare Dokumentation der Sicherheitskonzeption erleichtert die zielgruppenspezifische Verteilung der Dokumente, beispielsweise könnte eine Richtlinie für die Anwendungsentwicklung nur an die Anwendungsentwickler für die Lotus Notes/Domino-Plattform bzw. an Administratoren verteilt werden.

Die im Folgenden genannten Punkte der Sicherheitskonzeption sind dabei abzuarbeiten und die Ergebnisse zu dokumentieren. Sind Teile der Sicherheitskonzeption für den speziellen Einsatz der Lotus Notes/Domino-Plattform in der Institution nicht relevant (z. B. wenn keine Anwendungsentwicklung für die Lotus Notes/Domino-Plattform stattfindet), ist dies in der Sicherheitsrichtlinie zu dokumentieren.

Sicherheitsrichtlinie für Lotus Notes/Domino

Im Rahmen der Sicherheitsrichtlinie sind folgende Aspekte zu berücksichtigen:

- Die Sicherheitsrichtlinie muss konform zu den geltenden Sicherheitsrichtlinien der Institution sein (siehe M 2.192 *Erstellung einer Leitlinie zur Informationssicherheit*).
- Es müssen die jeweiligen Zielgruppen und die für sie relevanten Konzepte/Richtlinien der Lotus Notes/Domino-Sicherheitskonzeption genannt werden.
- Die im Weiteren genannten Konzepte sind entweder als Bestandteil der Sicherheitsrichtlinie aufzunehmen oder zu referenzieren. Es ist dabei sicherzustellen, dass über die Referenzen die jeweils aktuelle Version der Konzepte verfügbar ist.
- Die Verbindlichkeit der Richtlinie für alle Zielgruppen (zum Beispiel Lotus Notes Benutzer, Lotus Domino Administratoren, Führungskräfte, Projektleiter, Softwareentwickler, Softwarearchitekten) ist sicherzustellen, falls nicht bereits für alle Richtlinien der Institution eine entsprechende allgemeine Regelung zur Verbindlichkeit besteht.
- Sind in der Institution mehrere Lotus Notes/Domino-Umgebungen (Installationen) im Einsatz, müssen umgebungsspezifische Besonderheiten der Sicherheitskonzeption dokumentiert sein.
- Die Sicherheitsrichtlinie für die Nutzung von Lotus Notes/Domino muss institutionsweit abgestimmt sein und allen Benutzern bekannt gegeben worden sein. Hierbei empfiehlt es sich, die wichtigsten Inhalte für die jeweiligen Zielgruppen in einer kurzen und prägnanten Form aufzubereiten, z. B. in Form eines Faltblattes oder einer Webseite. Wenn sich Sicherheitsvorgaben verändern, müssen alle Benutzer hierüber informiert werden.

Konzept zur Domänen- und Zertifikatshierarchie von Lotus Notes/Domino

Das Konzept zur Domänen- und Zertifikatshierarchie von Lotus Notes/Domino ist das Ergebnis der in M 2.206 *Planung des Einsatzes von Lotus Notes/Domino* beschriebenen Planungstätigkeit. Das Konzept ist vom Verantwortlichen stets aktuell zu halten und muss bei Veränderungen angepasst werden. Bei größeren Änderungen der Lotus Notes/Domino-Infrastruktur erfolgt dies in der Regel durch die zuständigen Projektleiter, System- und Softwarearchitekten. Änderungen an diesem hoch sicherheitsrelevanten Konzept bedürfen einer Abnahme durch das Informationssicherheitsmanagement.

Konzept zur Nutzung der Lotus Notes/Domino-eigenen Sicherheitsmechanismen: Verschlüsselung, Umgang mit Zertifikaten und Lotus Notes IDs

Lotus Notes/Domino stellt unterschiedliche Verschlüsselungsmechanismen sowohl zur Verschlüsselung beweglicher Daten (Kommunikationsverbindungen, Kommunikationsinhalte) als auch zur Verschlüsselung der Datenbestände (z. B. Datenbankverschlüsselung, E-Mail-Verschlüsselung) bereit. Es ist zu definieren, welche Lotus Domino-eigenen Mechanismen genutzt werden sollen. Die Konformität zu einem institutionsweiten allgemeinen Verschlüsselungskonzept bzw. die durch proprietäre Lotus Notes/Domino-Mechanismen bedingten Abweichungen sind zu dokumentieren. Das Schlüsselmanagement für Lotus Notes/Domino ist gemäß den Vorgaben des institutionsweiten Verschlüsselungskonzepts zu gestalten und muss dem Schutzbedarf der Lotus Notes/Domino-Plattform Rechnung tragen.

Der Umgang mit Zertifikaten, z. B. bei Rezertifizierung wegen Ablauf, Erstellung von Cross-Zertifikaten etc. ist gleichfalls in diesem Konzept zu regeln. Gefordert sind konkrete Regelungen und kein Verweis auf die grundsätzlich in Lotus Notes/Domino vorhandenen Mechanismen. So ist z. B. festzulegen, wann ein Versand per E-Mail zur Rezertifizierung an die Administratoren zulässig ist und wann nicht.

Da Lotus Notes IDs aufgrund der "Portabilität" ein Sicherheitsrisiko darstellen, muss geregelt werden, wo Kopien dieser IDs zu Wiederherstellungszwecken vorzuhalten sind und wie Prozesse im Umgang mit Lotus Notes IDs (z. B. Rezertifizierung, Wiederherstellung) ablaufen sollen.

Ab Lotus Notes 8.5 steht mit der Lotus Notes ID Vault ein Werkzeug zum Management von Lotus Notes IDs zur Verfügung, das u. a. die Wiederherstellung verlorener Lotus Notes IDs, verlorener Passwörter, Synchronisation von Kopien von IDs mit nativen Mitteln der Lotus Notes/Domino-Plattform ermöglicht bzw. bereits vorhandene Funktionalität der Plattform erweitert oder vereinfacht. Die Nutzung des Werkzeugs wird empfohlen. Der Einsatz ist jedoch zu planen und das Konzept zur Nutzung der Lotus Notes/Domino-eigenen Sicherheitsmechanismen entsprechend anzupassen.

Passwortrichtlinien für Lotus Notes/Domino

Lotus Notes/Domino besitzt seit jeher eigene Mechanismen zur Bewertung der Passwortgüte. Es ist daher erforderlich, die institutionsweiten Passwortrichtlinien mit entsprechenden Anmerkungen zu übernehmen oder aber speziell für Lotus Notes/Domino eine Anpassung der Passwortrichtlinie an die Lotus Notes Mechanismen vorzunehmen. Die Lotus Notes/Domino-Passwortrichtlinien sollten möglichst Teil der Sicherheitsrichtlinie von Lotus Notes/Domino sein. Wenn eine Anmeldung über Single-Sign-On erfolgt, ist dies in der Sicherheitsrichtlinie entsprechend zu vermerken. Die für den Single-Sign-On genutz-

te Passwortgüte muss den kumulierten Anforderungen der angeschlossenen Anwendungen bzw. Systeme genügen.

Protokollierungs- und Auswertungskonzept für Lotus Notes/Domino

Konform zu der institutionsweit gültigen Richtlinie zur Protokollierung und Auswertung sicherheitsrelevanter Daten/Ereignisse ist ein konkretes Konzept für die Lotus Notes/Domino-Plattform zu erstellen. Abstimmvorgänge mit Datenschutzbeauftragten, Betriebsrat, Personalrat und anderen in diese Konzepte einzubindenden Stellen sind dann erforderlich, wenn keine entsprechende allgemeingültige Richtlinie zur Protokollierung und Auswertung vorliegt oder diese nicht den erforderlichen Detaillierungsgrad aufweist.

Bei der Erstellung der Sicherheitsrichtlinie ist zu berücksichtigen, dass die Vorgaben im Hinblick auf die auszuwertenden Datenvolumina realistisch sind und eine Umsetzung im Betrieb mit den vorhandenen Ressourcen möglich ist. Werden in der Institution bereits Werkzeuge zur zentralen Protokollierung und automatischen Protokollauswertung eingesetzt, ist zu prüfen, ob die Lotus Notes/Domino-Protokollierung und -Auswertung mit deren Hilfe erfolgen kann.

Archivierungskonzept für Lotus Notes/Domino

Die Lotus Notes/Domino-Plattform kann unterschiedliche archivierungspflichtige Daten beinhalten: E-Mails, archivierungspflichtige Workflow-Elemente, Datenbanken archivierungspflichtiger Lotus Notes-Anwendungen und Dienste usw. Bei der Nutzung von Lotus Notes/Domino als zentrales System zum Identitätsmanagement fallen auch hier archivierungspflichtige Daten an. Es ist daher erforderlich, ein fachliches und technisches Archivierungskonzept für die Lotus Notes/Domino-Plattform zu erstellen und entsprechend umzusetzen oder das vorhandene institutionsweite Archivierungskonzept an die Anforderungen der Lotus Notes/Domino-Umgebung anzupassen.

Konzepte zur Absicherung aller genutzter Lotus Domino Dienste

In der Regel wird die Absicherung aller Dienste (oft auch auf der Ebene installierter Module) in der Sicherheitsrichtlinie gefordert. Die Dokumentation der Maßnahmen zur Absicherung der Dienste muss nicht zwingend in der Sicherheitsrichtlinie für Lotus Notes/Domino erfolgen, da sie sich schwerpunktmäßig nur an die Zielgruppe der Administratoren und an das Informationssicherheitsmanagement richtet, sondern kann auch im Rahmen des Betriebskonzeptes erfolgen. Es sollten sowohl die technischen Maßnahmen an der Lotus Notes/Domino-Plattform (Härtung, Konfiguration server- und clientseitiger Komponenten) als auch organisatorische Maßnahmen und genutzte zusätzliche Sicherheitskomponenten zur Absicherung aller Dienste beschrieben werden.

Konzept zum Umgang mit sicherheitsgefährdenden Altanwendungen und für deren Betrieb benötigten sicherheitsgefährdenden Konfigurationen der Lotus Notes/Domino-Plattform

Ältere Lotus Domino-Anwendungen, die nicht migriert werden können, erfordern eventuell "unsichere" Einstellungen, um auf neueren Plattformen betrieben werden zu können. Wenn auf diese nicht verzichtet werden kann, ist es erforderlich, konzeptionell festzuhalten, wie diese betrieben und überwacht werden können, um das entstehende Sicherheitsrisiko zu minimieren. Insbesondere ist darauf zu achten, dass "unsichere" Parametrisierungen der Plattform nur punktuell zum Einsatz kommen und nicht aus Gründen der Kompatibilität mit den Altlagen zum institutionsweiten Standard erhoben werden.

Richtlinie für die Anwendungsentwicklung für die Lotus Notes/Domino-Plattform

Lotus Notes/Domino bietet sowohl die Möglichkeit der Anwendungsentwicklung unter den bisherigen, proprietären Technologien als auch die Anwendungsentwicklung unter einer Eclipse-basierten Java-Entwicklungsumgebung. Für jede der beiden Möglichkeiten ist, falls sie genutzt wird, eine entsprechende Richtlinie für die Anwendungsentwicklung zu erstellen. Diese Richtlinien müssen sowohl Coding-Standards für die nutzbaren Programmiersprachen als auch Best Practice der Entwicklung wie auch eine Beschreibung des Anwendungsentwicklungsprozesses beinhalten.

Richtlinie für die Anwendungsintegration mit der Lotus Notes/Domino-Plattform

Lotus Notes/Domino wird zunehmend als Plattform für server- und clientseitige Anwendungsintegration positioniert, sowohl durch den neuen Lotus Notes Client, der in der strategischen Positionierung des Herstellers als "universeller" Client gesehen wird, als auch durch die Möglichkeit der SAP-Integration. Um Anwendungsintegration nicht zu einer Quelle von sicherheitstechnischen Schwachstellen werden zu lassen, ist es erforderlich, eine plattformspezifische Richtlinie zur Anwendungsintegration mit der Lotus Notes/Domino-Plattform zu erstellen.

Schutz vor Schadprogrammen für Lotus Notes/Domino

Der Schutz vor Schadprogrammen für Lotus Notes/Domino ist die konzeptionelle Umsetzung der allgemeinen, institutionsweit gültigen Vorgaben zum Schutz vor Schadprogrammen. Dazu gehört sowohl der Schutz vor Schadprogrammen an Netzübergängen, an denen Lotus Domino als Web- oder E-Mail-Gateway zum Einsatz kommt, als auch der "nachgelagerte" Schutz vor Schadprogrammen der Lotus Domino Datenbanken (einschließlich der E-Mail-Datenbanken). Das Zusammenspiel der standardmäßig installierten server- oder clientseitigen Schutzprogramme mit den installierten Lotus Notes/Domino-Komponenten ist gleichfalls in diesem Konzept zu beschreiben.

Härtungskonzept und Konfigurationsvorgaben für Lotus Notes/Domino

Die zu installierenden Komponenten von Lotus Notes/Domino sind entsprechend dem Schutzbedarf und ihrem Einsatzszenario zu härten und zu konfigurieren. Es ist neben den im Konzept zur Absicherung der genutzten Dienste beschriebenen Absicherungsmaßnahmen auf Ebene der Dienste auch eine "Basishärtung" des Servers konzeptionell zu beschreiben. Zudem ist zu beschreiben, welche Dienste nicht genutzt werden und wie sie entsprechend deinstalliert (bzw. nicht installiert) werden können. Für alle genutzten Clienttypen (auch browserbasierte Clients) sind die clientseitig erforderlichen Härtungs- bzw. Konfigurationsvorgaben konzeptionell zu beschreiben.

Konzept zur Nutzung von Push-Diensten

Die Nutzung des Lotus Domino E-Mail-Dienstes in Verbindung mit Push-Diensten kann über die Anbindung fremder Push-Dienste (wie z. B. bei der Einbindung von Smartphones) oder über die Nutzung der Komponente *Lotus Notes Traveler* erfolgen. Es ist erforderlich, dass bei der Nutzung von Push-Diensten die anfallenden sicherheitsrelevanten Themen konzeptionell beschrieben werden.

Prüffragen:

- Existieren aktuelle Sicherheitsrichtlinien für die Nutzung von Lotus Notes?
- Sind alle relevanten Sicherheitsvorgaben der Institution auf Lotus Notes abgebildet?
- Werden alle Benutzer über neue oder veränderte Sicherheitsvorgaben zu Lotus Notes informiert?

M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: IT-Sicherheitsbeauftragter, Leiter IT

Die IT-Komponenten, die innerhalb einer hauseigenen Liegenschaft eingesetzt werden, sind im Allgemeinen durch infrastrukturelle Sicherheitsmaßnahmen ausreichend vor Missbrauch und Diebstahl geschützt. Häufig sollen aber IT-Systeme oder Datenträger auch außer Haus eingesetzt werden, z. B. bei Dienstreisen oder Telearbeit. Um auch diese ausreichend schützen zu können, muss die Mitnahme von Datenträgern und IT-Komponenten klar geregelt werden.

Dabei muss festgelegt werden,

- welche IT-Komponenten bzw. Datenträger außer Haus mitgenommen werden dürfen,
- wer IT-Komponenten bzw. Datenträger außer Haus mitnehmen darf,
- welche grundlegenden IT-Sicherheitsmaßnahmen dabei beachtet werden müssen (Virenschutz, Verschlüsselung sensitiver Daten, Aufbewahrung, etc.).

Die Art und der Umfang der anzuwendenden Sicherheitsmaßnahmen für extern eingesetzte IT-Komponenten hängen einerseits vom Schutzbedarf der darauf gespeicherten IT-Anwendungen und Daten und andererseits von der Sicherheit der Einsatz- bzw. Aufbewahrungsorte ab.

Grundsätzlich sollte für alle IT-Komponenten, die extern eingesetzt werden sollen, eine entsprechende Genehmigung eingeholt werden.

Bei größeren Institutionen, bei denen der Zutritt zu den Liegenschaften durch Pförtner bzw. Wachdienste kontrolliert wird, sollte überlegt werden, ob diese angewiesen werden sollten, in Stichproben zu überprüfen, inwieweit die Regelungen für die Mitnahme von Datenträgern und IT-Komponenten eingehalten werden.

Außerhalb der organisationseigenen Liegenschaften sind die Benutzer für den Schutz der ihnen anvertrauten IT verantwortlich. Darauf und auf die zu ergreifenden Vorsichtsmaßnahmen sind sie hinzuweisen. Dazu gehören folgende Regeln:

- IT-Systeme müssen stets sicher aufbewahrt werden. Bei Dienstreisen sollten sie nicht unbeaufsichtigt gelassen werden. Insbesondere sollten sie nicht in Fahrzeugen zurückgelassen werden (siehe auch M 1.33 *Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz*).
- IT-Systeme wie Laptops oder Mobiltelefone und deren Anwendungen können im Allgemeinen durch PINs oder Passwörter abgesichert werden. Diese Mechanismen sollten auch genutzt werden.
- IT-Systeme oder Datenträger, die sensitive Daten enthalten, sollten möglichst komplett verschlüsselt werden (siehe auch M 4.29 *Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme*). Wenn IT-Systeme eine Verschlüsselungsfunktion ohne weitere Hilfsmittel ermöglichen, ist es

empfehlenswert, das diese Funktionen auch genutzt werden, wenn lediglich weniger sensitive Daten auf den IT-Systemen enthalten sind.
- Die Verwaltung, Wartung und Weitergabe von extern eingesetzten IT-Systemen sollte geregelt werden. Hierzu können beispielsweise Pools eingerichtet werden (siehe auch M 1.35 *Sammelaufbewahrung tragbarer IT-Systeme* bzw. M 2.190 *Einrichtung eines Mobiltelefon-Pools*).
- Es sollte protokolliert werden, wann und von wem welche IT-Komponenten außer Haus eingesetzt wurden.

Prüffragen:

- Gibt es Regelungen für die Mitnahme von Datenträgern und Komponenten?
- Werden die Benutzer von extern eingesetzten IT-Komponenten auf die Regelungen hingewiesen, die von ihnen einzuhalten sind?
- Hoher Schutzbedarf bezüglich Vertraulichkeit: Werden mobile IT-Systeme oder Datenträger durch vollständige Verschlüsselung der Datenträger geschützt?
- Werden die angebotenen Authentisierungsmechanismen genutzt, wenn IT-Komponenten extern eingesetzt werden?

M 2.303 Festlegung einer Strategie für den Einsatz von Smartphones, Tablets oder PDAs

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
Verantwortlich für Umsetzung: IT-Sicherheitsbeauftragter

Bevor in einer Organisation PDAs eingesetzt werden, muss festgelegt sein, welche generelle Strategie die Organisation im Hinblick auf die Nutzung der Geräte einnimmt. Insbesondere sind dafür die folgenden Fragen zu beantworten:

- Für welche Anwendungen sollen die PDAs eingesetzt werden?
- Werden den Mitarbeitern dienstliche PDAs zur Verfügung gestellt?
- Wird die Nutzung privater PDAs der Mitarbeiter erlaubt oder sogar offiziell unterstützt?

Insbesondere die Frage, für welche Zwecke PDAs eingesetzt werden sollen, ist für die späteren Entscheidungen wichtig, denn sie kann einen entscheidenden Einfluss auf die Auswahl anzuschaffender Geräte haben und muss in jedem Fall bei der Formulierung der Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung berücksichtigt werden.

Klassifikation der Daten

Jeder Benutzer und jede Institution sollte sich Gedanken darüber machen, welche Daten auf einem PDA gespeichert werden dürfen und welchen Schutzbedarf diese haben. In einem Unternehmen oder einer Behörde sollte dies nicht nur für Daten auf PDAs, sondern generell geklärt werden. So gibt es in Anwendungsfeldern und Geschäftsprozessen Daten, die einen höheren Schutzbedarf haben oder die besonderen Restriktionen unterliegen, z. B. personenbezogene, finanzrelevante, vertrauliche oder Copyright-geschützte Daten.

Daher sollten in einer Institution alle Arten von Daten danach kategorisiert sein, wie schutzbedürftig sie sind und welche Beschränkungen im Umgang mit ihnen beachtet werden sollten (siehe hierzu auch M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*).

Damit die Mitarbeiter mit diesen Einstufungen auch sinnvoll umgehen können, empfiehlt es sich, diesen hierzu leicht verständliche Tabellen und Beispiele an die Hand zu geben, in denen erläutert ist, welche Arten von Daten auf den verschiedenen IT-Systemen oder Anwendungen gespeichert oder verarbeitet werden dürfen und auch, an wen diese weitergegeben werden dürfen.

Nutzung von privaten PDAs

Aufgrund einer unzureichenden Ausstattung oder eines hohen Benutzerdruckes kann es vorkommen, dass private PDAs für dienstliche Zwecke benutzt werden. Das Sicherheitsmanagement bzw. die IT-Verantwortlichen sollten aber auf jeden Fall sicherstellen, dass auch die private Nutzung innerhalb der Institution nicht "wild" erfolgt, sondern klar geregelt ist. Sollen PDAs nur für Anwendungen wie Termin- und Adressverwaltung oder für E-Mail-Kommunikation eingesetzt werden, so kann die Nutzung privater PDAs normalerweise erlaubt werden, wenn keine sonstigen Gründe dagegen sprechen.

Falls die PDAs für eine Anwendung eingesetzt werden sollen, aus der sich für die Geräte ein hoher Schutzbedarf ergibt, so ist es sehr fraglich, ob dafür die Nutzung privater PDAs zugelassen werden sollte. Der Grund dafür ist insbesondere, dass private Geräte weitgehend dem Einfluss der zentralen Konfiguration und Administration entzogen sind und es deswegen praktisch keine Möglichkeit gibt, für die Geräte ein akzeptables Sicherheitsniveau zu gewährleisten. Es wird dringend empfohlen, in diesem Fall keine Nutzung privater PDAs zuzulassen.

Bei der Entscheidung sollte auch berücksichtigt werden, dass die Entscheidung, private PDAs zuzulassen, auch Auswirkungen auf die spätere IT-Strategie einer Organisation haben kann.

Beispiel:

In einem Unternehmen wurden zwar keine PDAs für die Mitarbeiter angeschafft, die Mitarbeiter wurden aber dennoch bei der Beschaffung privater Geräte und der Anbindung an die Arbeitsplatz-PCs beraten. Als das Unternehmen die PCs von Windows NT nach Windows 2000 migrierte, stellte sich heraus, dass es unter Windows 2000 keine passenden Treiber für die vorhandenen PDAs existierten. Durch die massiven Benutzerbeschwerden stand das Unternehmen vor der Wahl, den Benutzern neue PDAs zu finanzieren oder diesen weiter NT-basierte PCs zur Verfügung zu stellen.

Wenn ein Verbot ausgesprochen wird, private PDAs für Dienstzwecke zu benutzen oder sie in das Büro mitzubringen, sollte immer bedacht werden, dass solche Verbote überwacht werden müssen und dass sie auch ineffektiv sein können.

Die Entscheidung sollte zusammen mit den Entscheidungsgründen dokumentiert und den Mitarbeitern auf geeignete Art und Weise kommuniziert werden.

Prüffragen:

- Gibt es eine generelle Strategie für die Nutzung von PDAs?
- Ist festgelegt, welche Daten auf PDAs gespeichert werden dürfen?
- Nutzung privater PDAs: Ist die private PDA-Nutzung innerhalb der Institution klar geregelt?
- Wird beachtet, dass Verbote bezüglich privater PDAs zu überwachen sind und Konsequenzen bei Nichteinhaltung folgen müssen?

M 2.304 Sicherheitsrichtlinien und Regelungen für die Nutzung von Smartphones, Tablets und PDAs

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: IT-Sicherheitsbeauftragter, Leiter IT

Wenn in einer Institution entschieden wurde, PDAs einzusetzen, so müssen diese in die allgemeine Sicherheitsstrategie eingebunden werden.

Bei der Nutzung von PDAs gibt es eine Vielzahl von Möglichkeiten, diese vor Missbrauch zu schützen. Damit diese Möglichkeiten auch genutzt werden, sollte eine Sicherheitsrichtlinie erstellt werden, in der alle umzusetzenden Sicherheitsmechanismen beschrieben werden. Jede Institution sollte sich die Möglichkeiten und Risiken des PDA-Einsatzes bewusst machen. Hierbei sollten zwei Sicherheitsaspekte im Vordergrund stehen:

- die Sicherheit der auf PDAs gespeicherten Daten und
- die Auswirkung der PDA-Nutzung auf die Sicherheit anderer IT-Systeme innerhalb einer Institution.

Aufbauend auf die PDA-Sicherheitsrichtlinie sollte für die Benutzer ein kurzes und übersichtliches Merkblatt für die sichere Nutzung von PDAs erstellt werden.

Schutz vor Missbrauch

Ein PDA hat nicht nur für den Besitzer den Vorteil, leicht zu transportieren und unauffällig zu verwahren zu sein, sondern auch für einen Dieb. Daher sollte auch ein PDA stets sicher aufbewahrt werden. Bei Dienstreisen sollten sie nicht unbeaufsichtigt gelassen werden. Insbesondere sollten sie nicht in Fahrzeugen zurückgelassen werden.

Praktisch alle Varianten von PDAs und Organizern lassen sich durch PINs oder Passwörter gegen unbefugten Zugriff absichern. Leider sind nicht alle vom Hersteller angebotenen Sicherheitsmechanismen so sicher, wie es wünschenswert wäre. Daher sollten sich PDA-Benutzer informieren, wie zuverlässig die vorhandenen Sicherheitsmechanismen sind, z. B. über das Internet.

Solange keine besseren Sicherheitstools installiert sind, sollten aber auf jeden Fall die vorhandenen Sicherheitsmechanismen genutzt werden (siehe auch M 4.228 *Nutzung der Sicherheitsmechanismen von Smartphones, Tablets und PDAs*). Alle Benutzer sollten sich aber über deren Wirkung und insbesondere deren Grenzen im Klaren sein. Dabei sollten die Passwörter und PINs sorgfältig ausgewählt werden, also auch lang genug sein, damit sie nicht einfach überwunden werden können. Die Passwörter dürfen keinesfalls zusammen mit dem PDA aufbewahrt werden.

Sensibilisierung der Benutzer

Alle PDA-Benutzer sollten nicht nur über die Vorteile von PDAs aufgeklärt werden, sondern auch über potentielle Risiken und Probleme bei der Nutzung sowie über den Nutzen, aber auch die Grenzen der eingesetzten Sicherheitsmaßnahmen.

Da auch für die Betriebssysteme von PDAs (beispielsweise Palm OS, Windows CE bzw. Windows Mobile, Symbian OS) immer wieder neue Sicherheitslücken offengelegt werden, sollte sich das Sicherheitsmanagement regelmä-

ßig über aktuelle Risiken informieren. Gegebenenfalls ist es angebracht, die Mitarbeiter regelmäßig über die neu bekanntgewordenen Gefahren zu informieren und damit auch zu sensibilisieren.

Regelungen zur PDA-Nutzung

Allgemeine Regelungen

Auf einem PDA sind Daten in der Regel schlechter geschützt als auf IT-Systemen innerhalb der Organisation. Unabhängig davon, ob privat oder dienstlich angeschaffte PDAs genutzt werden, sollte der Arbeitgeber daher schriftlich regeln,

- welche Daten nicht auf einem PDA gespeichert werden dürfen,
- dass Daten nicht überall eingegeben bzw. abgerufen werden sollten, da sie dabei unter Umständen mitgelesen werden können,
- wie, wann und durch wen Datensicherungen des PDAs durchzuführen sind,
- unter welchen technischen Einsatzbedingungen die PDAs eingesetzt werden dürfen. Hierzu gehören vor allem die Festlegung von Sicherheitsmaßnahmen, die Auswahl und Installation der erforderlichen Sicherheitshard- und -software sowie Vorgaben für die sichere Konfiguration der betroffenen IT-Systeme.

Ein PDA sollte möglichst nicht unbeaufsichtigt bleiben. Falls ein PDA in einem Kraftfahrzeug zurückgelassen werden muss, so sollte das Gerät von außen nicht sichtbar sein. Das Abdecken des Gerätes oder das Einschließen in den Kofferraum bieten Abhilfe. Ein PDA stellt einen Wert dar, der potentielle Diebe anlocken könnte.

Wird ein PDA in fremden Büroräumen benutzt, so sind die Sicherheitsregelungen der besuchten Organisation zu beachten.

In fremden Räumlichkeiten wie Hotelzimmern sollte ein PDA nicht ungeschützt liegen gelassen werden. Alle Passwort-Schutzmechanismen sollten spätestens jetzt aktiviert werden. Das Verschließen des Gerätes in einem Schrank behindert Gelegenheitsdiebe.

Nutzung von privaten PDAs

Bei der Nutzung von privaten PDAs in einer Behörde oder einem Unternehmen sind unter anderem die folgenden Punkte zu regeln:

- Die sinnvolle Nutzung von PDAs erfordert im Allgemeinen eine Synchronisation mit einem PC, beispielsweise für Terminkalender, Adressbücher, E-Mail-Unterstützung und mehr. Daher muss geklärt werden, ob die Installation der dafür benötigten Hard- und Software erlaubt wird, und wer die Installation vornimmt. Dies sollte nicht den Benutzern selbst überlassen werden.
- Es muss geklärt werden, inwieweit der Benutzer-Support bei Problemen, die sich aus der Nutzung von privaten PDAs ergeben, Hilfestellung leistet. Ebenso sollte im Vorfeld abgesprochen werden, wie private PDAs in die IT-Strategie der Institution eingebunden werden.

Nutzung von dienstlichen PDAs

Bei der Nutzung von dienstlichen PDAs sind unter anderem die folgenden Punkte zu regeln:

- Es muss geklärt werden, ob dienstliche PDAs auch mit privaten PCs synchronisiert werden dürfen. Dies erleichtert einerseits Terminabstimmun-

gen, andererseits könnte dadurch Schadsoftware in die dienstlichen Systeme eingeschleppt werden und interne Dokumente könnten auf die privaten PCs gelangen.
- Die Benutzer sollten darauf hingewiesen werden, wie sie sorgfältig mit den PDAs umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen bzw. um eine lange Lebensdauer zu gewährleisten (z. B. Akkupflege, Aufbewahrung außerhalb von Büro- oder Wohnräumen, Empfindlichkeit gegenüber zu hohen oder zu niedrigen Temperaturen).
- Die Verwaltung, Wartung und Weitergabe von PDAs sollte geregelt werden.

Einbindung in andere Sicherheitslösungen

Bei der Benutzung von PDAs muss nicht nur überlegt werden, ob der Einsatz von Sicherheitssoftware zum Schutz des PDAs selber sinnvoll ist, sondern auch, wie der PDA mit der Sicherheitssoftware der Einsatzumgebung zusammenarbeitet. Dazu zwei Beispiele:

- Der Benutzer liest und schreibt auf seinem Desktop-PC häufig E-Mails, die verschlüsselt bzw. signiert sind. Außerdem möchte er seinen PDA nutzen, um unterwegs E-Mail zu bearbeiten. Mit verschlüsselten bzw. signierten Mails kann er aber aus verschiedenen Gründen Probleme bei der Weiter- verwendung auf dem PDA bekommen. So gibt es beispielsweise bisher nur sehr wenige Verschlüsselungs- bzw. Signaturanwendungen, die sowohl mit den einschlägigen Mailprogrammen auf Office-Systemen als auch auf PDAs kompatibel sind. Bei solchen Anwendungen werden außerdem oft Chipkarten oder andere Sicherheitstoken als sicherer Speicherplatz für die benötigten kryptographischen Schlüssel eingesetzt. Nur die wenigsten PDAs lassen sich aber um Chipkarten-Leseeinrichtungen erweitern. Viele PKI-Anwendungen arbeiten außerdem serverbasiert, benötigen also Zugriff auf einen Server, um beispielsweise Zertifikate überprüfen oder öffentliche Schlüssel von Kommunikationspartnern abrufen zu können.
- Im Unternehmen werden alle Daten, sowohl auf den Clients als auch den Servern, ausschließlich verschlüsselt gespeichert. Wenn Benutzer nun interne Daten auf PDAs transferieren wollen, kann zum einem passieren, dass sie unterwegs feststellen, dass sie zugriffsgeschützte Dateien geladen haben, die sie auf dem PDA nicht lesen können. Dies ist der für die Vertraulichkeit der Daten bessere Fall. Typischerweise werden die auf den PDA übertragenen Daten dort nämlich nicht oder nur schwach verschlüsselt, so dass sie weniger stark geschützt sind als auf den internen Systemen.

Auch solche Fälle, also die Einbindung von PDA-Applikationen in andere Sicherheitssoftware im Unternehmen, muss daher unbedingt in der PDA-Sicherheitsrichtlinie geregelt werden, um zu vermeiden, dass durch die PDA-Nutzung das festgelegte Sicherheitsniveau reduziert wird.

Wo nötig: Nutzungsverbot von PDAs

Es sollte überlegt werden, ob die Nutzung oder sogar das Mitbringen von PDAs in allen oder bestimmten Bereichen einer Behörde oder eines Unternehmens eingeschränkt werden sollte. Dies kann z. B. dort sinnvoll sein, wo das Mitschneiden von Gesprächen oder das Fotografieren unterbunden werden soll.

Wenn die Sicherheitsrichtlinie der Institution es nicht zulässt, dass fremde IT-Systeme wie beispielsweise PDAs mitgebracht werden, muss an allen Eingängen deutlich darauf hingewiesen werden. Dies sollte dann auch regelmä-

ßig kontrolliert werden. Für die Besucher sollte in diesem Fall eine Möglichkeit geschaffen werden, mitgebrachte Mobiltelefone, PDAs oder Notebooks sicher aufzubewahren. Beispielsweise können an den Eingängen Schließfächer zur Verfügung gestellt werden.

Prüffragen:

- Existiert eine aktuelle Sicherheitsrichtlinie für Smartphones, Tablets und PDAs, in der alle umzusetzenden Sicherheitsmechanismen beschrieben sind?
- Sind Passwörter und PINs für die Nutzung von Smartphones, Tablets und PDAs ausreichend komplex und werden nicht zusammen mit dem jeweiligen Gerät aufbewahrt?
- Informiert sich das Sicherheitsmanagement regelmäßig über aktuelle Risiken der Nutzung von Smartphones, Tablets und PDAs und informiert erforderlichenfalls die Mitarbeiter?
- Bei Nutzung dienstlicher Smartphones, Tablets und PDAs: Ist die Verwaltung, Wartung und Weitergabe der betroffenen Geräte geregelt?
- Ist die Einbindung der auf Smartphones, Tablets und PDAs installierten Applikationen in andere Sicherheitssoftware in der entsprechenden Sicherheitsrichtline geregelt?

M 2.305 Geeignete Auswahl von Smartphones, Tablets oder PDAs

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator, Beschaffungsstelle, Leiter IT

Smartphones, Tablets oder PDAs gibt es in verschiedenen Varianten und Geräteklassen. Diese unterscheiden sich nicht nur in ihren Abmessungen und im Leistungsumfang, sondern auch bei Sicherheitsmechanismen und Bedienkomfort. Zudem stellen sie unterschiedliche Anforderungen an Hard- und Software-Komponenten im Einsatzumfeld.

Aufgrund der Vielzahl von Modellen mit den unterschiedlichsten Betriebssystemen sind Kompatibilitätsprobleme mit anderer Hard- und Software wahrscheinlich.

Wenn einmal beschlossen worden ist, innerhalb einer Institution Smartphones, Tablets oder PDAs einzusetzen, sollte zunächst eine Anforderungsanalyse durchgeführt werden. Ziel der Anforderungsanalyse ist es, alle im konkreten Fall in Frage kommenden Einsatzszenarien zu bestimmen und daraus Anforderungen an die benötigten Hard- und Softwarekomponenten abzuleiten und in einer Liste zu dokumentieren.

Anhand dieser Anforderungsliste sind dann die am Markt erhältlichen Produkte zu bewerten und die zu beschaffenden Geräte auszuwählen. Werden in einer Institution private Smartphones, Tablets oder PDAs dienstlich genutzt, dürfen nur solche private Geräte erlaubt werden, die diese Anforderungen erfüllen. Die Praxis zeigt, dass es aufgrund verschiedener Einsatzanforderungen durchaus sinnvoll sein kann, verschiedene Gerätetypen anzuschaffen. Die Gerätevielfalt sollte aber zur Vereinfachung des Supports eingeschränkt werden.

Außerdem ist sicherzustellen, dass die mobilen Endgeräte und die darauf verwendete Software zentral und effektiv verwaltet werden können (siehe M 4.230 *Zentrale Administration von Smartphones, Tablets und PDAs*). Auch sollte die notwendige Serverinfrastruktur einen möglichst geringen administrativen Aufwand erfordern.

Die folgende Liste gibt einen groben Überblick über mögliche allgemeine Bewertungskriterien, erhebt jedoch keinen Anspruch auf Vollständigkeit und kann um weitere allgemeine Anforderungen erweitert werden.

Allgemeine Kriterien

Wartung
- Lässt sich das Produkt einfach warten?
- Bietet der Hersteller regelmäßige Software-Updates an?
- Können für das Produkt Wartungsverträge abgeschlossen werden?

Zuverlässigkeit/Ausfallsicherheit
- Wie zuverlässig und ausfallsicher ist das Produkt?
- Ist das Produkt im Dauerbetrieb einsetzbar?
- Gibt es einen im Produkt integrierten Backup-Mechanismus?
- Kann eine automatische Datensicherung durchgeführt werden?

- Lässt sich das Produkt sicher löschen?

Benutzerfreundlichkeit
- Können Benutzer die Systeme ohne größere Schulungsmaßnahmen effektiv, sicher und fehlerfrei nutzen?
- Ist die Synchronisations-Software so konfigurierbar, dass die Benutzer möglichst wenig mit technischen Details belastet werden? Ist die Sicherheit dabei trotzdem immer gewährleistet?
- Sind Abmessungen und Gewicht bezogen auf den Einsatzzweck angemessen? Ist die Akku-Laufzeit ausreichend für die tägliche Arbeit?

Kosten
- Wie hoch sind die Anschaffungskosten der Hard- und Software?
- Wie hoch sind die voraussichtlichen laufenden Kosten der Hard- und Software (Wartung, Betrieb, Support)?
- Wie hoch sind die voraussichtlichen Personalkosten (Administrator/Support)?
- Müssen zusätzliche Soft- oder Hardware-Komponenten angeschafft werden (z. B. Docking-Station, Konvertierungssoftware)?

Funktion

Installation und Inbetriebnahme
- Lässt sich das Produkt einfach installieren, konfigurieren und nutzen?
- Kann das Gerät sowie die Synchronisations-Software so konfiguriert werden, dass die vorgegebenen Sicherheitsziele erreicht werden?
- Können wichtige Konfigurationsparameter vor Veränderungen durch unbefugte Benutzer geschützt werden?
- Arbeitet das Produkt mit gängiger Hard- und Software zusammen (Betriebssysteme, Treiber)?

Administration
- Enthält die mitgelieferte Produktdokumentation eine genaue Darstellung aller technischen und administrativen Details?
- Können die Smartphones, Tablets oder PDAs über eine zentral gesteuerte Management-Software administriert werden? Ist die administrative Schnittstelle so gestaltet, dass auf fehlerhafte, unsichere oder inkonsistente Konfigurationen hingewiesen wird oder diese verhindert werden?

Protokollierung
- Bietet das Produkt Protokollierung an?
- Ist der Detailgrad der Protokollierung konfigurierbar?
- Werden durch die Protokollierung alle relevanten Daten erfasst?

Kommunikation und Datenübertragung
- Unterstützt das Smartphone, Tablet oder der PDA alle benötigten Datenübertragungstechniken (z. B. WLAN, Bluetooth, GSM, UMTS, LTE oder Infrarot)?

Sicherheit

Kommunikation, Authentisierung und Zugriff
- Hat das Smartphone, Tablet oder der PDA geeignete Mechanismen zur Identifikation und Authentisierung der Benutzer?
- Können mit dem Produkt die Daten zu anderen Endgeräten gesichert übertragen werden? Gilt dies für alle Schnittstellen, also z. B. auch für drahtlose Verbindungen?
- Können zusätzliche Sicherungsmechanismen (z. B. Verschlüsselungs- oder Virenschutzprogramme) genutzt werden?

- Erlaubt die Produktarchitektur die nachträgliche Installation neuer Sicherheitsmechanismen?
- Wird dem mobilen Benutzer nur nach erfolgreicher Authentisierung der Zugang zu lokalen Endgeräten erlaubt?

Trotz einer Produktauswahl durch das IT-Management sollte immer damit gerechnet werden, dass Mitarbeiter andere Smartphones, Tablets oder PDAs bevorzugen und versuchen, diese im Betrieb einzusetzen und eventuell sogar Unterstützung dafür einfordern. Hierfür sollte eine geeignete Vorgehensweise definiert werden.

Manche Funktionen von Smartphones, Tablets oder PDAs sind nur in Verbindung mit externen Dienstleistern nutzbar. Über einen externen Dienstleister sollten jedoch keine internen Daten ausgetauscht werden, wenn die Vertraulichkeit und Integrität der Daten nicht gewährleistet ist. So ist beispielsweise die Übertragung über ein Mobilfunknetz meist zunächst verschlüsselt ("Luftschnittstelle"), die Daten werden dann aber oft innerhalb des Netzes des Mobilfunkanbieters unverschlüsselt übertragen und auf dem Server des Dienstbetreibers unverschlüsselt gespeichert. Im Zweifelsfall sollen solche Dienste daher nicht genutzt werden.

Prüffragen:

- Wurde die Beschaffungsentscheidung mit den Administratoren und dem technischen Personal abgestimmt?
- Wurde eine Bewertung der relevanten Geräte anhand der Anforderungsanalyse durchgeführt?
- Wurde eine Anforderungsanalyse durchgeführt?

M 2.306 Verlustmeldung

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Benutzer

Bei Ausfall, Defekt, Zerstörung, Verlust oder Diebstahl eines dienstlich genutzten IT-Systems, sollte dies umgehend gemeldet werden. Das gilt auch für private Geräte, die dienstlich genutzt werden, und für mobile Datenträger. Hierfür sollte es in jeder Organisation klare Meldewege und Ansprechpartner geben.

Auch Defekte bei geringpreisigen Datenträgern sollten gemeldet werden, damit das IT-Management erkennen kann, ob hiervon größere Lieferungen betroffen sind. Insbesondere bei Datenträgern, die für Datensicherungen und Archivierung eingesetzt werden, ist eine hohe Verlässlichkeit und eine lange Lebensdauer wichtig. Bei einem Verlust oder Diebstahl wiederum muss schnell gehandelt werden, da es hier nicht nur um die Wiederbeschaffung der Geräte geht, sondern auch darum, potenziellen Missbrauch der betroffenen Informationen zu verhindern.

Auf Laptops, Smartphones, Tablets, PDAs und ähnlichen Geräten, aber auch auf mobilen Datenträgern wie USB-Sticks können sich vertrauliche Daten befinden, nach deren Verlust umgehend gehandelt werden muss, beispielsweise:

- Zugangsdaten wie Passwörter: Alle Zugangsdaten im eventuell betroffenen IT-System müssen umgehend geändert werden.
- Als vertraulich eingestufte Informationen (z. B. Patientenakten): Alle betroffenen Bereiche (z. B. Fachabteilung, Kunden, etc.) müssen benachrichtigt werden, um entsprechende Maßnahmen ergreifen zu können.

Bei Verlust von mobilen Endgeräten mit einer Funkverbindung sollten Maßnahmen zum Sperren, Löschen und Lokalisieren der mobilen Endgeräte genutzt werden. Die meisten Mobile-Device-Management-Lösungen bieten diese Funktionen an. Dafür sind im Vorfeld klare Regeln zu definieren und entsprechende Maßnahmen in Absprache mit dem Benutzer, dessen Endgerät verloren ging, unverzüglich zu ergreifen (siehe M 6.159 *Vorsorge vor Verlust und Diebstahl von Smartphones, Tablets und PDAs*).

Wenn verlorene Geräte oder Datenträger wieder auftauchen, sollten sie auf eventuelle Manipulationen untersucht werden, z. B. ob Schrauben geöffnet, Siegel entfernt wurden oder sich das Gewicht gegenüber dem Auslieferungszustand geändert hat. Besteht ein Verdacht, sollte das Gerät entweder gleich entsorgt oder von einem Spezialisten weiter untersucht werden. Um sicherzustellen, dass sich keine manipulierten Programme auf den wiedererlangten Geräten befinden, müssen die Geräte zumindest neu installiert werden (siehe M 4.28 *Software-Reinstallation bei Benutzerwechsel eines Laptops*). Wiedergefundene Datenträger sollten mit derselben Vorsicht behandelt werden, da sich hierauf Schadsoftware befinden könnte.

Prüffragen:

- Wissen die Benutzer, wie und wo sie Verlustmeldungen abgeben können?

M 2.312 Konzeption eines Schulungs- und Sensibilisierungsprogramms zur Informationssicherheit

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter Personal
Verantwortlich für Umsetzung: IT-Sicherheitsbeauftragter, Vorgesetzte

Die Mitarbeiter sind wesentliche Erfolgsfaktoren, um Informationssicherheit in einer Institution zu etablieren und aufrechtzuerhalten. Sie sind es, die technische Schutzsysteme nutzen oder administrieren, die Richtlinien und Vorgaben mehr oder weniger sorgfältig beachten und die aus Unkenntnis oder Vorsatz sicherheitsrelevante Fehler machen können.

Die im Rahmen eines Sicherheitskonzeptes realisierten technischen und organisatorischen Maßnahmen wirken sich in vielfältiger Weise auf die einzelnen Mitarbeiter aus. So könnten sie zu regelmäßigen Passwortwechseln gezwungen sein, bestimmte Bereiche der Institution ohne Genehmigung nicht betreten dürfen, ihre Mitarbeiterausweise gut sichtbar tragen oder regelmäßig Sicherheitsschulungen besuchen müssen.

Ziel jeder Institution sollte es daher sein, dass alle Mitarbeiter den Wert und die Notwendigkeit einer angemessenen Informationssicherheit zur Erfüllung ihrer Aufgaben und den Fortbestand der Institution erkennen, akzeptieren und aktiv unterstützen. Sie sollten die bestehenden Regelungen und Maßnahmen beachten und durch ihr Verhalten dazu beitragen, die Informationssicherheit aufrechtzuerhalten und weiterzuentwickeln. Auch sollten sie sicherheitskritische Situationen möglichst frühzeitig erkennen und darauf richtig reagieren.

Dies setzt eine systematische Sensibilisierung der Mitarbeiter voraus, die durch einen kontinuierlichen Prozess in der Institution zu verankern ist. Aufbauend auf der Sensibilisierung sollten die Mitarbeiter durch ergänzende Schulungen alle erforderlichen Informationen und Fähigkeiten vermittelt bekommen (siehe M M 2.557 *Konzeption eines Schulungsprogramms zur Informationssicherheit*). Sensibilisierungs- und Schulungsprogramme sind somit eng verwandte Themengebiete, denen auf allen Organisationsebenen eine hohe Bedeutung zugemessen werden sollte. Damit das besondere Gewicht von Sensibilisierungsmaßnahmen erkennbar ist und die benötigten Ressourcen zur Planung, Umsetzung und Aufrechterhaltung verfügbar sind, muss das Management die Maßnahmen unterstützen (siehe M 3.96 *Unterstützung des Managements für Sensibilisierung und Schulung*).

Nachfolgend sind die Schritte aufgeführt, mit denen ein Sensibilisierungsprogramm erstellt werden kann:

Ziel der Sensibilisierung festlegen

Sensibilisierung für Informationssicherheit bedeutet, dass bei Mitarbeitern die Wahrnehmung von Informationssicherheit geschärft und ihr Sicherheitsbewusstsein entsprechend den Anforderungen der Institution geschult wird.

Zu Beginn der Sensibilisierung sollte ein Ziel definiert und im weiteren Verlauf dieser Maßnahme zielgruppenbezogen verfeinert werden. So können später Inhalte passgenau entwickelt und der Erfolg der Maßnahmen gemessen wer-

den. Bei der Zieldefinition sollte die Frage im Vordergrund stehen, warum Informationssicherheit für die Institution und ihre Mitarbeiter wichtig ist.

Beispiel für eine Zieldefinition:

- Die Mitarbeiter erkennen die Bedeutung von Informationssicherheit für die Institution und ihren Arbeitsplatz.
  Sie kennen die relevanten Gefährdungen und können die Auswirkungen von Sicherheitsvorfällen und Verstößen gegen geltende Regelungen beurteilen. Sie akzeptieren die Maßnahmen zur Informationssicherheit und sind bereit, diese zu beachten und in ihrem Arbeitsumfeld aktiv an deren Aufrechterhaltung und Weiterentwicklung mitzuarbeiten.

Zielgruppenanalyse durchführen

Durch die Zielgruppenanalyse werden Mitarbeiter mit vergleichbaren Merkmalen in Bezug auf die Informationssicherheit identifiziert, wie z. B. ¿Administratoren", "Mitarbeiter der Personalabteilung" oder "externe Mitarbeiter". Weiterhin sollten hier auch Entwicklungen der Mitarbeiterlaufbahn betrachtet werden, die für die Institution charakteristisch sind, z. B. Abteilungs-, Funktions- oder Standortwechsel.

Durch die Zielgruppenanalyse können die Sensibilisierungsmaßnahmen an spezielle Anforderungen und unterschiedliche Hintergründe der Mitarbeiter angepasst werden (siehe M 3.93 *Analyse der Zielgruppen für Sensibilisierungs und Schulungsprogramme*).

Sensibilisierungsziel pro Zielgruppe detaillieren

Die Sensibilisierungsmaßnahmen sind zielgruppengerecht aufzubereiten. Als Ergebnis können z. B. Auswirkungen von Sicherheitsvorfällen für die jeweiligen Mitarbeiter so praxisnah wie möglich beschrieben werden. Weiterhin hat es sich auch als äußerst wirksam erwiesen, Beispiele aus dem privaten Umfeld der Mitarbeiter in Sensibilisierungsprogramme mit aufzunehmen, wie der Verlust der Digitalfotos aus dem letzten Urlaub oder ein verlorenes Smartphone.

Inhalte der Sensibilisierung festlegen

Sensibilisierungskampagnen können alle Themen beinhalten, die begründen, warum Informationssicherheit für die Institution und ihre Mitarbeiter wichtig ist. Hierzu zählen z. B. relevante Gefährdungen oder beispielhafte wie auch reale Sicherheitsvorfälle, an denen richtiges Verhalten trainiert werden kann. Dabei sollte darauf geachtet werden, dass genügend Inhalte einen engen Bezug zur Institution und der angesprochenen Zielgruppe haben. Zusätzlich können Beispiele aus vergleichbaren Institutionen oder aussagekräftigen Publikationen die Inhalte untermauern.

Medien und Methoden auswählen

Es sind solche Medien und Methoden auszuwählen, die sich eng an der herrschenden Kultur der Institution orientieren. Ziel ist es, die Mitarbeiter mit vertretbaren Kosten möglichst eindrucksvoll und nachhaltig zu erreichen und für Informationssicherheit zu sensibilisieren. Das heißt, die Wahrnehmungen, Emotionen und Fähigkeiten der Mitarbeiter für Schwachstellen und Vorfälle in ihrer Arbeitsumgebung müssen gestärkt werden, damit sie diese frühzeitig erkennen, bewerten und richtig darauf reagieren. Dabei sollte auf reine Anweisungstexte, ausführliche und detaillierte schriftliche Regelungen sowie auf eine für die Zielgruppe unverständliche Fachsprache zugunsten einer kurzen

und prägnanten Kommunikation verzichtet werden (siehe auch M 3.47 *Durchführung von Planspielen zur Informationssicherheit*).

Sensibilisierungsmaßnahmen umsetzen

Sensibilisierung und Schulung sind eng verwandte Themen, die sich in der Umsetzung ergänzen und aufeinander aufbauen. Sensibilisierung soll die Mitarbeiter zum Handeln motivieren (siehe M 2.198 *Sensibilisierung der Mitarbeiter für Informationssicherheit*). Die richtigen Verhaltensweisen werden anschließend durch entsprechende Schulungsmaßnahmen weiter unterstützt (siehe M 2.557 *Konzeption eines Schulungsprogramms zur Informationssicherheit*). Es ist in der Praxis eine große Herausforderung, Mitarbeiter für Informationssicherheit zu interessieren und das richtige Verhalten aufrechtzuerhalten. Bekanntermaßen fallen Lernkurven nach Schulungen ohne unterstützende Maßnahmen schnell wieder ab. Deshalb muss der Lernstoff durch geeignete Maßnahmen, z. B. durch regelmäßige Wiederholungen, gefestigt werden (siehe M 3.95 *Lernstoffsicherung*).

Erfolg von Sensibilisierung messen

Der Erfolg der festgelegten Sensibilisierungsziele ist zu messen und auszuwerten. Dafür sollte der Sensibilisierungsstand der Teilnehmer vor, während und nach der Maßnahme anhand geeigneter Kennzahlen oder Kriterien erfasst werden. So lässt sich verfolgen, ob die Kampagne erfolgreich ist und wie sich die Sensibilisierung entwickelt. Weitere Informationen sind in Maßnahme M 3.94 *Messung und Auswertung des Lernerfolgs* dargestellt.

Sensibilisierungsprogramm aktualisieren

Informationssicherheit ist in einer Institution permanenten Veränderungen unterworfen. IT-Systeme, Prozesse, Leistungsspektren, Wettbewerbssituationen wandeln sich und damit einhergehend auch Gefährdungslagen, Risikobewertungen und erforderliche Sicherheitsmaßnahmen. Zusätzlich müssen die Ergebnisse der bisherigen Sensibilisierungsmaßnahmen betrachtet werden, insbesondere notwendige Veränderungen aufgrund der Messung und Auswertung des Lernerfolgs.

Diese Veränderungen müssen daher sorgfältig analysiert werden. Das Sensibilisierungsprogramm ist regelmäßig zu aktualisieren.

Prüffragen:

- Liegt ein zielgruppenorientiertes Sensibilisierungsprogramm vor?
- Wird das Sensibilisierungsprogramm regelmäßig überprüft und aktualisiert?

M 2.390 Außerbetriebnahme von WLAN-Komponenten

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator

Wenn WLAN-Komponenten außer Betrieb genommen werden, müssen alle sensiblen Informationen gelöscht werden. Hierbei müssen insbesondere die Authentikationsinformationen für den Zugang zum WLAN und anderer erreichbarer Ressourcen, die in der Sicherheitsinfrastruktur und anderen Systemen gespeichert sind, entfernt bzw. als ungültig deklariert werden. Dies bedeutet, dass beispielsweise kryptographische Schlüssel sicher gelöscht und Zertifikate für digitale Signaturen gesperrt werden müssen.

Außerbetriebnahme von WLAN-Clients

Als WLAN-Clients findet eine Vielzahl verschiedener Geräte Verwendung. Hierzu zählen unter anderem:

- Laptops
- PDAs, Smartphones und ähnliche Geräte mit WLAN-Unterstützung
- WLAN-fähige Telefone, Drucker und Kameras

Die WLAN-Funktionalität ist typischerweise eine neben diversen anderen Funktionen bei diesen Endgeräten. Bei der Außerbetriebnahme dieser Endgeräte ist daher zu berücksichtigen, ob solche Geräte sicherheitskritische WLAN-Informationen beinhalten, die zu löschen, zu übertragen bzw. zu archivieren sind, z. B.:

- Informationen über den Benutzer des Endgerätes
- Zertifikate bzw. zugehörige private Schlüssel (für Benutzer oder Geräte)
- Kennwörter für WLAN-Zugänge
- Schlüsselmaterial von Authentikationsverfahren wie z. B. WPA-PSK-Schlüssel
- PIM-Daten, also Kontaktinformationen, Termine usw.

Hierfür sind je nach Gerät und Speicherung geeignete Verfahren zur Vernichtung, Löschung oder Wiederverwendung zu nutzen. Bei Zertifikaten ist beispielsweise ein Eintrag in die entsprechende CRL vorzunehmen, um das Zertifikat zu widerrufen.

Falls ein WLAN-Client gestohlen wird, sind mindestens alle oben aufgeführten Informationen zu berücksichtigen, und es ist dafür zu sorgen, dass die Informationen nicht länger zum Zugriff auf WLANs der betroffenen Institution genutzt werden können.

Außerbetriebnahme von Access Points

Bei der Außerbetriebnahme von Access Points ist grundsätzlich das Gleiche zu beachten wie bei WLAN-Clients. Mindestens folgende sicherheitsrelevante Informationen sind, sofern zutreffend, zu löschen, zu übertragen bzw. zu archivieren:

- Pre-Shared Keys (PSK) von WPA bzw. WPA2
- RADIUS-Schlüssel (RADIUS Shared Secrets)
- IPSec-Schlüssel (PSKs bzw. private Schlüssel zu Zertifikaten)
- Benutzerdaten (insbesondere bei integrierten WLAN-Benutzerverwaltungen)
- Konfigurationsinformationen wie z. B. IP-Adressen und Namen von RADIUS-Servern, Name des Access Points selbst, IP-Adresse, SSID

Hierfür sind je nach Gerät und Speicherung geeignete Verfahren zur Vernichtung, Löschung oder Wiederverwendung zu nutzen. Die entsprechenden Verfahren müssen rechtzeitig ausgewählt und getestet werden.

Oft enthalten Access Points weitere Daten (beispielsweise Konfigurationsdaten), die in einem nichtflüchtigen Speicher abgelegt sind, oder sind von außen beschriftet (beispielsweise mit dem Rechnernamen, SSID, IP-Adresse und weiteren technischen Informationen). Diese Informationen sollten nach Möglichkeit vor der Weitergabe des Gerätes entfernt werden, da ein Angreifer auch aus solchen Informationen eventuell Hinweise für mögliche Angriffe ziehen kann.

Es wird empfohlen, anhand der oben gegebenen Empfehlungen eine Checkliste zu erstellen, die bei der Außerbetriebnahme eines Systems abgearbeitet werden kann, damit kein Schritt vergessen wird.

Prüffragen:

- Existieren Vorgaben für die Außerbetriebnahme von WLAN-Komponenten?
- Ist sichergestellt, dass alle sensiblen Daten (z. B. Zertifikate, Passwörter, Benutzerkonten, Beschriftungen, etc.) auf den WLAN-Komponenten zuverlässig gelöscht werden?

M 2.430 Sicherheitsrichtlinien und Regelungen für den Informationsschutz unterwegs

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter
Verantwortlich für Umsetzung: Benutzer, IT-Sicherheitsbeauftragter

Nicht nur innerhalb der Räumlichkeiten einer Institution müssen Informationen angemessen geschützt werden, dies ist natürlich auch außerhalb erforderlich. Mitarbeiter müssen mit sensiblen Informationen auch auf Geschäfts- oder Privatreisen sorgfältig umgehen.

Es sollte eine Sicherheitsrichtlinie erstellt werden, in der beschrieben ist, was Mitarbeiter bei Geschäfts- oder Privatreisen beachten müssen. Diese kann auch in der Richtlinie für die sichere Nutzung mobiler IT-Systeme integriert sein (siehe M 2.309 *Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung*). Zusätzlich sollte für die Mitarbeiter ein kurzes und übersichtliches Merkblatt für das richtige Verhalten unterwegs erstellt werden.

Sensibilisierung der Benutzer

Die Mitarbeiter sollten darüber aufgeklärt werden, dass sie vertrauliche Informationen unterwegs nicht mit fremden Personen austauschen dürfen. Insbesondere sollte die Identität des Kommunikationspartners hinterfragt werden, bevor detaillierte Auskünfte gegeben werden (siehe auch G 3.45 *Unzureichende Identifikationsprüfung von Kommunikationspartnern*). Vertrauliche Informationen sollten auch nicht in Hör- und Sichtweite von Externen diskutiert oder weitergegeben werden.

Weiterhin müssen die Mitarbeiter darüber informiert sein, welche Informationen unterwegs bearbeitet werden dürfen. Hierzu sollten die Informationen entsprechend klassifiziert sein, damit die Benutzer eventuelle Einschränkungen klar erkennen können (siehe auch M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*).

Mitarbeiter sollten unter anderem über folgende Aspekte informiert werden:

- Mitarbeiter müssen sich vor der Reise über die Sicherheitslage, Gebräuche und Gesetze des Reiselandes informieren. Hierbei sind beispielsweise die Länder- und Reiseinformationen des deutschen Auswärtigen Amts hilfreich.
- Auf Reisen sollten möglichst keine sensiblen Informationen mitgeführt werden, die nicht unbedingt benötigt werden. Falls dies doch notwendig ist, sollten diese im Handgepäck mitgeführt werden. Das Gepäck sollte nie unbeaufsichtigt bleiben.
- Sensible Informationen sollten nicht unbeaufsichtigt im Hotelzimmer, in Tagungs- oder fremden Büroräumen verbleiben. Das Verschließen des Gerätes in einem Schrank behindert Gelegenheitsdiebe. Hochschutzbedürftige Informationen sollten allerdings auch nicht in einem hoteleigenen Safe verwahrt werden.
- Für die Kommunikation mit der eigenen Institution und Geschäftspartnern sollten nur gesicherte Verbindungen benutzt werden. Da E-Mails ebenso wie Festnetz- und Mobiltelefone überwacht sein könnten, sollte die Kommunikation möglichst mit einer Ende-zu-Ende-Verschlüsselung abgesichert werden, wenn hochschutzbedürftige Informationen weitergegeben werden. Auch bei fremden Faxanschlüsse ist Vorsicht geboten, da die zu

übertragenden Dokumente auf dem Faxgerät gespeichert und später ausgedruckt, also kopiert werden könnten.
- Mitarbeiter sollten misstrauisch werden, wenn sie sich unterwegs ungewöhnlich stark ausgefragt fühlen. Sie sollten niemals Gespräche mit Fremden über Reisezweck und Arbeitgeber führen.
- Geschenke, die digitale Speicher enthalten, z. B. USB-Sticks, sollten mit besonderer Vorsicht behandelt werden, da diese Schadsoftware enthalten könnten. Die Annahme von Geschenken von Geschäftspartnern kann ohnehin problematisch sein, da Gegenleistungen erwartet werden könnten.

Entsorgung von Datenträgern und Dokumenten

Auch unterwegs gibt es häufiger Material, das entsorgt werden soll, schon alleine, damit das Gepäck noch tragbar bleibt. Während es aber innerhalb der eigenen Institution eingeübte Verfahren gibt, wie alte oder unbrauchbare Datenträger und Dokumente entsorgt werden (siehe auch M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln*), ist dies unterwegs nicht immer möglich. Daher ist vor der Entsorgung ausgedienter Datenträger und Dokumente genau zu überlegen, ob diese sensible Informationen enthalten könnten. Ist dies der Fall, müssen die Datenträger und Dokumente im Zweifelsfall wieder mit zurück transportiert werden.

Weiterhin ist zu beachten, dass Experten auch von defekten Datenträgern unter Umständen wertvolle Informationen zurückgewinnen können. Solche Datenträger dürfen deshalb ebenfalls nicht einfach weggeworfen werden, wenn darauf schützenswerte Daten gespeichert sein könnten.

Auch Akten- und Datenvernichter ("Shredder") in fremden Institutionen sollten mit Vorsicht betrachtet werden, da hier nicht unbedingt ersichtlich ist, wer die Entsorgung durchführt bzw. wie zuverlässig diese ist.

Die Sicherheitsrichtlinie muss daher Regelungen enthalten, wie Mitarbeiter unterwegs mit ausgedienten Datenträgern und Dokumenten umgehen sollen.

Prüffragen:

- Existiert eine Sicherheitsrichtlinie für den Informationsschutz unterwegs?
- Ist jeder Mitarbeiter darüber informiert, was die wichtigsten Sicherheitsmaßnahmen bei Geschäfts- und Privatreisen sind?
- Ist geregelt, wie Mitarbeiter unterwegs mit ausgedienten Datenträgern und Dokumenten umgehen sollen?

M 2.442 Einsatz von Client-Betriebssytemen ab Windows Vista auf mobilen Systemen

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator, Benutzer

Der Einsatz eines mobilen Rechners ist mit typischen Gefährdungen verbunden, die sich aus dem mobilen Einsatz ergeben. Beim Einsatz von Windows ab Windows Vista auf mobilen Rechnern ist, wie für alle mobilen Rechner, der Baustein B 3.203 *Laptop* zu beachten. Für die Bereiche Datenverschlüsselung, Datensicherung und lokal installierte Firewall stellen Clients ab Windows Vista eigene Mechanismen zur Verfügung. Zu diesen werden nachfolgend Empfehlungen ausgesprochen.

Windows Phone 8 ist ein Betriebssystem für Smartphones. Es basiert auf dem Kernel von Windows 8 und beinhaltet somit auch Sicherheitsmechanismen von Windows 8 (z.B. Secure Boot, BitLocker). Die im Folgenden beschriebenen Maßnahmen sind damit z. T. auch für Geräte mit Windows Phone 8 anwendbar.

UEFI Secure Boot

Einige Sicherheitsfunktionen des Betriebssystems können umgangen werden, wenn es einem Angreifer gelingt, auf dem System ein anderes Betriebssystem zu starten, das unter seiner Kontrolle steht. Hierzu kommen oft Live-Systeme zum Einsatz, die von mobilen Datenträgern gebootet werden. Mit "Secure Boot" verfügt der BIOS-Nachfolger UEFI über eine Funktion, die das Booten unautorisierter Betriebssysteme verhindert und beim Booten das eingerichtete Betriebssystem auf Manipulationen untersucht. Auf mobilen Systemen sollte Secure Boot zwingend zum Einsatz kommen. Nähere Ausführungen hierzu finden sich in Maßnahme M 4.49 *Absicherung des Boot-Vorgangs für ein Windows-System*.

Datenverschlüsselung

Mobile Rechner befinden sich häufig in Umgebungen, die ein deutlich niedrigeres Sicherheitsniveau als geschützte Büroumgebungen bieten. Daher sollten die auf dem mobilen Rechner befindlichen schützenswerten Daten verschlüsselt werden (siehe auch M 4.29 *Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme*). Neben einer Reihe von Drittprodukten können zur Verschlüsselung auch die in Windows Vista und Windows 7 integrierten Mechanismen eingesetzt werden:

- EFS (Encrypting File System) kann zur Verschlüsselung einzelner Dateien und/oder Verzeichnisse eingesetzt werden (siehe M 4.147 *Sichere Nutzung von EFS unter Windows*).
- Verschlüsselung der Offline-Dateien.
  Offline-Dateien sind im Grunde Kopien von Dokumenten, die sich auf einer Freigabe im Netz befinden. Sie werden auf dem lokalen Rechner in einer Datenbank gespeichert, so dass der Zugriff auf die Dokumente auch dann erhalten bleibt, wenn die Freigabe im Netz nicht erreichbar ist. Die Möglichkeit, diese Offline-Dateien zu verschlüsseln, wurde unter Windows XP eingeführt.
  Der gesamte Speicher für Offline-Dateien, der Dateien aller Benutzer beinhaltet, wird mit einem computerspezifischen Schlüssel verschlüsselt. Die

Verschlüsselung ist transparent für den Benutzer und kann nur von Administratoren aktiviert und deaktiviert werden.

Der zusätzliche Einsatz des EFS empfiehlt sich, wenn die zu schützenden Daten auf dem mobilen Rechner auch dann verschlüsselt sein sollen, wenn der mobile Rechner ab Windows Vista eingeschaltet ist. Wenn an den Dateien oder Laufwerken, die mittels EFS geschützt sind, gearbeitet wird, liegen auch hier die Daten unverschlüsselt vor.

Unter Windows Vista ohne SP1 empfiehlt sich der Einsatz der Verschlüsselung der Offline-Dateien , wenn der lokale Ordner für Offline-Dateien auf dem mobilen Rechner von der Bootpartition in eine andere Partition verschoben worden ist.

Die Strategie zum Schutz der auf einem mobilen Rechner befindlichen Daten ist nach Bedarf anhand der konkreten Umstände und im Einzelfall festzulegen.

Datensicherung

Zur Vermeidung von Datenverlusten müssen regelmäßige Datensicherungen durchgeführt werden. Vertiefende Informationen hierzu sind in M 6.32 *Regelmäßige Datensicherung* zu finden.

Seit Windows Vista können einzelne Dateien gesichert oder komplette PC-Sicherungsabbilder (Images) von Partitionen erstellt werden (siehe M 6.78 *Datensicherung unter Windows Clients*).

Wenn Netzlaufwerke zur Aufnahme der Datensicherung konfiguriert sind, kann eine Sicherung nur erfolgen, wenn die mobilen Rechner mit dem Backup-Server untereinander vernetzt sind. Die Zeiten zur Datensicherung müssen daher entsprechend geplant werden.

Für die Datensicherung können Wechselmedien eingesetzt werden. Wenn dies beabsichtigt wird, müssen die entsprechenden Zugriffe auf die Wechselmedien zur Datensicherung und zur Datenrücksicherung möglich sein. Dies muss bei der technischen Durchsetzung von Zugriffsbeschränkungen auf Wechselmedien berücksichtigt werden (siehe M 4.339 *Verhindern unautorisierter Nutzung von Wechselmedien unter Windows-Clients ab Windows Vista*).

Die Strategie zur Datensicherung eines mobilen Rechners (Sicherung einzelner Dateien, Windows Complete PC-Sicherungsabbild oder Drittprodukt sowie Sicherungszeiten und -orte) ist nach Bedarf anhand der konkreten Umstände und im Einzelfall festzulegen.

Lokal installierte Firewall

Im Gegensatz zu stationären institutionssinternen Desktops besteht bei mobilen Rechnern die Möglichkeit, dass sie direkt an das Internet angeschlossen werden. Der Schutz durch eine lokal installierte Firewall ist in diesem Fall unabdingbar.

Clients ab Windows Vista bieten mit der Windows Firewall eine Kombination aus "Personal Firewall" und IPSec-Gateway. Die Firewall kann über das Windows Sicherheitscenter konfiguriert werden. Seit Windows 7 kann die Firewall auch im Wartungscenter unter der Rubrik *Sicherheit* konfiguriert werden. Für eine deutlich feiner granulierte Konfigurationsmöglichkeit der Windows Firewall steht seit Windows Vista ein Snap-in für die Managementkon-

sole (*mmc.exe*) zur Verfügung. Ein Snap-in ist eine Ergänzungskomponente einer Konsole für bestimmte administrative Aufgaben.

Die Windows Firewall kann neben eingehenden auch ausgehenden Datenverkehr kontrollieren. In der Standardeinstellung wird der eingehende Datenverkehr bis auf die konfigurierten Ausnahmen blockiert (Whitelist-Ansatz) und der ausgehende Datenverkehr bis auf die konfigurierten Ausnahmen durchgelassen (Blacklist-Ansatz).

Die Standardeinstellung der Windows Firewall hängt von der zugrunde liegenden Windows Version ab. Unter Windows Vista und Windows 7 Enterprise sowie Windows Vista Business und Windows 7 Professional sind an der Windows Firewall nur wenige Ports geöffnet. Unter Windows Vista sowie Windows 7 Ultimate dagegen sind zahlreiche lokale Windows-Dienste von außen erreichbar.

Die Windows Firewall nutzt den Windows Dienst "Network Location Awareness" (NLA). Für jede Netzumgebung (auch Netztyp genannt) kann der Administrator eigene Richtlinien für die Windows Vista beziehungsweise Windows 7 Firewall konfigurieren. Dabei unterscheiden Clients ab Windows Vista die drei Netzumgebungen *Domäne* (bei Windows 7 *Domänennetzwerk)*, *Öffentlich* und *Privat*. Befindet sich ein Client erstmalig in einem Netz, dann erfragt Windows ab Windows Vista vom Benutzer, welche Netzumgebung gerade vorherrscht. Hierzu benötigt der Benutzer administrative Berechtigungen. Liegen diese nicht vor, dann wählt das Betriebssystem ab Windows Vista die Klassifikation *Öffentlich.* Ist das Netz eine Domäne mit dem Windows Client als Mitglied, dann wählt Windows automatisch die Netzumgebung *Domäne/Domänennetzwerk.*

Einmal klassifizierte Netze werden vom NLA-Dienst anhand verschiedener Kriterien wie der MAC-Adresse des Default-Gateways wiedererkannt. Nur ein Benutzer mit administrativen Berechtigungen kann eine andere Klassifikation vornehmen sowie das Verhalten der Windows Firewall für eine bestimmte Klassifikation ändern.

Das Standardverhalten der Windows Firewall gibt folgende Einstellungen für die Netzumgebungen *Domäne*, *Öffentlich* und *Privat* vor.

Für die Netzumgebung *Domäne* gilt:

- Die Windows Firewall wird aktiviert
- Die Windows Firewall bezieht die Richtlinieneinstellungen aus der Active Directory-Domäne.
- Die Konfiguration der Netzerkennung und der Datei- und Druckerfreigabe basiert auf den aus der Active Directory-Domäne herunter geladenen Gruppenrichtlinien.

Für die Netzumgebung *Öffentlich* gilt:

- Die Windows Firewall wird aktiviert.
- Die Netzerkennung (NLA) wird deaktiviert.
- Jegliche Datei- und Druckerfreigabe wird deaktiviert, inklusive der Freigabe von Wechselmedien.

Für die Netzumgebung *Privat* gilt:

- Die Windows Firewall wird aktiviert.
- Die Netzerkennung (NLA) wird aktiviert.
- Jegliche Datei- und Druckerfreigabe wird deaktiviert, inklusive der Freigabe von Medien

Aller Wahrscheinlichkeit nach werden mobile Rechner in unterschiedlichen Umgebungen einen Zugang zu einem Netz haben. Typische Netzumgebungen sind das LAN der eigenen Institution, ein LAN am Heimarbeitsplatz und ein Internetzugang an einem öffentlichen WLAN-Hotspot. Clients ab Windows Vista unterstützen die automatische Erkennung einer Netzumgebung und wenden unterschiedliche Firewall-Regelsätze in Abhängigkeit von der aktuellen Netzumgebung an. Soll der Benutzer diese Eigenschaft nutzen können, muss er zumindest beim ersten Zugang zu einem Netz über administrative Rechte verfügen. Der Benutzer muss dann mindestens in der korrekten Zuweisung einer Netzumgebung und gegebenenfalls auch in der Anpassung von Regelsätzen geschult werden.

Die Strategie zum Einsatz der lokalen Firewall auf einem mobilen Rechner (Netzumgebungs-abhängige Regelsätze, Möglichkeit der Zuordnung der Netzumgebung durch einen Benutzer) ist nach Bedarf anhand der konkreten Umstände und im Einzelfall festzulegen. Dabei ist zu prüfen, ob die windowseigene Firewall auch in komplexeren Szenarien, wie im Zusammenspiel mit einem Virtual Private Network (VPN), die benötigte Schutzwirkung entfaltet oder ob auf ein Produkt eines Drittherstellers zurückgegriffen werden muss.

Prüffragen:

- Ist der Boot-Vorgang bei UEFI-basierten mobilen IT-Systemen mit Secure Boot abgesichert?
- Werden die Daten auf einem mobilen Client ab Windows Vista durch Verschlüsselung und Datensicherung geschützt?
- Wird die Strategie zum Einsatz der lokalen Firewall auf einem mobilen Rechner nach Bedarf anhand der konkreten Umstände und im Einzelfall festgelegt?

M 2.461 Planung des sicheren Bluetooth-Einsatzes

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: IT-Sicherheitsbeauftragter, Leiter IT

Bluetooth kann anhand der vielen verfügbaren Anwendungsprofile in unterschiedlichen Szenarien zum Einsatz kommen. Daher sind im Vorfeld einige Planungen in der Institution notwendig, um Bluetooth sicher betreiben zu können. Generell ist festzulegen, welche Strategie die Institution im Hinblick auf Bluetooth einnimmt und in welchem Umfang die einzelnen Funktionen und Anwendungsprofile verwendet werden sollen.

Generell müssen zwei Arten von Bluetooth-Geräten unterschieden werden:

- Endgeräte mit Bluetooth-Funktionalitäten (kurz: Bluetooth-Endgeräte), beispielsweise Mobiltelefone, Smartphones, Laptops usw..
- Peripheriegeräte mit Bluetooth-Funktionalitäten (kurz: Bluetooth-Peripheriegeräte), beispielsweise Maus, Tastatur, Headset usw.

Bluetooth-Endgeräte verfügen in der Regel über alle Funktionen der Bluetooth-Spezifikationen und die implementierten Sicherheitsfunktionen können frei verwendet werden. Bluetooth-Peripheriegeräte erweitern Bluetooth-Endgeräte durch ihre speziellen Funktionen. Sie können in der Regel die vorhandenen Sicherheitsfunktionen allerdings nur eingeschränkt nutzen. Bluetooth-Peripheriegeräte verwenden dafür meist einzelne Anwendungsprofile der Bluetooth-Endgeräte.

Der Einsatzzweck der Bluetooth-Peripheriegeräte ist meist durch die Bauart festgelegt. So kann ein Bluetooth-Headset ausschließlich zur Sprachübermittlung und eine Bluetooth-Tastatur nur als Eingabegerät verwendet werden. Die Endgeräte haben im Gegenzug eine Vielzahl von Einsatzmöglichkeiten. So kann beispielsweise ein Mobiltelefon über Bluetooth einem Laptop Modem-Funktionalitäten anbieten oder es können Daten zwischen zwei Bluetooth-Endgeräten ausgetauscht werden.

Zunächst muss also überlegt werden, für welche Zwecke innerhalb und außerhalb der Institution Bluetooth-Geräte eingesetzt werden sollen. Im nächsten Schritt ist zu definieren, in welchen Bereichen und unter welchen Rahmenbedingungen Bluetooth eingesetzt werden darf und in welchen nicht. So sollte beispielsweise in Institutionsbereichen, in denen geschäftskritische Informationen verarbeitet werden, keine Bluetooth-Eingabegeräte verwendet werden, da bei diesen über Keylogging-Angriffe Tastatureingaben mitgeschnitten werden könnten. Daher muss klar geregelt sein, welche Bluetooth-Funktionen in welchen Bereichen der Institution eingesetzt werden darf. Auch wenn die Bluetooth-Nutzung innerhalb bestimmter räumlicher Grenzen untersagt wird, können sich trotzdem Geräte mit Bluetooth-Schnittstellen innerhalb dieser Bereiche befinden. Um zu verhindern, dass diese von außen angesprochen werden, sind entweder die Bluetooth-Schnittstellen dieser Geräte zu deaktivieren oder die Mitnahme von Geräten mit Bluetooth-Schnittstellen wie z. B. Mobiltelefonen oder PDAs in diese Bereiche zu verbieten.

Darüber hinaus muss entschieden werden, welche Sicherheitsfunktionen grundlegend eingesetzt werden sollen, um die Bluetooth-Geräte und die Kommunikation zwischen zwei Bluetooth-Geräten abzusichern (siehe M 3.79 *Einführung in Grundbegriffe und Funktionsweisen von Bluetooth*). Diese Entscheidung ist die Grundlage für die sichere Konfiguration und den sicheren

Betrieb der Bluetooth-Geräte (siehe M 4.362 *Sichere Konfiguration von Bluetooth* und M 4.363 *Sicherer Betrieb von Bluetooth-Geräten*). Ebenso müssen Regelungen für die Benutzer existieren, die beschreiben, was bei der Nutzung von Bluetooth-Geräten und deren Sicherheitsfunktionen beachtet muss.

Die Rahmenbedingungen für die Bluetooth-Nutzung müssen in der Sicherheitsrichtlinie der Institution verankert sein.

Um Bluetooth und die damit verbundenen Geräte sicher betreiben zu können, sind die folgenden Punkte wesentlich:

- Die Arbeitsweise und Technik der eingesetzten drahtlosen Kommunikationssysteme müssen von den für den Betrieb Verantwortlichen vollständig verstanden werden.
- Die Sicherheit der eingesetzten Technik sollte regelmäßig evaluiert werden. Ebenso sollten regelmäßig die Sicherheitseinstellungen der benutzten Endgeräte (z. B. Mobiltelefone, Laptops, PDAs) untersucht werden. Sicherheitsrelevante Patches und Updates müssen schnellstmöglich aufgespielt werden.
- Die Rahmenbedingungen für die Bluetooth-Nutzung müssen in der Sicherheitsrichtlinie der Institution verankert sein.
- Es ist festzulegen, ob die Bluetooth-Nutzung genehmigt oder unterbunden werden soll. Beispielsweise kann es aus Sicherheitsgründen sinnvoll sein, die Bluetooth-Nutzung bei dienstlichen IT-Geräten generell oder in bestimmten Bereichen zu untersagen.
- Um die übertragenen Daten zu schützen, müssen Vorgaben ausgearbeitet werden, die sich unter anderem mit der Auswahl adäquater Verschlüsselungs- und Authentikationsverfahren, deren Konfiguration und Schlüsselmanagement beschäftigen.

Sicherheitshinweise für die Bluetooth-Nutzung

Den Benutzern sollten einfache und klare Sicherheitshinweise für die Bluetooth-Nutzung zur Verfügung gestellt werden. In diesen muss unter anderem erklärt werden, welche Verantwortung die Benutzer bei Bluetooth-Nutzung übernehmen, welche Einstellungen an den Bluetooth-Geräten sicherheitsrelevant sind,sowie welche Einstellungen von den Benutzern vorgenommen werden dürfen bzw. müssen und welche von den Administratoren durchgeführt werden. Darüber hinaus ist darin zu definieren welche Arten von Daten über Bluetooth übertragen werden dürfen.

Viele von Endbenutzern verwendete Geräte wie Mobiltelefone oder PDAs besitzen Bluetooth-Schnittstellen, die bei der Auslieferung meistens nicht deaktiviert sind. Es muss klar geregelt sein, ob diese Bluetooth-Schnittstellen genutzt werden dürfen, und wenn ja, unter welchen Rahmenbedingungen.

Um Benutzer nicht mit zu vielen Details zu belasten, kann es sinnvoll sein, eine eigene Bluetooth-Benutzerrichtlinie zu erstellen. In einer solchen Nutzungsrichtlinie sollten dann kurz die Besonderheiten bei der Bluetooth-Nutzung beschrieben werden, wie z. B.

- unter welchen Rahmenbedingungen Bluetooth-Komponenten genutzt werden dürfen,
- wie Bluetooth-Endgeräte korrekt zu installieren und zu verwenden sind,
- welche Schritte bei (vermuteter) Kompromittierung von Bluetooth-Komponenten zu unternehmen sind, vor allem, wer zu benachrichtigen ist.

Die Sicherheit von Bluetooth basiert stark auf der Güte der verwendeten Bluetooth-Passwörter. Diese müssen daher sehr sorgfältig ausgewählt werden, Benutzer und Administratoren sind über deren herausgehobene Bedeutung

zu informieren (siehe auch M 3.80 *Sensibilisierung für die Nutzung von Bluetooth*).

Wichtig ist auch, dass klar beschrieben wird, wie mit Client-seitigen Sicherheitslösungen umzugehen ist. Dazu gehört beispielsweise, dass keine sicherheitsrelevanten Konfigurationen verändert werden dürfen.

Außerdem sollte die Nutzungsrichtlinie ein klares Verbot enthalten, ungenehmigt Bluetooth-Komponenten anzuschließen. Des Weiteren sollte die Richtlinie insbesondere im Hinblick auf die Nutzung von klassifizierten Informationen, beispielsweise Verschlusssachen, Angaben dazu enthalten, welche Informationen über Bluetooth übertragen werden dürfen und welche nicht. Benutzer sollten für Bluetooth-Gefährdungen sowie für Inhalte und Auswirkungen der Bluetooth-Richtlinie sensibilisiert werden.

Prüffragen:

- Existiert eine aktuelle Sicherheitsrichtlinie für die Bluetooth-Nutzung?
- Existieren dokumentierte Rahmenbedingungen für die sichere Bluetooth-Nutzung?

M 2.558 Sensibilisierung der Mitarbeiter zur Informationssicherheit bei Mobiltelefonen, Smartphones, Tablets und PDAs

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter Personal
Verantwortlich für Umsetzung: Personalabteilung, Vorgesetzte

Zusätzlich zur allgemeinen Schulung und Sensibilisierung zur Informationssicherheit (siehe M 3.5 *Schulung zu Sicherheitsmaßnahmen* und M 2.198 *Sensibilisierung der Mitarbeiter für Informationssicherheit*) müssen Mitarbeiter, die Mobiltelefone, Smartphones, Tablets und PDAs einsetzen, für die besonderen Aspekte der Informationssicherheit bei diesen Geräten sensibilisiert werden. Für die Schulungs- und Sensibilisierungsplanung sind daher die Mitarbeiter, die diese Geräte nutzen, gesondert zu erfassen und entsprechend diesem Plan zu schulen und zu sensibilisieren.

Mobiltelefone, Smartphones, Tablets und PDAs sind durch ihre geringe Größe und den vergleichsweise hohen Preis besonders gefährdet, verloren oder gestohlen zu werden. Eine Erhebung der Pointsec aus dem Jahre 2005 in einem großen Chicagoer Taxiunternehmen mit 900 Taxen ergab, dass in einem Zeitraum von sechs Monaten 85619 Mobiltelefone und 21460 PDAs in den Fahrzeugen liegen gelassen worden sind. Mitarbeiter sind daher besonders darauf hinzuweisen, diese Geräte nicht aus den Augen zu lassen und bei einem Verlust umgehend angemessene Maßnahmen wie Ortung, Löschung und Sperrung der Geräte selbst bzw. durch den IT-Betrieb zu veranlassen.

Mit dem Verlust des Gerätes sind, wenn weitere Sicherheitsmaßnahmen fehlen, auch die Daten auf dem Gerät verloren. Heutige Endgeräte können Datenmengen im zweistelligen Gigabyte-Bereich speichern, was ausreichend Platz für vertrauliche Geschäftsdaten, Preiskalkulationen, Adressbücher und E-Mails bietet. Deswegen müssen Sicherheitsmaßnahmen ergriffen werden, wie z. B. die vollständige Verschlüsselung aller Daten auf dem Endgerät und die Sperrung des Gerätes durch ein Passwort, nachdem es mehrere Minuten nicht benutzt wurde. Erfahrungsgemäß werden solche notwendigen Maßnahmen von den Mitarbeitern kritisch gesehen, da der Aufwand bei der Nutzung der Endgeräte steigt. Daher müssen die Mitarbeiter für die hier genannte Gefährdung der Informationssicherheit sensibilisiert und in der zusätzlichen Sicherheitsmaßnahme geschult werden.

Mobiltelefone, Smartphones und Tablets können in der Regel auf das Internet und auf E-Mails zugreifen. Mitarbeiter müssen die damit verbundenen Gefahren kennen: Das Gerät kann mit Schadsoftware infiziert werden. Schützenswerte Daten können vom Gerät gestohlen bzw. das Gerät kann zum Abhören von Raumgesprächen (siehe G 5.95 *Abhören von Raumgesprächen über Mobiltelefone*) und Telefonaten genutzt werden. Daher müssen die Geräte vor Schadsoftware geschützt werden, beispielsweise durch die Installation geeigneter Schutzsoftware. Zudem sollte überlegt werden, den gesamten Datenverkehr der Mobiltelefone, Smartphones oder Tablets über VPN durch einen Server der Institution zu leiten, um dort bereits Schadsoftware und Angriffe abzuwehren. Auch für diese Gefährdungen und die dadurch entstehenden Einschränkungen müssen die Mitarbeiter entsprechend sensibilisiert werden.

Da oft leichtfertig mit der Abhörgefahr im Telekommunikationsbereich umgegangen wird, sollten Institutionen prüfen, inwieweit die bisherigen Maßnahmen zur Aufklärung ihrer Mitarbeiter über Gefährdungen im Telekommunikationssektor ausreichen. Gegebenenfalls ist es angebracht, die Mitarbeiter regelmäßig über die Abhörgefahren zu informieren und damit auch zu sensibilisieren.

Die Mitarbeiter sollten auch darüber aufgeklärt werden, dass sie vertrauliche Informationen nicht ohne Weiteres telefonisch weitergeben sollten. Insbesondere sollte die Identität des Kommunikationspartners hinterfragt werden, bevor detaillierte Auskünfte gegeben werden (siehe G 3.45 *Unzureichende Identifikationsprüfung von Kommunikationspartnern*). Bei der Benutzung von Mobiltelefonen sollten sie außerdem darauf achten, dass vertrauliche Mitteilungen nicht in der Öffentlichkeit besprochen werden. Dies gilt insbesondere auch bei Kurzmitteilungen, die von einer vermeintlich bekannten Nummer abgesendet wurden (siehe G 5.192 *Vortäuschen falscher Anrufer-Telefonnummern oder SMS-Absender* (Spoofing)). Werden über Kurzmitteilungen oder Chats vertrauliche Informationen angefragt, sollte immer durch einen Rückruf überprüft werden, ob die Anfrage wirklich vom vorgegebenen Kommunikationspartner stammt. Eine solche Überprüfung sollte auch stattfinden, wenn unerwartet von einer bekannten Nummer ein Dateianhang oder ein Link geschickt wurde.

Immer wieder kursieren spektakuläre, aber falsche Warnmeldungen (siehe G 5.80 *Hoax*). Damit nicht wertvolle Arbeitszeit auf die Prüfung des Wahrheitsgehaltes solcher Nachrichten verschwendet wird, sollten alle Mitarbeiter schnellstmöglich über das Auftreten eines neuen Hoax informiert werden. Es gibt verschiedene Informationsdienste, die entsprechende Warnungen weitergeben.

Diese Sicherheitsmaßnahmen schränken den Komfort der Endgeräte in der Regel ein. So führt die vollständige Verschlüsselung zu einer längeren Wartezeit beim Einschalten des Gerätes, ein angemessenes Passwort laufend einzugeben, wird als störend empfunden und den kompletten Datenverkehr durch VPN durch einen Server der Institution zu leiten, führt zu längerer Wartezeit beim Surfen im Internet. Zudem erhöht jedes zusätzliche Sicherungsprogramm den Stromverbrauch und verkürzt damit die Akkulaufzeit. Diese Einschränkungen können daher dazu führen, dass die Mitarbeiter Sicherheitsmaßnahmen zu umgehen versuchen, weshalb im Rahmen der Sensibilisierung der Mitarbeiter besonders auf die Gefährdung der Informationssicherheit durch mobile Endgeräte wie Mobiltelefon, Smartphone oder Tablet eingegangen werden muss, damit die Maßnahmen auch dauerhaft wirksam sein können.

Prüffragen:

- Werden die Mitarbeiter für die besonderen Gefährdungen der Informationssicherheit durch Mobiltelefone, Smartphones, Tablets und PDAs sensibilisiert?
- Ist in der Sensibilisierungsplanung die Gruppe der Mitarbeiter mit Mobiltelefonen, Smartphones, Tablets und PDAs besonders berücksichtigt?

M 3.87 Einführung in Lotus Notes/ Domino

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Fachverantwortliche, IT-Sicherheitsbeauftragter

Grundbegriffe und historische Entwicklung der Lotus Notes/Domino-Plattform

Lotus Notes/Domino ist eine Produktfamilie des Bereichs Lotus Software des Herstellers IBM. Ursprünglich von Iris Associates entwickelt, wurde die Lotus Notes Groupware-Plattform das erfolgreichste Produkt der Lotus Software Corporation und über Jahrzehnte die am Markt dominierende Plattform für Kommunikation und Zusammenarbeit (*Communication Platform*). Seit der Verfügbarkeit von Microsoft Exchange und Outlook ist eine kommerzielle Alternative zu Lotus Notes/Domino vorhanden, die ebenfalls signifikante Marktanteile besitzt. Daneben gibt es eine Reihe von Open Source Produkten, mit denen sich die Funktionalität dieser beiden Plattformen abbilden lässt, von denen jedoch nur einzelne Komponenten (wie der Apache Webserver) hohe Marktanteile besitzen.

Mit Aufgabe des IBM Workplace Konzeptes (einer Parallelentwicklung zu Lotus Notes mit Groupware- und Office-Funktionalität auf der technologischen Basis von Open Office und WebSphere Plattform) wurde die Lotus-Produktpalette beim Hersteller strategisch und technisch aufgewertet, bis hin zur strategischen Positionierung des Lotus Notes Full Clients als universellem Client. Das Konzept des universellen Clients sieht die Nutzung eines einzigen Clients für den Zugriff auf unterschiedliche Anwendungen vor und schreibt praktisch die Nutzung eines einzigen Browsers als Client für eine Vielzahl von Web-Anwendungen in die Welt der Fat bzw. Full Clients fort. Hersteller mit umfangreichem Anwendungsportfolio können durch die Bereitstellung eines standardisierten (Full)-Clients für alle angebotenen Anwendungen, die umfangreichere Client-Funktionalitäten als über einen Browser möglich sind, Synergien nutzen.

Offene Standards ergänzen oder ersetzen zunehmend die proprietäre Lotus Notes/Domino-Welt. Lotus Notes/Domino unterstreicht damit zunehmend den Status einer Plattform. Dazu gehört eine breite Reihe von Basis-Diensten, wie E-Mail, Kalender/Terminplaner, Web-Zugriff, Presence und Instant Messaging sowie eine umfangreiche Unterstützung von Anwendungsentwicklung für diese Plattform. Mit eigenentwickelten Anwendungen können die Basis-Dienste um unternehmensspezifische Elemente ergänzt werden, wie z. B. Terminplanung mit Berücksichtigung unternehmensspezifischer Ressourcendatenbanken. Es können aber auch weitgehend unabhängige Anwendungen entwickelt werden, wie z. B. Anwendungen zur Abbildung von Vorgehensmodellen im Projektgeschäft. Hinzu kommen vielfältige Integrationsmöglichkeiten für andere Plattformen, offene Standards und ein Angebot von zusätzlichen Produkten des Herstellers und Dritter für die Lotus Notes/Domino-Plattform.

Im Folgenden wird der Begriff *Lotus Notes/Domino-Plattform* für die Summe der verfügbaren bzw. in der Institution eingesetzten Lotus Notes/Domino-Komponenten eines definierten Releasestandes verwendet, während der Begriff *Lotus Notes/Domino-Umgebung* für eine konkrete Instanz (Installation) mit definierter Funktionalität steht, beispielsweise das über Lotus Domino Dienste und Notes-Clients aufgebaute Intranet der Institution. Innerhalb einer Institu-

tion können mehrere Lotus/Domino-Umgebungen, aber auch mehrere Plattformen (durch den Paralleleinsatz unterschiedlicher Releases von Lotus Notes/Domino) im Einsatz sein.

Die Lotus Notes/Domino-Plattform beinhaltet server- und clientseitige Komponenten, die die anfallende Kommunikation, Datenhaltung und Datenverarbeitung abwickeln.

Lotus Domino ist die Bezeichnung für die serverseitig zu installierende Basiskomponente, während Lotus Notes die clientseitige Basiskomponente bezeichnet. Es ist grundsätzlich möglich, nur serverseitige oder nur clientseitige Komponenten zu nutzen. In der Regel enthält jedoch eine Lotus Notes/Domino-Umgebung sowohl serverseitige wie auch clientseitige Lotus-Komponenten.

Ursprünglich als klassische Client-Server-Anwendung in proprietärer Technologie mit einem Fat Client konzipiert, hat Lotus Notes/Domino grundlegende Änderungen erfahren. Als Clients können mittlerweile auch browserbasierte Clients (iNotes) oder Clients für mobile Endgeräte wie PDAs, Smartphones etc. genutzt werden. Daneben steht der "klassische" Client in einer proprietären (Basic Client) und einer auf dem Standard der Eclipse-Plattform basierenden Variante (*Standard bzw. Full Client*) zur Verfügung. Die Nutzung fremder E-Mail-Clients über POP3 und IMAP-Standards ist gleichfalls möglich.

Serverseitig wurde die Menge der verfügbaren Dienste des Domino-Servers erhöht und eine bessere Anbindung an die unter Web 2.0 zusammengefassten neuen Internet-Standards geschaffen.

Heutige Notes/Domino-Einsatzszenarien können sehr unterschiedlich ausfallen. Von dem einfachen Einsatz als zentrales E-Mail-System mit zusätzlichen Workgroup-Funktionen bis hin zu einer Vielzahl an vernetzten Diensten auf unterschiedlich ausgeprägten Domino-Servern, die im Unternehmens-Intranet, diversen Extranets und an der Schnittstelle zum Internet betrieben werden. Diese Dienste können über unterschiedlich ausgeprägte Clients genutzt werden, wobei Notes/Domino sowohl server- wie auch clientseitig als Integrationsplattform genutzt werden kann, z. B. für den Zugriff auf SAP-Systeme. Aus diesem Grund weder Intranet-Architektur noch Internet-Architektur für den Einsatz von Notes/Domino betrachtet, sondern die Absicherung der von der Notes/Domino-Umgebung bereitgestellten Dienste, abhängig vom Einsatzszenario.

Sicherheitsrelevante Entwicklungen der Lotus Notes/Domino-Plattform

Die Lotus Notes/Domino-Plattform hat sich mit den aktuellen Releases 8.0.x und 8.5.x sowohl bezüglich ihrer Funktionalität als auch der eingesetzten Technologie stark weiterentwickelt. Dies betrifft die Anzahl und Funktionalität der bereitgestellten Domino-Dienste, die Anzahl und Funktionalität der möglichen Domino-Clients sowie die Einsatzszenarien der Plattform.

Aus Sicherheitssicht sind insbesondere folgende Entwicklungen wichtig, um eine Absicherung der Notes/Domino-Plattform vornehmen zu können:

- Die Bedeutung elektronischer Kommunikation und Zusammenarbeit nimmt immer weiter zu. Durch die Einbindung in fast alle Geschäftsprozesse steigt auch Schutzbedarf der über Lotus Notes implementierten Dienste, wie z. B. E-Mail und Intranet-/Extranet-Zugang. Dies führt in Summe zu einem ansteigenden Schutzbedarf der Lotus Notes/Domino-Plattform.
- Zu neueren Internet-Diensten, wie Presence und Instant Messaging, sind bislang wenig Betrachtungen zu potentiellen Gefährdungen vorhanden

und damit auch ein nicht besonders ausgeprägtes Bewusstsein zu den damit verknüpften IT-Risiken.
- Die Architektur der Plattform befindet sich im Wandel: Von einer reinen Client-Server-Architektur mit Fat Client ausgehend ist die Lotus Notes/Domino-Plattform heute eine dienstbasierte Plattform. Diese beinhaltet unterschiedlich konfigurierbare Serverkomponenten und Dienste, eine komplexe Entwicklungsumgebung und mehrere Clients, die entweder für den gesamten Funktionsumfang der Plattform genutzt werden können oder selektiv für definierte Dienste (wie z. B. POP3 und IMAP-Clients für E-Mail).
- Die stark gestiegene Komplexität der Software durch Anbindung an etablierte Plattformen des Herstellers und Standards (DB2 als DBMS, Eclipse, Websphere-Technologie, W3C-Standards) vergrößert erheblich die Anzahl potentieller Schwachstellen und erschwert den Überblick: Architektur, Schnittstellen und kritische Komponenten sind aus Sicherheitsgesichtspunkten zunehmend schwerer zu bewerten.
- Die durch Einbindung neuer Technologieplattformen entstehende Heterogenität der Codebasis (clientseitig Eclipse, serverseitig Websphere-Technologie, Web 2.0-Standards) verlangt ein breiteres technologisches Know-How bei der Absicherung der Lotus Notes/Domino-Plattform.
- Die umfangreichen Integrationsmöglichkeiten der Notes-Plattform, speziell die Alloy-Komponente zur SAP-Integration, aber auch die anderen Möglichkeiten server- und clientseitiger Integration können bei entsprechender Nutzung den Schutzbedarf einzelner Lotus Notes/Domino-Komponenten (z. B. des Clients bei Umsetzung einer Universal Client Strategie) wesentlich erhöhen.

Universeller Client

Obwohl sich vielfach Web-Browser als Anwendungsfrontends durchgesetzt haben, ist für komplexe Anwendungen oftmals noch ein "klassischer" Client vorhanden, der deutlich mehr Funktionalität bieten kann als der "einfache" Web-Browser. Mittels Browser-Plugins oder des Ajax-Frameworks kann zwar die Funktionalität des Browser-basierten Clients erweitert werden, die Absicherung und Wartung der Komponenten wird jedoch erschwert.

Große Anbieter von Software versprechen sich durch das Konzept eines "universellen" Clients zum einen die Vereinfachung bei der Entwicklung klassischer Clients für die angebotenen Anwendungen, zum anderen aber auch die Reduzierung des beim Kunden anfallenden Installations- und Administrationsaufwands.

IBM besitzt mit dem bisherigen, proprietären Notes Client einen breit akzeptierten Client, der die umfangreiche Funktionalität der Lotus Notes/Domino-Plattform erschließt und bei vielen Kunden auch als Client für Eigenentwicklungen unter Lotus Notes/Domino genutzt wird.

Das Eclipse-Framework ist für die Lotus Notes/Domino-Plattform sowohl Entwicklungs-Framework wie auch Runtime-Framework für den Full Client. Das Framework wird von IBM unterstützt und hat als freie Plattform für Java breite Akzeptanz.

Mit der Umstellung des Notes Clients auf die Eclipse-Plattform unter Notes 8 (Standard bzw. Full Client) und der Freigabe der Eclipse-basierten Lotus Notes/Domino-Entwicklungsumgebung Domino Designer hat IBM alle Voraussetzungen geschaffen, um den Notes Client als universellen Client nicht nur für die eigene Produktfamilie, sondern allgemein für Java-basierte Anwendungen zu etablieren.

Die Auswirkungen eines universellen Clients auf die Informationssicherheit können erheblich sein und sind daher im Vorfeld einer Einführung konzeptionell zu betrachten. Folgende Aspekte sind besonders zu berücksichtigen:

- Die Sicherheitsbetrachtung unterschiedlicher Anwendungen vereinfacht sich bei Verwendung eines universellen Clients, da die Sicherheitsmechanismen des Clients nur einmalig bewertet werden müssen.
- Der Schutzbedarf des Clients steigt durch das anzuwendende Maximum- und Kumulationsprinzip für die unterschiedlichen, den Client nutzenden Anwendungen sowohl bei der Verfügbarkeit, Vertraulichkeit wie auch bei der Integrität.
- Die Absicherung kann sich durch die höhere Komplexität des Lotus Notes Clients schwieriger gestalten. Dazu trägt auch bei, dass es sich bei dem Full Client um einen aus einem Entwicklungsrahmenwerk erzeugten Client handelt, der viel offener (und damit angreifbarer) ist als ein reiner, proprietärer Anwendungsclient wie der Basic Client.

Anwendungsintegration mit Lotus Notes/Domino

Die Lotus Notes/Domino-Plattform wird seitens des Herstellers zunehmend auch als Plattform für Anwendungsintegration positioniert. Technisch wird dies durch offene Standards für Schnittstellen und die Ergänzung der proprietären Lotus-Technologie durch bewährte Technologie der WebSphere-Plattform und des Eclipse-Rahmenwerks abgebildet.

Anwendungsintegration über Lotus Notes Clients

Die erweiterten Möglichkeiten der clientseitigen Anwendungsintegration (z. B. über Web Services) sind ein weiteres Plus für den Full Client und stärken die strategische Position des Lotus Notes Clients als universeller Client. Clientseitige Anwendungsintegration ist oftmals einfacher und schneller zu realisieren als serverseitige Anwendungsintegration, da keine oder geringe Eingriffe in die Betriebsabläufe der zu integrierenden Anwendungen erforderlich sind.

Anwendungsintegration über den Lotus Domino Server

Die vorhandenen Möglichkeiten der serverseitigen Integration, z. B. durch die Anbindung von DB2-Datenbanken, über den Domino Application Server oder unter Nutzung des Lotus Enterprise Integrator for Domino (zusätzlich lizenzierbares Produkt der *Lotus Extended Products*), positionieren die Lotus Notes/Domino-Plattform als Alternative zu proprietären Produkten zur Anwendungsintegration.

In Zusammenarbeit mit SAP entwickelte Produkte wie z. B. Alloy ermöglichen den Zugriff auf SAP-Systeme aus dem Lotus Notes Client und stärken damit die Position des Clients als universeller Client, wobei der Domino-Server und der SAP Application Server über entsprechende Plugins kommunizieren.

Analog zum universellen Client steigt auch bei der Nutzung von Lotus Notes/Domino als Plattform zur Anwendungsintegration den Schutzbedarf sowohl der clientseitigen Notes-Komponenten wie auch der entsprechend für Integration genutzten serverseitigen Domino-Komponenten. Die umzusetzenden Sicherheitsmaßnahmen können daher deutlich aufwendiger ausfallen als bei alleiniger Nutzung der Lotus Notes/Domino-Funktionalität und der für die Lotus Notes/Domino-Plattform bereitgestellten Eigenentwicklungen.

M 4.3 Einsatz von Viren-Schutzprogrammen

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator, Benutzer

Zum Schutz vor Schadprogrammen können unterschiedliche Wirkprinzipien genutzt werden. Programme, die IT-Systeme nach sämtlichen bekannten Schadprogrammen durchsuchen, haben sich in der Vergangenheit als wirksames Mittel in der Schadprogramm-Prävention erwiesen. Entsprechend der in M 2.157 *Auswahl eines geeigneten Viren-Schutzprogramms* beschriebenen Anforderungen sollten daher Viren-Schutzprogramme eingesetzt werden.

Bei mobilen Endgeräten, wie Smartphones, Tablets oder PDAs, ist zusätzlich Maßnahme M 4.466 *Einsatz von Viren-Schutzprogrammen bei Smartphones, Tablets und PDAs* umzusetzen.

Schutz von Internet-Diensten

Am zentralen E-Mail-Gateway muss ein Viren-Schutzprogramm eingesetzt werden, das ein- und ausgehende E-Mails prüft.

Alle weiteren Internet-Dienste (HTTP, FTP, etc.) sollten ebenfalls mit spezialisierter Schutzsoftware abgesichert werden. Wenn dies beispielsweise aufgrund von Performance-Problemen nicht möglich ist, muss zumindest die Ausführung aktiver Inhalte von nicht vertrauenswürdigen Seiten technisch unterbunden werden.

Regelmäßige Untersuchung des gesamten Datenbestands

Auch wenn das Viren-Schutzprogramm bei jedem Dateizugriff eine Prüfung auf Schadprogramme durchführt, ist eine regelmäßige Untersuchung aller Dateien auf Clients und Datei-Servern sinnvoll. So können auch Schadprogramme gefunden werden, für die es noch keine Erkennungssignatur gab, als sie gespeichert wurden. In derartigen Fällen muss beispielsweise untersucht werden, ob das Schadprogramm vor seiner Entdeckung bereits vertrauliche Daten gesammelt, Schutzfunktionen deaktiviert oder Code aus dem Internet nachgeladen hat.

Aus Performance-Gründen sollte eine vollständige Prüfung des Datenbestands in Zeiten durchgeführt werden, in denen die IT-Ressourcen nicht stark beansprucht werden. Ideal ist es, wenn die Software die Auslastung des Rechners überwacht und dessen "Arbeitspausen" automatisch für die Überprüfung nutzt. Auf den Arbeitsplatz-Rechnern könnte das Viren-Schutzprogramm z. B. auch mit dem Start des Bildschirmschoners gekoppelt werden.

Datenaustausch und Datenübertragung

Daten, die versendet werden sollen, müssen unmittelbar vor dem Versand auf Schadprogramme geprüft werden. Analog müssen empfangene Daten unmittelbar nach dem Empfang auf Schadprogramme geprüft werden. Diese Überprüfungen sind sowohl beim Zugriff auf Datenträger als auch bei der Datenübertragung über Kommunikationsverbindungen erforderlich. Die Überprüfungen sollten so weit wie möglich automatisiert werden.

Als zusätzliche Maßnahme können Prüfstellen für von außen kommende Programme, Dateien und Datenträger eingerichtet werden. Die Prüfstellen sind separate IT-Systeme, die nicht in das lokale Netz integriert sind. Mittels eines

Viren-Schutzprogramms werden auf den Prüfstellen alle von außen kommenden Programme und Dateien zentral getestet und freigegeben.

Dieses Vorgehen kann beispielsweise notwendig sein, wenn besonders hohe Sicherheitsanforderungen vorliegen oder wenn ein besonders gefährliches Schadprogramm im Umlauf ist.

Wechselwirkungen mit Verschlüsselungstechniken

Beim Einsatz von Verschlüsselungstechniken müssen die potentiellen Auswirkungen auf den Schutz vor Schadprogrammen bedacht werden. Werden Daten verschlüsselt, so können Systemkomponenten bzw. Anwendungen auf diese Daten nicht zugreifen, solange sie nicht über die entsprechenden Schlüssel verfügen. Dies impliziert, dass ein Viren-Schutzprogramm entweder im Kontext des Benutzers laufen oder mit den entsprechenden kryptografischen Schlüsseln ausgestattet werden muss, um eine verschlüsselte Datei auf Schadprogramme überprüfen zu können. Wird jedoch die Benutzer-Kennung, unter der das Viren-Schutzprogramm ausgeführt wird, mit den entsprechenden kryptografischen Schlüsseln ausgestattet, entstehen neue Sicherheitsrisiken, die es zu vermeiden gilt. Daher wird der Einsatz eines residenten Viren-Schutzprogramms empfohlen, welches die Prüfung auf Schadprogramme im Benutzer-Kontext bei jedem Zugriff auf eine Datei durchführt.

Schutz vor unerlaubter Deaktivierung oder Änderung

Die Viren-Schutzprogramme auf den Clients und Endgeräten müssen so konfiguriert sein, dass die Benutzer keine sicherheitsrelevanten Änderungen an den Einstellungen der Viren-Schutzprogramme vornehmen können. Insbesondere muss sichergestellt sein, dass die Benutzer die Viren-Schutzprogramme nicht deaktivieren können.

Prüffragen:

- Sind Viren-Schutzprogramme auf allen IT-Systemen installiert, auf denen dies laut Sicherheitskonzept vorgesehen ist?
- Wird sichergestellt, das sowohl Scanprogramm als auch Signaturen stets auf dem aktuellsten Stand sind?
- Sind die Nutzer mit dem Scanprogramm vertraut, insbesondere mit der Möglichkeit des "On-Demand-Scans"?
- Wird das zentrale E-Mail-Gateway durch ein Viren-Schutzprogramm gesichert?
- Ist für die genutzten Internet-Dienste ein ausreichender Schutz vor Schadprogrammen gewährleistet?
- Wird eine regelmäßige Untersuchung des gesamten Datenbestandes auf Schadprogramme durchgeführt?
- Bei Auffinden eines Schadprogrammes: Wird untersucht, ob das gefundene Schadprogramm vor seiner Entdeckung bereits vertrauliche Daten gesammelt, Schutzfunktionen deaktiviert oder Code aus dem Internet nachgeladen hat?
- Wird bei Datenaustausch und Datenübertragung eine Suche nach Schadprogrammen durchgeführt?
- Ist auch für verschlüsselte Daten ein ausreichender Schutz vor Schadprogrammen gewährleistet?
- Ist sichergestellt, dass die Benutzer keine sicherheitsrelevanten Änderungen an den Einstellungen der Viren-Schutzprogramme vornehmen können?

M 4.114 Nutzung der Sicherheitsmechanismen von Mobiltelefonen

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Benutzer

Mobiltelefone und dazu angebotene Dienstleistungen können an verschiedenen Stellen durch PINs oder Passwörter abgesichert werden. Hierzu gehören:

Zugriff auf die SIM-Karte

Die SIM-Karte kann durch eine vier- bis achtstellige PIN gegen unberechtigten Zugriff geschützt werden. Mit dieser PIN identifiziert sich der Teilnehmer gegenüber der Karte. Gelangt ein Unbefugter in den Besitz einer SIM-Karte, kann er ohne Kenntnis der PIN diese Karte nicht aktivieren. Um eine missbräuchliche Benutzung der SIM-Karte zu verhindern, sollte daher unbedingt die PIN-Abfrage aktiviert werden, sodass die PIN nach dem Einschalten des Mobiltelefons eingegeben werden muss. Die PIN sollte nicht zusammen mit dem Mobiltelefon bzw. der SIM-Karte aufbewahrt werden.

Bei der Auslieferung ist meist die PIN-Abfrage deaktiviert und eine PIN voreingestellt. Bei der ersten Benutzung sollte unbedingt die PIN geändert und aktiviert werden. Hierbei sollte keine triviale oder leicht vorhersagbare PIN gewählt werden (1111, Geburtsdatum, etc.).

Hinweis: Auf der Tastatur der meisten Mobiltelefone sind unter den Ziffern Buchstaben unterlegt. Dies kann dazu benutzt werden, sich statt PINs Passwörter auszuwählen, die leichter zu merken sind, aber natürlich auch wieder nicht zu einfach sein sollten. Beispiel: "4AUGEN" entspricht der PIN "428436".

Nach dreimaliger falscher PIN-Eingabe wird die SIM-Karte in der Regel gesperrt. Um diese Sperre aufheben zu können, muss ein achtstelliger Entsperrcode eingegeben werden. Dieser wird häufig auch als PUK (Personal Unblocking Key) oder Super-PIN bezeichnet. Nach zehnmaliger Falscheingabe der PUK wird die Karte unbrauchbar. Dieser Entsperrcode wird normalerweise in einem PIN-Brief zusammen mit der SIM-Karte ausgeliefert. Er sollte äußerst sorgfältig und vor unbefugtem Zugriff geschützt aufbewahrt werden. Die PUK darf auf keinen Fall zusammen mit dem Mobiltelefon aufbewahrt werden.

Neben der PIN gibt es mit der PIN2 noch eine weitere Geheimzahl, mit der der Zugriff auf bestimmte Funktionen der SIM-Karte abgesichert werden kann. Sie wird häufig benutzt für Konfigurationsänderungen der SIM-Karte, die nicht vom Benutzer selbst durchgeführt werden können, z. B. Nutzungsrestriktionen. Dies kann aber beispielsweise auch ein Firmentelefonbuch sein, das nur nach der Eingabe der PIN2 geändert werden kann. Die PIN2 hat einen eigenen Entsperrcode (PUK2).

Zugriff auf das Mobiltelefon

Darüber hinaus gibt es im Allgemeinen noch einen Sicherheitscode für das Mobiltelefon (Geräte-PIN), um den Zugriff auf bestimmte Funktionen zu schützen. Auch dieser sollte schnellstmöglich auf einen individuell gewählten Wert gesetzt werden. Er sollte notiert und vor unbefugtem Zugriff geschützt aufbewahrt werden. Alternativ bieten moderne Mobiltelefone einen Zugriffsschutz per Passwort, Gesten, Fingerabdruck oder Gesichtserkennung. Das Mobilte-

lefon sollte so eingestellt werden, dass der Sicherheitscode nach einigen Minuten Untätigkeit erneut eingegeben werden muss. Es sollte eine PIN, ein Passwort oder, eine Geste nach der jeweiligen Sicherheitsrichtlinie der Institution gewählt werden. Alternativ kann ein Fingerabdruckscanner benutzt werden. Da eine Gesichtserkennung bereits mit einfachen Fotos vom Gesicht des Benutzers getäuscht werden kann, sollte dieses Verfahren nicht eingesetzt werden.

Diebstahlschutz durch zusätzliche Applikationen

Moderne Mobiltelefone bieten die Möglichkeit, durch zusätzliche Applikationen das Mobiltelefon bei Verlust oder Diebstahl zu orten, seine Daten zu löschen bzw. es komplett zu sperren. Es sollte eine passende Applikation ausgewählt und eingesetzt werden. Die betreffenden Mitarbeiter sollten im Umgang mit dieser Applikation geschult werden.

Zugriff auf Mailbox

Beim Netzbetreiber kann für jeden Teilnehmer eine Mailbox eingerichtet werden, die unter anderem als Anrufbeantworter dient. Da die Mailbox von überall und auch von beliebigen Endgeräten aus abgefragt werden kann, muss sie mit einer PIN vor unbefugtem Zugriff geschützt werden. Bei der Neueinrichtung vergibt der Netzbetreiber hierzu eine voreingestellte PIN. Diese sollte unbedingt sofort geändert werden.

Weitere Kennwörter

Neben den diversen oben aufgeführten Geheimnummern kann es für verschiedene Nutzungsarten noch weitere Kennwörter geben. Dies ist z. B. der Fall beim Zugriff auf Benutzerdaten beim Netzbetreiber. So muss bei Fragen an die Hotline wegen der Abrechnung unter Umständen ein Kennwort genannt werden. Auch kostenpflichtige Dienstleistungen wie z. B. der Abruf von Informationen oder die Durchführung bestimmter Konfigurationen seitens des Netzbetreibers bzw. Mobilfunkanbieters werden häufig durch zusätzliche Kennwörter geschützt. Diese sollten, wie alle anderen Passwörter auch, sorgfältig ausgewählt, sicher aufbewahrt und nicht an Dritte weitergegeben werden.

Generell sollte mit allen PINs und Passwörtern sorgfältig umgegangen werden (siehe auch M 2.11 *Regelung des Passwortgebrauchs*).

Hinweis: Angreifer haben in jüngster Zeit wiederholt versucht, telefonisch die PIN oder PUK von Mobilfunknutzern zu erfragen, indem sie sich als Mitarbeiter eines Netzbetreibers ausgegeben und einen technischen Defekt vorgetäuscht haben. Über Geheimnummern sollte **nie** telefonisch Auskunft gegeben werden!

Es gibt viele verschiedene Sicherheitsmechanismen bei Mobiltelefonen. Welche hiervon vorhanden sind bzw. wie diese aktiviert werden können, ist abhängig vom eingesetzten Mobiltelefon, von der SIM-Karte und vom gewählten Netzbetreiber. Daher sollten die Bedienungsanleitung und die Sicherheitshinweise des Netzbetreibers sorgfältig daraufhin ausgewertet werden. Beim Einsatz von Firmentelefonen empfiehlt es sich, die wichtigsten Sicherheitsmechanismen sowohl vorzukonfigurieren als auch auf einem übersichtlichen Handzettel zu dokumentieren.

Einige Modelle bieten auch die Möglichkeiten von Kennwort geschützten SIM-Locks. Dadurch kann z. B. zusätzlich verhindert werden, dass das Gerät nach einem Diebstahl mit einer anderen SIM-Karte problemlos weiter betrieben wer-

den kann. Weiterhin kann mit einem SIM-Lock verhindert, dass in ein unbeaufsichtigtes Gerät eine SIM mit Schadpotential eingelegt wird.

Prüffragen:

- Wurden die notwendigen Sicherheitsmechanismen für die Nutzung von Mobiltelefonen ausgewählt und auf den Geräten vorkonfiguriert?
- Welche Sicherheitsmechanismen sind für die Nutzung von Mobiltelefonen vorgeschrieben?
- Sind die Benutzer über die notwendigen Sicherheitsmechanismen für die Nutzung von Mobiltelefonen informiert?

M 4.128 Sicherer Betrieb der Lotus Notes/Domino-Umgebung

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator, Fachverantwortliche

Der sichere Betrieb der Lotus Notes/Domino-Umgebung umfasst alle Regeltätigkeiten, die zur Aufrechterhaltung der Funktionsfähigkeit der Lotus Notes/Domino-Umgebung vonnöten sind. Dazu gehört die Administration von Lotus Notes/Domino, die Durchführung von Upgrades und Migrationen, die regelmäßige Datensicherung und bei Bedarf Datenarchivierung sowie die Tätigkeiten zur Überwachung des Betriebs und der Sicherheit der Plattform. Änderungen an den Diensten, die außerhalb von Upgrades und Migrationen stattfinden (z. B. die Aktivierung bislang nicht genutzter Dienste, Inbetriebnahme neuer Datenbanken und Ähnliches), sind vergleichbar mit dem Verfahren bei Upgrades und Migrationen durchzuführen. Dies beinhaltet die Einhaltung der Vorgaben zur Dokumentation (einschließlich der systemseitigen Protokollierung der vorgenommenen Änderungen und Archivierung der Protokolle) und Einhaltung der Vorgaben für kritische Administrationstätigkeiten (z. B. Vier-Augen-Prinzip oder Freigabeverfahren für Dienste oder Komponenten wie Datenbanken oder Schnittstellen).

Betriebskonzept

Der sichere Betrieb der Lotus Notes/Domino-Umgebung erfordert ein Betriebskonzept, das alle angesprochenen betriebsrelevanten Themenfelder ausreichend detailliert regelt. Das Betriebskonzept muss auf weitere betriebsrelevante Konzepte (siehe M 2.207 *Sicherheitskonzeption für Lotus Notes/Domino*) verweisen.

Datensicherung

Eine regelmäßige Datensicherung ist Teil eines sicheren Betriebs und ist in einem Datensicherungskonzept zu dokumentieren. Dieses ist nicht Teil der Notfallvorsorge, sondern Teil des regulären Betriebs der Plattform, ist aber mit der Notfallplanung abzustimmen. Wird diese Vorgehensweise zur Datensicherung auch im Rahmen der Archivierung genutzt, so muss das Datensicherungskonzept mit dem in M 2.207 *Sicherheitskonzeption für Lotus Notes/Domino* beschriebenen Archivierungskonzept abgestimmt werden.

Da Lotus Notes/Domino seine Informationen (sowohl Nutzdaten als auch interne Verwaltungsdaten, Konfigurationen, Protokolle etc.) in proprietären Datenbanken hält, muss das Datensicherungskonzept neben der Sicherung von Konfigurationsdateien (wie notes.ini) auch die Sicherung dieser Datenbanken abdecken. Allgemeine Empfehlungen zur Sicherung von Datenbanken finden sich in der Maßnahme M 6.49 *Datensicherung einer Datenbank*.

Folgende Besonderheiten der Lotus Notes/Domino-Plattform sind zu berücksichtigen:

- Ab Domino Release 5 und dem ODS (*On-Disc Structure*) 41 unterstützt Lotus Notes/Domino die Transaktionsprotokollierung für Datenbanken. Dies ist nicht nur wegen der erweiterten Möglichkeiten der inkrementellen Datensicherung über die Sicherung und das Nachfahren von Transaktionsprotokollen von Bedeutung, sondern auch wegen der Reparatur beschädigter Datenbanken über ein Einspielen des Backups und der Transaktionsprotokolle.

- Die Transaktionsprotokollierung ist für alle Datenbanken mit hohem Schutzbedarf in Bezug auf Verfügbarkeit oder Integrität, insbesondere auch für die Systemdatenbanken von Lotus Notes/Domino, einzurichten. Dabei sind insbesondere die Parameter *Protokollierungsart*, *Automatisches Fixup von beschädigten Datenbanken* und *Leistung zur Laufzeit bzw. beim Neustart* für den Einsatzzweck angemessen zu konfigurieren.
- In den neueren Domino-Versionen ist es möglich, Lotus Notes/Domino-Datenbanken in einer DB2-Datenbank abzulegen und über die Lotus Notes/Domino-Plattform darauf zuzugreifen. Wird diese Möglichkeit genutzt, muss das Sicherungskonzept für Lotus/Notes Domino auch die Sicherung der genutzten DB2-Datenbanken beinhalten.
- Datensicherungen komplexer Betriebsumgebungen mit umfangreichen Abhängigkeiten, die z. B. durch die Verwendung von Replikation entstehen können, sollten möglichst nicht manuell, sondern unter Verwendung dafür geeigneter Sicherungstools durchgeführt werden. Tools des Herstellers der zu sichernden Plattform (im diesem Fall Tivoli Storage Manager und Tivoli Data Protection for Domino) sind oftmals auf die Eigenheiten der Plattform abgestimmt, daher sind die Inkompatibilitätsrisiken geringer als bei Tools von Fremdanbietern.

Anwendungsentwicklung für die Lotus Notes/Domino-Plattform

Wird Anwendungsentwicklung für die Lotus Notes/Domino-Plattform betrieben, gehören zum sicheren Betrieb der Plattform auch die Verfahren zur Überführung der Anwendungen in den Betrieb. Diese müssen nicht nur gewährleisten, dass eine formell richtige Übergabe stattfindet, sondern auch, dass die geforderten Schritte zur Absicherung der Anwendungsentwicklung umgesetzt wurden.

Der Betrieb einer Lotus Notes/Domino-Umgebung mit Eigenentwicklung ist anders abzusichern als der einer Standard-Umgebung, insbesondere auch unter Berücksichtigung der Thematik "Altlagen" und "Produktivnahme von Eigenentwicklungen".

Wie allgemein üblich hat auch für die Lotus Notes/Domino-Plattform eine angemessene Trennung zwischen Entwicklungsumgebungen, Umgebungen für Test und Qualitätssicherung und Produktivumgebungen zu erfolgen. Es ist vielfach möglich, als Entwicklungsumgebungen und Umgebungen für Test und Qualitätssicherung Lotus Notes/Domino-Umgebungen unter Verwendung von Virtualisierung zu nutzen, auch unter dem Aspekt niedrigerer Lizenzkosten (siehe dazu M 2.493 *Lizenzmanagement und Lizenzierungsaspekte in der Beschaffung für Lotus Notes/Domino*). Abhängig vom Schutzbedarf kann auch über Virtualisierung eine ausreichende Trennung der Umgebungen realisiert werden.

Bei der Trennung der Umgebungen ist zu berücksichtigen, dass in der Regel kein Zugriff mit Entwicklerclients (Domino Designer) auf die Produktivumgebungen zuzulassen ist. Sollte ein Entwicklerzugriff auf eine Produktionsumgebung aus betrieblichen Erfordernissen in Ausnahmesituationen benötigt werden, sind im Vorfeld im Rahmen des Betriebskonzepts Verfahren zu definieren, die die Überwachung und Qualitätssicherung dieses Zugriffs sicherstellen. Der Zugriff hat transparent und anhand der Protokollierung nachvollziehbar zu erfolgen.

Die Verfahren, um eigenentwickelte Anwendungen in den Produktivbetrieb zu übernehmen, müssen sicherstellen, dass:

- eine formelle Abnahme der Anwendung durch die Verantwortlichen erfolgt,

- fachliche Tests, Integrationstests und Performanztests der Anwendung in ausreichendem Maß durchgeführt wurden,
- die in die Produktivumgebung eingebrachten Objekte und die getesteten Objekte übereinstimmen,
- die in die Produktivumgebung eingebrachten Objekte frei von Schadsoftware (siehe hierzu auch B 1.6 *Schutz vor Schadprogrammen*) sind und
- die Richtlinie für die Anwendungsentwicklung für die Notes/Domino-Plattform (siehe M 2.207 *Sicherheitskonzeption für Lotus Notes/Domino*) bei der Entwicklung nachvollziehbar angewendet wurde.

Bei zugekauften Anwendungen für die Lotus Notes/Domino-Umgebung sollten im Rahmen der Möglichkeiten vergleichbare Qualitätsmaßstäbe gelten wie für Eigenentwicklungen, wobei die Einhaltung der Richtlinie für die Anwendungsentwicklung durch entsprechende Aussagen und Zertifizierungen des Herstellers zu ersetzen ist.

Anwendungsintegration mit der Lotus Notes/Domino-Plattform

Anwendungsintegration mit Lotus Notes/Domino (siehe M 2.493 *Lizenzmanagement und Lizenzierungsaspekte in der Beschaffung für Lotus Notes/Domino*) kann die Sicherheitsanforderungen an die Plattform im Betrieb völlig verändern.

Clientseitige Anwendungsintegration kann den Schutzbedarf des Lotus Notes Clients bezüglich aller drei Grundwerte erhöhen. Dies gilt auch für die Nutzung spezieller Integrationskomponenten wie das gemeinschaftlich mit SAP entwickelte Produkt *Alloy* zum Zugriff auf SAP-Systeme aus Lotus Notes. Dies hat in der Regel Auswirkungen auf die Konfiguration und Nutzung des Notes Clients. Die in M 4.229 *Sicherer Betrieb von Smartphones, Tablets und PDAs* geforderte sichere Konfiguration des Clients muss dies berücksichtigen. Der sichere Betrieb der Plattform ist um eine entsprechende clientseitige Protokollierung und Auswertung, mit Fokus auf die clientseitig integrierten Anwendungen, zu ergänzen.

Serverseitige Anwendungsintegration kann beispielsweise über die Nutzung von DB2-Datenbanken für Notes-Daten realisiert werden, oder aber über die Nutzung spezieller Integrationskomponenten. Daneben gibt es weitere Integrationslösungen über den Domino DIIOP-Dienst, Domino XML (DXL) und Domino JSP, die insbesondere die Integration mit der Websphere-Middleware unterstützen. Die Nutzung von Web Services der eigenen Institution oder von Fremdanbietern über die entsprechenden Schnittstellen von Lotus Notes/Domino fällt auch unter diese Betrachtungen.

Bei serverseitiger Anwendungsintegration erhöht sich der Schutzbedarf der entsprechenden Notes/Domino-Anwendungen und Dienste entsprechend unter Berücksichtigung des Schutzbedarfs der über die Integration eingebundenen Anwendungen und Dienste. Dies ist sowohl bei der serverseitigen Konfiguration der Dienste des Domino-Servers aus M 4.116 *Sichere Installation von Lotus Notes/Domino* zu berücksichtigen wie auch in der Festlegung der in M 4.132 *Überwachung der Lotus Notes/Domino-Umgebung* zu monitorenden Parameter und Ereignisse. Auch die Parameter für das in M 4.427 *Sicherheitsrelevante Protokollierung und Auswertung für Lotus Notes/Domino* beschriebene Logging sind anzupassen.

Anwendungsintegration ist daher, wie unter M 2.207 *Sicherheitskonzeption für Lotus Notes/Domino* gefordert, konzeptionell im Rahmen einer Richtlinie für die Anwendungsintegration zu betrachten. Die Einhaltung der Richtlinie ist bei der Produktivnahme der Integrationslösung zu prüfen.

Ist der Betrieb der Lotus Notes/Domino-Umgebung (oder einzelner Komponenten hiervon) ausgelagert, verbleibt die Verantwortung für die Gewährleistung eines sicheren Betriebs bei der auslagernden Institution, während die Durchführung der dazu erforderlichen Regeltätigkeiten bei der Institution und/oder einem oder mehreren Dienstleistern stattfindet. Der IT-Grundschutz-Baustein B 1.11 *Outsourcing* beschreibt die für eine Auslagerung oder Teilauslagerung erforderlichen besonderen Sicherheitsmaßnahmen.

Upgrades und Migrationen im Betrieb

Für den sicheren Betrieb der Lotus Notes/Domino-Umgebung sind die in M 4.116 *Sichere Installation von Lotus Notes/Domino* angeführten Hinweise zu Upgrades und Migrationen zu berücksichtigen.

Administrationstätigkeiten

Die administrativen Tätigkeiten sind nach Möglichkeit anhand eines Administrationshandbuches, das die in M 2.206 *Planung des Einsatzes von Lotus Notes/Domino* angesprochene Planung administrativer Tätigkeiten dokumentiert, durchzuführen. Insbesondere bei Auslagerungen ist dies das Mittel, um eine nachvollziehbare Qualität kritischer Administrationstätigkeiten zu gewährleisten. Der Detaillierungsgrad dieses Administrationshandbuches ist abhängig vom Schutzbedarf der Lotus Notes/Domino-Plattform. Die Verbindlichkeit des Administrationshandbuches für die Durchführung administrativer Tätigkeiten ist sicherzustellen, entweder über die Verabschiedung als institutionseigene Richtlinie oder, bei ausgelagerter Administration, über die Aufnahme in die Vereinbarungen zur Erbringung der Dienstleistung.

Überwachung im Betrieb

Eine Überwachung der Lotus Notes/Domino-Umgebung im Betrieb ist erforderlich. Die Maßnahmen M 4.132 *Überwachung der Lotus Notes/Domino-Umgebung* und M 4.427 *Sicherheitsrelevante Protokollierung und Auswertung für Lotus Notes/Domino* beschreiben weitere Aspekte, die als Teil des sicheren Betriebs der Lotus Notes/Domino-Plattform umzusetzen sind.

Nutzung von Lotus Notes/Domino als führendes System für institutionsweites Identitätsmanagement

Die Zertifikatshierarchie (PKI) von Lotus Notes/Domino kann als Basis des institutionsweiten Identitätsmanagements genutzt werden. Dies hat in der Regel sehr große Auswirkungen auf den Schutzbedarf der Lotus Notes/Domino-Umgebung, da das Identitätsmanagement in der Regel der Kern des zentralen Berechtigungsmanagements ist. Eine solche Situation erfordert im Betrieb meistens einen im Hinblick auf alle Grundwerte strikt abgesicherten, dedizierten Domino-Server, der die dafür erforderlichen Dienste bereitstellt.

Die erforderliche Planung für die Nutzung der Zertifikatshierarchie von Lotus Notes/Domino als Basis des ist bereits in der Maßnahme M 2.206 *Planung des Einsatzes von Lotus Notes/Domino* unter den Punkten "Architekturplanung unter Berücksichtigung von Sicherheitsaspekten", "Planung der Rolle von Notes/Domino im institutionsweiten Identitätsmanagement", "Planung der Domänen- und Zertifikatshierarchie" umrissen.

Aus betrieblicher Sicht müssen insbesondere die administrativen Prozesse rund um die Zertifikatshierarchie sowie die Überwachung, Protokollierung und Auswertung und die Archivierung den erhöhten Schutzbedarf des Servers, der die Dienste der Zertifikatshierarchie bereitstellt, berücksichtigen.

Anbindung von Lotus Notes/Domino an ein externes, zentrales Identitätsmanagement

Die Anbindung von Notes/Domino an ein externes, zentrales Identity-Management von Fremdanbietern (wie z. B. den *Oracle Identity Manager*, das *Microsoft Identity and Access Management*, *Novell eDirectory*) oder des eigenen Herstellers (*IBM Tivoli Identity Management*) ändert den Schutzbedarf der Lotus Notes/Domino Zertifikatshierarchie.

Abhängig vom Schutzbedarf der Lotus Notes/Domino-Umgebung wird die Schnittstelle zur Anbindung an das externe Identitätsmanagement in der Regel im Hinblick auf alle Grundwerte entsprechend hohen Schutzbedarf aufweisen. Dies ist in den betrieblichen Prozessen, insbesondere in der Administration, Überwachung, Protokollierung und Auswertung entsprechend zu berücksichtigen. Bei Umsetzung von M 6.73 *Notfallplanung und Notfallübungen für die Lotus Notes/Domino-Umgebung* ist der Ausfall des externen Identitätsmanagements bzw. der Anbindung an das externe Identitätsmanagement angemessen zu berücksichtigen.

Prüffragen:

- Ist ein dokumentiertes Betriebskonzept oder eine vergleichbare Betriebsdokumentation für die Lotus Notes/Domino-Umgebung vorhanden?
- Berücksichtigt das Datensicherungskonzept die Größe und Komplexität der zu sichernden Datenbanken?
- Ist die Vorgehensweise zur Produktivnahme von Anwendungen für die Lotus Notes/Domino-Umgebung dokumentiert?
- Ist die Vorgehensweise bei den wesentlichen Administrationstätigkeiten im Betrieb dokumentiert?
- Werden die Domino-Server, auf denen der CA-Prozess (Zertifizierungsprozess) läuft, bei entsprechender Nutzung der Domino-Zertifikatsinfrastruktur entsprechend überwacht und protokolliert?
- Ist bei Nutzung der Domino-CA (Certificate Authority, Zertifizierungsstelle) für weitere Anwendungen außerhalb der Lotus Notes/Domino-Plattform der erhöhte Schutzbedarf von Lotus Notes/Domino berücksichtigt?
- Ist bei einer vorhandenen Lotus Notes/Domino-Anbindung an ein externes, zentrales Identitätsmanagement dies in dem Betriebshandbuch entsprechend berücksichtigt?

M 4.228 Nutzung der Sicherheitsmechanismen von Smartphones, Tablets und PDAs

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Benutzer, Administrator

Smartphones, Tablets oder PDAs und zugehörige Anwendungen können an verschiedenen Stellen durch PINs oder Passwörter abgesichert werden. Alle Benutzer müssen sich über Wirkung und Grenzen der Sicherheitswerkzeuge im Klaren sein.

Zugriffsschutz für Smartphone, Tablet oder PDA

Heute besitzen alle mobilen Endgeräte eine Zugriffssicherung, die meistens über eine Passwortabfrage realisiert ist. Auch wenn nicht alle vom Hersteller angebotenen Sicherheitsmechanismen so sicher sind, wie es wünschenswert wäre, sollten sie benutzt werden, solange nichts Besseres vorgegeben ist.

Im Auslieferungszustand der Geräte ist meist die Passwortabfrage deaktiviert und oft ein triviales Passwort voreingestellt. Bei der ersten Benutzung muss daher das Passwort geändert und aktiviert werden, sodass zumindest bei jedem Einschalten des Gerätes eine Passwort-Eingabe erforderlich ist. Für diese Passwörter und PINs sollten dieselben Regeln gelten wie für Passwörter zu sonstigen IT-Systemen (siehe M 2.11 *Regelung des Passwortgebrauchs*). Auf keinen Fall dürfen sie zu kurz oder zu einfach gewählt sein. Die Passwörter dürfen keinesfalls zusammen mit dem Smartphone, Tablet oder PDA aufbewahrt werden.

Viele Smartphones, Tablets oder PDAs lassen sich über die USB-Schnittstelle mit einem PC sehr leicht administrieren und stellen über USB oder sogar die Luftschnittstelle weitreichende Systemfunktionen (sogenannte Debugging-Funktionen) bereit. Diese Schnittstelle muss deaktiviert werden, wenn sie nicht benutzt wird, da sonst ohne Kenntnis des Benutzers Daten ausgelesen oder beliebige Anwendungen installiert oder deinstalliert werden können.

Automatische Sperre / Pausenschaltung

Smartphones, Tablets oder PDAs sehen im Allgemeinen auch die Möglichkeit einer automatischen Sperre vor, die sich bei Arbeitsunterbrechungen nach kurzer Zeit selbst aktiviert. Erst nach Eingabe des entsprechenden Passwortes ist die weitere Nutzung des Endgerätes möglich. Ist eine Pausenschaltung vorhanden, so sollte sie unbedingt genutzt werden. Der Zugriffsschutz sollte sich bereits nach einer kurzen Phase von Inaktivität einschalten, zu empfehlen sind hier maximal 5 Minuten.

Benutzer-Information

Damit ein ehrlicher Finder eines Smartphones, Tablets oder PDAs weiß, an wen er sich wenden kann, sollte das Endgerät so eingerichtet werden, dass nach dem Einschalten eine entsprechende Information auf dem Bildschirm erscheint. Bei privat genutzten Smartphones, Tablets oder PDAs sollte hier möglichst nicht die vollständige Privatadresse angegeben werden, damit ein Dieb nicht auch noch diese Information für einen Einbruch bei einer vermuteten Abwesenheit des Benutzers ausnutzen kann. In der Regel reichen der Name und eine E-Mail-Adresse aus. Wenn diese Funktion nicht systemseitig

zur Verfügung steht, sollte eine entsprechende Applikation installiert oder ein eigens gestalteter Sperrbildschirmbild dafür verwendet werden.

Weitere Sicherheitsmechanismen

Es gibt viele verschiedene Sicherheitsmechanismen bei Smartphones, Tablets oder PDAs wie Verschlüsselung oder zeitgesteuerte Deaktivierung. Welche hiervon vorhanden sind bzw. wie diese aktiviert werden können, ist abhängig vom eingesetzten Endgerät. Daher sollte die Bedienungsanleitung sorgfältig daraufhin gelesen werden. Sollen auf einem Smartphone, Tablet oder PDA vertrauliche und besonders zu schützende Daten gespeichert werden, so sollten diese verschlüsselt werden. Bietet das Endgerät keine eingebaute Verschlüsselungsfunktion, so sollte ein zusätzliches Verschlüsselungsprodukt eingesetzt werden.

Beim Einsatz von Smartphones, Tablets oder PDAs in Behörden oder Unternehmen empfiehlt es sich, die wichtigsten Sicherheitsmechanismen sowohl vorzukonfigurieren als auch auf einem übersichtlichen Handzettel verständlich für die Benutzer zu dokumentieren. Wenn möglich sollte dieser Zettel auch in elektronischer Form auf dem Endgerät an einer leicht zu findenden Stelle hinterlegt werden.

Prüffragen:

- Verfügen die eingesetzten Smartphones, Tablets oder PDAs über Einschalte-Passwörter? Sind diese aktiviert?

M 4.229 Sicherer Betrieb von Smartphones, Tablets und PDAs

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator, Benutzer

Die sinnvolle Nutzung von Smartphones, Tablets oder PDAs erfordert im Allgemeinen eine Kopplung mit anderen IT-Systemen, beispielsweise dem Arbeitsplatzrechner, einen Serverdienst für die Geräteverwaltung oder -steuerung oder einen Cloud-Dienst. Die Installation und Konfiguration der dafür benötigten Hard- und Software sollte zentral geregelt sein und durchgeführt werden. Ohne entsprechende Tests und Freigaben sollte keinerlei Installation erfolgen. Bei vielen Smartphones und Tablets ist die Synchronisation mit Cloud-Diensten voreingestellt und erfolgt nahezu automatisch. Es muss verhindert werden, dass ungewollt Daten zu diesen Diensten abfließen. Dies ist insbesondere bei jeder neu installierten Anwendung zu prüfen. Gegebenenfalls sind entsprechende Gegenmaßnahmen zu ergreifen.

Sicherheitsmechanismen und -einstellungen für mobile Endgeräte sollten festgelegt und für die Benutzer verständlich dokumentiert werden, damit sie die Geräte korrekt benutzen können. Daher ist explizit zu verbieten, dass die Konfiguration geändert wird. Außerdem müssen die Benutzer für Sinn und Zweck der gewählten Einstellungen sensibilisiert werden. Soweit technisch möglich, sollten Sicherheitsmechanismen so gewählt und konfiguriert werden, dass die Benutzer möglichst wenig Einflussmöglichkeiten haben. Dies ist in der Regel am einfachsten durch eine zentrale Mobile Device Management-(MDM)Lösung möglich. MDM-Lösungen können Passwortrichtlinien erlassen, Konfigurationen überprüfen, installierte Anwendungen verwalten und den Patch-Stand vom Betriebssystem und der Virenschutz-Software überprüfen. Es wird empfohlen eine MDM-Lösung einzusetzen oder zumindest zu prüfen, ob damit der sichere Betrieb von Smartphones, Tablets und PDAs am effizientesten erreicht wird (siehe auch M 4.230 *Zentrale Administration von Smartphones, Tablets und PDAs*).

Smartphones, Tablets und PDAs sind in der Regel nicht in der Lage, verschiedene Benutzerkonten bereitzustellen. Daher gibt es auch im Allgemeinen keine ausgefeilten Mechanismen zur Rollentrennung. Das bedeutet insbesondere, dass es selten Bereiche gibt, die nur für Administratoren zugänglich sind. Benutzer können also nicht ohne Weiteres daran gehindert werden, sicherheitsrelevante Konfigurationsänderungen durchzuführen. Dies kann nur durch entsprechende Regelungen und Sensibilisierung der Benutzer erreicht werden. Hilfreich ist es außerdem, regelmäßig die Einstellungen zu kontrollieren bzw. diese durch Administrationstools bei der Synchronisierung wieder auf die vorgegebenen Werte zurückzusetzen.

Die Sicherheit aller zur Synchronisation mit dem Smartphone, Tablet oder PDA benutzten Endgeräte ist wesentlich für die Sicherheit des jeweiligen mobilen Geräts. Wenn auf den stationären Endgeräten Daten oder Programme manipuliert worden sind, können diese auf das Smartphone, das Tablet oder den PDA durchgereicht werden, ohne dass dies erkannt werden kann.

Die Synchronisationssoftware sollte so konfiguriert werden, dass vor der Installation von Programmen eine Rückfrage beim Benutzer erfolgt. Der Synchronisationsvorgang sollte nicht unbeobachtet ablaufen. Es sollte protokolliert werden, welche Programme und Daten jeweils transferiert bzw. aktuali-

siert wurden und diese Protokolle sollten zumindest sporadisch auf ungewöhnliche Einträge überprüft werden.

Für die Auswahl und Installation von Applikationen ist ein geeignetes Test- und Freigabeverfahren umzusetzen (siehe M 4.467 *Auswahl von Applikationen für Smartphones, Tablets und PDAs*). Werden in einer Behörde oder einem Unternehmen private Smartphones, Tablets oder PDAs dienstlich benutzt, sind solche Verfahren, wenn überhaupt, viel schwieriger umzusetzen.

In der Sicherheitsrichtlinie sollte festgehalten werden, welche Daten und Programme auf den Smartphones, Tablets oder PDAs gespeichert werden dürfen. Davon hängen auch weitere Sicherheitsmaßnahmen ab. Beispielsweise hat ein Tablet, auf dem ausschließlich weniger schützenswerte Daten gespeichert werden, einen anderen Schutzbedarf als ein Endgerät, auf dem kryptografische Schlüssel und Zugangsparameter für IT-Systeme und Netze abgelegt sind.

Es gibt Schadprogramme, die speziell für Smartphones, Tablets oder PDAs konzipiert worden sind. Sie lesen persönliche Daten aus, rufen kostenpflichtige Servicerufnummern an oder versenden SMS-Spam. Einige Schadprogramme sind auch darauf spezialisiert, Authentisierungsinformationen, beispielsweise die mobile TAN für Online-Banking, an Kriminelle weiterzuleiten. Die meisten Hersteller von Viren-Schutzprogrammen haben deswegen Virenscanner für Smartphones, Tablets oder PDAs in die Produktpalette mit aufgenommen. Nicht vergessen werden darf in diesem Zusammenhang auch der Virenschutz aufseiten der zur Synchronisation eingesetzten Endgeräte oder Diensteanbieter. Auch diese müssen mit aktuellen Virenschutz-Programmen ausgestattet sein. Dies muss insbesondere auch für private PCs oder Laptops gelten, mit denen das dienstliche Endgerät eventuell auch synchronisiert wird.

Wenn über Smartphones, Tablets oder PDAs Internet-Dienste genutzt werden, muss jede Datenverbindung zur Institution verschlüsselt werden, beispielsweise durch ein VPN. Zudem sollte der E-Mail-Client und Web-Browser SSL bzw. TSL beherrschen und hierüber auch verschlüsselt kommunizieren, beispielsweise für den Zugriff auf unternehmens- oder behördeninterne Server. Einige der für mobile Endgeräte verfügbaren Browser unterstützen auch aktive Inhalte, also Java, ActiveX und/oder Javascript. Wie bei anderen IT-Systemen ist auch hier zu beachten, dass je nach Art dieser Programme mit ihrem Ausführen eventuell ein Sicherheitsrisiko verbunden sein kann. Daher sollten aktive Inhalte im Web-Browser im Regelfall abgeschaltet sein und nur aktiviert werden, wenn diese aus einer vertrauenswürdigen Quelle kommen, also z. B. von den WWW-Seiten eines ihnen bekannten Anbieters.

Da kleine und mobile Geräte häufig verloren werden, müssen für den Einsatz in einer Institution Bestandsverzeichnisse angelegt werden. Sie sollten mindestens folgende Informationen enthalten: Identifizierungsmerkmale wie Gerätenummern oder Inventarnummern, Art des Gerätes, Betriebssystem, Installationsdatum und Konfigurationsbesonderheiten, Aufstellungsort (wenn stationär), Benutzer sowie Administratoren.

Prüffragen:

- Wird die Installation und Konfiguration von Hard- und Software für die Kopplung von PDAs mit IT-Systemen zentral durchgeführt und geregelt?
- Existiert eine verständliche PDA-Sicherheitsrichtlinie für Benutzer?
- Gibt es ein Test- und Freigabeverfahren für PDA-Applikationen?
- Wird die PDA-Synchronisation protokolliert und sporadisch überprüft?

- Sind PDAs und die zur Synchronisation eingesetzten PCs mit aktuellen Virenschutz-Programmen ausgestattet?
- Gibt es ein PDA-Bestandsverzeichnis?

M 4.230 Zentrale Administration von Smartphones, Tablets und PDAs

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator

Die Administration mobiler Endgeräte ist keine einfache Aufgabe, vor allem bei großen Institutionen und bei Benutzern, die sich häufig und in aller Welt bewegen. Es gibt Tools, die eine zentrale Administration und die Umsetzung von Sicherheitsrichtlinien erleichtern. Mit solchen Tools können dann beispielsweise zentrale Vorgaben an die Passwortgestaltung umgesetzt oder auch der Zugriffsschutz beim Synchronisationsvorgang verbessert werden. Daher sollte ein solches Mobile Device Management (MDM)-Tool eingesetzt werden.

Grundsätzlich ist eine gut überlegte Einbindung in die vorhandene IT-Umgebung notwendig, um die Benutzer durch den Komfort eines MDM-Tools davon abzuhalten, unkontrollierte und damit potenziell unsichere Smartphones, Tablets oder PDAs in die Unternehmens-IT einzuschleppen. Durch eine zentrale Administration können nicht nur Software und Informationen verteilt, sondern auch die organisationseigenen Sicherheitsrichtlinien durchgesetzt werden, z. B. für Authentikation, Zugriff oder Datensicherung.

Beim Einsatz eines MDM-Tools werden Smartphones, Tablets oder PDAs typischerweise nicht mehr mit einem lokalen Endgerät synchronisiert, sondern mit einem Server. Daher können Daten dann nicht nur von einer Station aus abgeglichen werden, sondern von allen mit dem Server verbundenen Geräten. Diese Synchronisation muss kryptografisch abgesichert sein. In vielen Fällen werden die Daten nicht mehr kabelgebunden, sondern per Funktechnik, z. B. über ein WLAN, synchronisiert. Daher sollte beispielsweise darauf geachtet werden, dass hierfür nur kryptografisch abgesicherte WLANs verwendet werden. Ist die Leitung jedoch durch eine verschlüsselte VPN-Verbindung geschützt, kann auch über ein nicht gesichertes WLAN (z. B. in Cafés oder Hotels) synchronisiert werden.

Bei der Synchronisation über einen Server lassen sich aber auch Sicherheitsvorgaben technisch forcieren, indem sicherheitsrelevante Einstellungen auf ihre vorgegebenen Werte zurückgesetzt werden. Typische Funktionen solcher Tools zum zentralen Mobile Device Management sind unter anderem:

- Über Personal Information Manager (PIM) können Termine verwaltet und Adressbücher geführt werden, und dies nicht nur für einzelne Benutzern, sondern auch für Arbeitsgruppen. Das Management der PIM-Daten, anderer Informationen und der Applikationen, die auf den diversen Endgeräten vorhanden sein sollen, kann zentral gesteuert werden. Dadurch können z. B. Applikationen remote installiert und konfiguriert werden.
- Es können aber auch zentrale Adressen-Sammlungen und andere Daten gepflegt und weitergegeben werden. Dies erleichtert besonders bei einer Vielzahl von mobilen Mitarbeitern, die unterwegs eingepflegten Daten den anderen Mitarbeitern schnell und komfortabel zur Verfügung zu stellen.
- Daten können zentral gesichert werden, ohne dass die Benutzer sich darum kümmern müssen. Ebenso kann vorgegeben werden, wann bzw. wie oft Daten zu sichern oder zu synchronisieren sind und welche Randbedingungen dabei eingehalten werden müssen.
- Auch Rückmeldungen über den Status der Smartphones, Tablets oder PDAs sind möglich, sodass Diagnosen aus der Ferne durchgeführt werden können.

- Es können Benutzerprofile angelegt werden, um die Benutzerverwaltung zu vereinfachen.
- Es lassen sich organisationsspezifisch einstellbare Passwortregeln und andere Sicherheitsregeln vorgeben.
- Wenn die MDM-Lösung für verschiedene Benutzungskontexte, wie z. B. privat und dienstlich, ausgelegt ist (siehe M 4.468 *Trennung von privatem und dienstlichem Bereich auf Smartphones, Tablets und PDAs*), kann sie beide Bereiche voneinander trennen. Dies geschieht vielfach über eine Container-Lösung, bei der im Container eine Verwaltung privater PIM-Daten möglich ist oder sogar Anwendungen installiert werden können.
- Viele MDM-Lösungen bieten auch spezielle Maßnahmen für den Fall an, dass das Endgerät verloren geht. So können Smartphones und Tablets mit solchen Programmen aus der Ferne gelöscht, gesperrt und lokalisiert werden. Diese Funktionen sollten von der zentralen Stelle, bei der der Verlust des Endgerätes gemeldet wird, in Absprache mit dem Benutzer und nach vorher klar definierten Regeln ausgeführt werden (siehe M 2.306 *Verlustmeldung* und M 6.159 *Vorsorge vor Verlust und Diebstahl von Smartphones, Tablets und PDAs*).

Diese Funktionen können im Allgemeinen nicht nur über die bei älteren Geräten oft gebräuchlichen Dockingstationen, sondern auch über andere Schnittstellen wie WLAN oder Bluetooth angeboten werden.

Ein Tool zum zentralen Management von Smartphones, Tablets und PDAs sollte möglichst alle in der Organisation eingesetzten Betriebssysteme dieser mobilen Endgeräte unterstützen, damit nicht mehrere solcher Tools parallel eingesetzt werden müssen. Dasselbe gilt natürlich für die eingesetzte Groupware und E-Mail-Plattform.

Prüffragen:

- Werden Tools für das zentrale PDA-Management eingesetzt?

M 4.231 Einsatz zusätzlicher Sicherheitswerkzeuge für Smartphones, Tablets oder PDAs

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator, Benutzer

Es gibt diverse Zusatzwerkzeuge, mit denen die Sicherheit von PDAs verbessert werden kann. Diese bieten erweiterte Sicherheitsfunktionen wie beispielsweise

- Verschlüsselung des Dateisystems und der Speicherkarteninhalte oder auch nur einzelner Dateien oder Datenbanken,
- Verbesserung der Authentisierung, z. B. durch einfachere oder sicherere Authentisierungsverfahren,
- Absicherung der Verbindung zu anderen Komponenten, z. B. durch Verschlüsselung der Kommunikation oder durch Erzeugung von Einmalpasswörtern für die Anmeldung über externe IT-Systeme,
- Virenschutz und
- Verhinderung des unautorisierten Zugriffs auf das Gerät.

Dadurch kann die PDA-Sicherheit bis zu einem gewissen Grad erhöht werden. Dafür müssen die Benutzer die erweiterten Sicherheitsmechanismen aber auch genau kennen. Sie sollten zum einen über deren Nutzen und Schwächen informiert sein und zum anderen über deren Handhabung. Generell sollte aber allen Anwendern klar sein, dass es nahezu unmöglich ist, auf einer unsicheren Plattform mit schwachen Sicherheitsmechanismen eine zuverlässig sichere Applikation zu implementieren. Für viele der PDA-Sicherheitsprodukte sind schon Warnmeldungen über Sicherheitslücken herausgegeben worden. Auch mit der verfügbaren Zusatz-Sicherheitssoftware für PDAs werden nur einige, aber nicht alle vorhandenen Sicherheitsprobleme beim PDA-Einsatz behoben.

Trotzdem sollte geprüft werden, inwieweit solche Tools für den jeweiligen Einsatzzweck sinnvoll sind, da sie helfen, das Gefährdungspotential zu senken. Der Einsatz solcher Tools ist vor allem dann anzuraten, wenn PDAs als Sicherheitstoken oder für die Speicherung sensibler Daten eingesetzt werden. So gibt es beispielsweise Tools zur Verbesserung des Zugriffsschutzes, zur Verschlüsselung einzelner Dateien oder des gesamten Systems und für eine zentrale Administration.

Prüffragen:

- Wurde geprüft, ob der Einsatz zusätzlicher Sicherheitswerkzeuge für PDA sinnvoll ist?
- Werden die Benutzer im Umgang mit den zusätzlichen Sicherheitswerkzeugen geschult?

M 4.234 Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator, Fachverantwortliche, Mitarbeiter

IT-Systeme und Datenträger sind dem ständigen Wandel der Technik unterworfen. Daher werden sie häufiger ausgetauscht als viele andere Arbeitsmaterialien. Bevor IT-Systeme oder Datenträger außer Betrieb genommen werden, muss geklärt werden, wie dies ablaufen soll und wie mit den darauf gespeicherten Informationen umzugehen ist. Es muss vor allem sichergestellt werden, dass weder wichtige Daten, die eventuell auf diesen gespeichert sind, verloren gehen, und noch dass vertrauliche Daten auf den Datenträgern zurück bleiben.

Bevor IT-Systeme oder Datenträger ausgesondert werden, müssen sie gesichtet werden, ob sich darauf noch Daten befinden, die noch benötigt werden. Diese müssen dann auf anderen Datenträgern gesichert bzw. archiviert werden. Es sollte überprüft werden, dass wirklich alle Daten korrekt gesichert wurden. Weitere Informationen zu diesem Themenkomplex finden sich in den Bausteinen B 1.4 *Datensicherungskonzept* und B 1.12 *Archivierung*.

Bei der Außerbetriebnahme eines IT-Systems sollte außerdem geprüft werden, ob noch Datensicherungsmedien vorhanden sind, die während seines Betriebs benutzt wurden. Auch diese müssen gelöscht oder unbrauchbar gemacht werden, wenn die darauf gespeicherten Daten nicht mehr benötigt werden.

Danach muss geklärt werden, ob die IT-Systeme oder Datenträger vernichtet oder an Dritte weitergegeben werden sollen. Häufig werden IT-Systeme nach der Aussonderung weiterverwendet, beispielsweise können ausrangierte IT-Systeme an andere Abteilungen weitergegeben werden, an Mitarbeiter verschenkt oder verkauft werden. Außerdem muss geregelt werden, wie darauf gespeicherte Informationen entweder zur weiteren Verwendung gesichert oder zuverlässig entfernt werden.

Falls Datenträger an Externe weitergegeben werden sollen, müssen diese sicher überschrieben werden. Auch wenn auf den ersten Blick keine schützenswerten Informationen mehr vorhanden sind, können die Daten unzureichend gelöscht worden sein, so dass noch Restinformationen zu finden sind. Es muss sichergestellt sein, dass alle Daten und Anwendungen vorher sorgfältig gelöscht wurden (siehe auch M 2.433 *Überblick über Methoden zur Löschung und Vernichtung von Daten*).

Wurden auf dem Datenträger Daten mit hohem Schutzbedarf gespeichert, führen die Verfahren, um diese Daten zuverlässig zu löschen, häufig zur physikalischen Zerstörung der Datenträger.

Bei der Regelung der Außerbetriebnahme von IT-Systemen und Datenträgern dürfen auch die Geräte nicht vergessen werden, die nicht unbedingt als IT-Systeme wahrgenommen werden, aber eine Vielzahl vertraulicher Daten enthalten können, wie Mobiltelefone, Drucker, Kopierer oder Faxgeräte. Beispielsweise sollte bei Weitergabe oder Verkauf von Faxgeräten darauf geachtet werden, dass die internen Speicher für Telefaxverbindungsdaten und Telefaxin-

halte sicher gelöscht werden. Außerdem sollten alle Kennzeichnungen und Aufkleber von den Geräten und Datenträgern entfernt werden, die Hinweise auf deren vorigen Verwendungszweck geben, wie beispielsweise Etiketten mit IP-Adressen und Rechnernamen.

Ebenso müssen auch die IT-Systeme und Speichermedien sicher gelöscht und entsorgt werden, deren Betrieb und/oder Wartung ausgelagert wurde. Deren sichere Außerbetriebnahme inklusive Entsorgung oder Rückgabe muss in den entsprechenden Verträgen geregelt sein.

Die Vorgehensweise für die Außerbetriebnahme von IT-Systemen und Datenträgern innerhalb der Institution muss nachvollziehbar dokumentiert sein. Es wird empfohlen, anhand der oben gegebenen Empfehlungen eine Checkliste zu erstellen, die bei der Außerbetriebnahme von IT-Systemen abgearbeitet werden kann. Auf diese Weise kann vermieden werden, dass einzelne Schritte vergessen werden. Es empfiehlt sich, dass die einzelnen Schritte vom jeweils Zuständigen schriftlich bestätigt werden.

Prüffragen:

- Existiert eine klar definierte Vorgehensweise zur Außerbetriebnahme von IT-Systemen und Datenträgern?
- Werden bei allen Arten von IT-Systemen und Datenträgern vor einer Aussonderung alle gespeicherten Daten sorgfältig gelöscht?
- Wird die geregelte Außerbetriebnahme von IT-Systemen und Datenträgern innerhalb der Institution nachvollziehbar dokumentiert?

M 4.323 Synchronisierung innerhalb des Patch- und Änderungsmanagements

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator, Änderungsmanager

In den meisten Behörden und Unternehmen werden häufig Änderungen an der IT-Infrastruktur vorgenommen. Auf diese Änderungen muss der Patch- und Änderungsmanagementprozess reagieren. Dabei muss gewährleistet werden, dass die jeweiligen Patches und Änderungen zeitnah und möglichst gleichzeitig auf alle betroffenen IT-Systeme aufgespielt werden.

Bei mobilen Endgeräten oder auch bei Überlastung der verwendeten Netztechnologie kann es vorkommen, dass IT-Systeme bei der Verteilung von Hard- oder Software-Änderungen nicht erreichbar sind. Für solche Fälle müssen geeignete Mechanismen etabliert werden, die sicher stellen, das sich Systeme erst dann wieder am Netz anmelden können, wenn sie mit geeigneten Updates versorgt wurden. Es gibt verschiedene Werkzeuge, die vor einem Zugriff auf das Produktivnetz überprüfen, ob Sicherheitsprogramme und Sicherheitspatches auf dem aktuellsten Stand sind, und bei Sicherheitsmängeln den Zugriff auf das interne Netz abweisen. In der Regel werden solche Tools dazu benutzt, den Softwarestand der Systeme zunächst festzustellen und dann die Software zur Aktualisierung zusammen zu stellen. Je nach Art des Patch- und Änderungsprozesses können diese dann automatisch oder nach vorheriger Freigabe für diese Systeme verteilt und installiert werden. Änderungen die einen Systemneustart erfordern, sollten als letztes installiert werden, oder erst beim Herunterfahren des IT-Systems. Je nach technischer Unterstützung und Umsetzung des Prozesses können die Aktualisierungen auch installiert werden und der danach nötige Neustart kann gesondert freigegeben werden.

Prüffragen:

- Wird auf Veränderungen an der IT-Infrastruktur auch im Patch- und Änderungsmanagementprozess reagiert?

M 4.465 Aussonderung von Mobiltelefonen, Smartphones, Tablets und PDAs

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter
Verantwortlich für Umsetzung: Leiter IT

Immer wieder werden auf gebrauchten Mobiltelefonen, Smartphones, Tablets und PDAs vertrauliche Daten der Vorbesitzer entdeckt und so die Informationssicherheit der Institution, die das Gerät verkauft oder ungenügend ausgesondert hat, verletzt. Auch für gezielte Angriffe werden Endgeräte von Institutionen aufgekauft und auf sensitive Daten hin untersucht.

Auf ausgesonderten Mobiltelefonen, Smartphones, Tablets und PDAs müssen alle schützenswerten Informationen auf geeignete Weise vernichtet werden. Dazu sollten der Gerätespeicher und die gegebenenfalls vorhandene Speicherkarte mit einer speziellen Software gelöscht werden. Das Gerät ist auf den Werkszustand zurückzusetzen. Außerdem muss überprüft werden, ob alle Daten auch wirklich gelöscht wurden, dazu kann der Verantwortliche spezielle Computer-Forensik-Software und Geräte einsetzen. Werden mittels forensischem Ansatz dennoch entsprechend kritische Daten gefunden und es existiert für das spezielle Mobiltelefon keine Methode zum sicheren Löschen, wird empfohlen, das Gerät zu vernichten. Wird nur die externe Speicherkarte ausgesondert oder entsorgt, sollte M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln* beachtet werden.

Soll ein Smartphone, Tablet oder PDA verkauft werden, bei dem durch Maßnahmen zur Informationssicherheit der Betriebssystemkern oder das Betriebssystem verändert wurde, so sollte berücksichtigt werden, dass durch diese Maßnahme in der Regel die Garantie bzw. der Support durch den Hersteller erlischt. Daher ist zu überlegen, ob diese Maßnahmen vor einem Verkauf rückgängig gemacht werden müssen.

Mobiltelefone, Smartphones, Tablets und PDAs dürfen in der Regel nicht über den Hausmüll entsorgt werden. Entsprechende Regelungen zur Entsorgung müssen beachtet und kontrolliert werden.

Prüffragen:

- Ist organisatorisch sichergestellt, dass mobile Geräte ausschließlich kontrolliert ausgesondert werden?
- Werden Hilfsmittel vorgehalten, um Daten sicher zu löschen und das Ergebnis zu kontrollieren?

M 4.466 Einsatz von Viren-Schutzprogrammen bei Smartphones, Tablets und PDAs

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator, Benutzer

Virenschutzprogramme für Smartphones, Tablets und PDAs haben in der Regel eine andere Schutzfunktion als ihre Pendants auf anderen Clients (siehe G 5.193 *Unzureichender Schutz vor Schadprogrammen auf Smartphones, Tablets und PDAs*).

Schutzprogramme gegen Schadsoftware müssen entsprechend dem Schutzbedürfnis der Institution und unter Berücksichtigung der Anforderungen an den Schutz vor Verlust und Diebstahl des Endgerätes (siehe M 6.159 *Vorsorge vor Verlust und Diebstahl von Smartphones, Tablets und PDAs*) ausgesucht werden. Sie sollten zentral installiert und eingerichtet werden.

Die Programme sollten täglich die Signaturdatenbank aktualisieren und mindestens einmal wöchentlich einen kompletten Scan durchführen. Da ein solcher Scan die Prozessor-Ressourcen des Endgerätes für eine gewisse Zeit stark beanspruchen kann, sollte er nur zu Zeiten stattfinden, in denen das Endgerät wenig oder gar nicht benutzt wird. Das Schutzprogramm sollte dabei alle Dateitypen untersuchen und infizierte Dateien zur späteren Analyse in den Quarantäneordner verschieben. Wenn es keine Quarantänefunktion gibt oder eine weitergehende Analyse der Schadsoftware aus anderen Gründen nicht möglich ist, sollte das Programm so eingestellt werden, dass es die infizierten Dateien sofort löscht. In jedem Fall ist über ein solches Ereignis der IT-Support beziehungsweise das Informationssicherheitsmanagement zu informieren. Das befallene Endgerät sollte so schnell wie möglich durch den IT-Betrieb genauer auf weitere Schadprogramme untersucht werden.

Wird ein Smartphone, Tablet oder PDA an einen PC angeschlossen und werden Daten auf dem mobilen Endgerät gespeichert, so sollte das Schutzprogramm die neuen Daten so schnell wie möglich untersuchen. Zudem sollte es auch neu installierte Anwendungen sofort auf Schadsoftware überprüfen und bei einem Virenfund diese deinstallieren.

Es sollte ein Virenschutzprogramm ausgesucht werden, das den Netzverkehr beim Surfen im Internet lokal auf Schadprogramme testet. Die Benutzer müssen darauf hingewiesen werden, dass sie nur mit diesem Schutz im Internet surfen dürfen. Sind die Endgeräte über VPN mit dem Netz der Institution verbunden und wird in der Institution bereits der gesamte Netzverkehr auf Schadprogramme untersucht, muss nicht zusätzlich lokal der Netzverkehr untersucht werden.

Prüffragen:

- Wurde auf dem Endgerät ein Viren-Schutzprogramm installiert, das mindestens wöchentlich alle Nutzerdaten auf Schadsoftware untersucht und täglich seine Viren-Datenbank aktualisiert?
- Ist das Viren-Schutzprogramm so konfiguriert, dass es den Webverkehr auf Schadsoftware untersucht und Infektionen abwehrt?
- Ist das Viren-Schutzprogramm so konfiguriert, dass neue Dateien und Anwendungen umgehend auf Schadsoftware untersucht und bei einem Virenfund gelöscht beziehungsweise deinstalliert werden?

M 4.467 Auswahl von Applikationen für Smartphones, Tablets und PDAs

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator, Benutzer

Applikationen (kurz Apps) für Smartphones, Tablets und PDAs werden in der Regel durch Online-Shops der Endgeräte- oder Betriebssystemhersteller vertrieben. In den regulären Shops werden Applikationen sowohl von großen Unternehmen als auch von einzelnen Entwicklern angeboten. Die Preise für die Applikationen sind sehr unterschiedlich und reichen von kostenlos bis in den mehrstelligen Bereich. Es stehen in der Regel für einen dienstlichen Verwendungszweck sehr viele Applikationen zu Verfügung.

Daneben gibt es noch einige Online-Shops, auf die in der Regel nur über Umwege zugegriffen werden kann, indem entweder ein "Jailbreak" (bei iPhone und iPad) durchgeführt wird oder bei Android in den Einstellungen die Installation aus unbekannten Quellen zugelassen wird. Ein Jailbreak sollte in keinem Fall ausgeführt werden und die Installation aus unbekannten Quellen sollte nur nach eingehender Prüfung der Quelle für einzelne Anwendungen ermöglicht werden.

Applikationen für Smartphones, Tablets und PDAs müssen entsprechend dem Einsatzzweck dieser Endgeräte und dem Schutzbedürfnis der Informationen auf dem Endgerät ausgewählt und vor dem Einsatz getestet werden. Deshalb sollte der IT-Betrieb vor der Installation eine Liste mit gewünschten Funktionen und Eigenschaften erstellen. Zudem sind Kriterien zu definieren, die Applikationen auf keinen Fall besitzen dürfen. Hierunter fällt beispielsweise das unbefugte Versenden des Adressbuches an Adresshändler. Anhand der Vorgaben sollten die infrage kommenden Applikationen auf Nutzerkommentare und Tests durch andere Stellen hin untersucht werden, um festzustellen, ob sie zuverlässig arbeiten und ob Sicherheitsupdates zeitnah zur Verfügung stehen. Danach sollten die jeweiligen Applikationen durch den IT-Betrieb getestet und überprüft werden und erst dann an die Benutzer ausgerollt werden. Es sollte überlegt werden, einen internen Shop für Anwendungen bereitzustellen, über den die Applikationen bezogen werden können.

Wenn es keine Applikationen gibt, die den Qualitäts- oder Sicherheitsanforderungen genügen, müssen die Anwendungen selbst entwickelt werden. Hierfür ist der Baustein B 5.25 *Allgemeine Anwendungen* zu berücksichtigen. Je nach Lizenz einer Anwendung ist es auch möglich, diese den eigenen Bedürfnissen anzupassen und beispielsweise kritische Programmaufrufe, wie etwa zu Werbeservern, Versenden des Adressbuches, grundlose GPS-Lokalisierung auszuschalten. Dies kann eine preiswerte Alternative zur Eigenentwicklung sein.

Wenn die Benutzer weitere Applikationen wünschen, die nicht oder nicht nur dienstlichen Zwecken dienen, sollte es auch dafür einheitliche Regeln geben. Wenn diese Programme, z. B. Kartenspiele oder Sudoku, die Informationssicherheit nicht gefährden und vom Mitarbeiter selbst bezahlt werden, kann die Applikation in der Regel erlaubt werden. Sollte dies nicht der Fall sein, ist dem Mitarbeiter die Entscheidung plausibel zu erklären, damit sie nicht umgangen wird.

Prüffragen:

- Werden Applikationen für die Endgeräte gezielt ausgesucht, angepasst und vor dem Einsatz getestet?

M 4.468 Trennung von privatem und dienstlichem Bereich auf Smartphones, Tablets und PDAs

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter
Verantwortlich für Umsetzung: Leiter IT

Werden Smartphones, Tablets oder PDAs dienstlich und privat benutzt, sollten beide Bereiche strikt getrennt werden. Dies ist auf verschiedene Arten möglich:

- Im einfachsten Fall wird auf den Geräten eine Applikation installiert, die einen Datencontainer mit allen dienstlichen Daten und Zugängen verwaltet. Diese Applikation muss für sämtliche dienstliche Tätigkeiten, wie E-Mail, Termine, Kontakte, Aufgaben, ausgelegt sein, einen eigenen Browser beinhalten und selbsttätig eine verschlüsselte Verbindung zur Institution aufbauen. Die Trennung zwischen den verschiedenen Applikationen erfolgt allerdings ausschließlich durch das Betriebssystem. Daher ist die Wirksamkeit dieser Trennung vom eingesetzten Betriebssystem und dessen Zugriffskontrollmöglichkeiten (Mandatory Access Control, MAC) abhängig und somit von System zu System unterschiedlich.
  Für die Datencontainer-Variante muss in der Regel nicht in das Betriebssystem selbst eingegriffen werden. Sie ist für verschiedene Betriebssysteme erhältlich. Unabhängig von welchem Hersteller eine Applikation für die Trennung zwischen privaten und dienstlichen Daten eingesetzt wird, sollte diese die dienstlichen Daten im Container verschlüsseln und so bei privater Nutzung des Endgerätes den Zugriff auf die Daten durch andere, gegebenenfalls bösartige Applikationen verhindern.
  Es kann zudem sinnvoll sein, dass der IT-Betrieb zusammen mit dem Sicherheitsmanagement eine Ausschlussliste ("Blacklist") von Anwendungen erstellt, die Funktionen oder Rechte besitzen, durch die die Informationssicherheit der dienstlichen Anwendungen gefährdet werden könnte.
  Zusätzlich sollten sich Benutzer vor einem Zugriff auf den Container erfolgreich authentisieren müssen. Verbindungen zum Netz der Institution müssen kryptografisch abgesichert werden. Lösungen, die dies nicht unterstützen, bieten keinen hinreichenden Schutz und sollten daher nicht eingesetzt werden.
- Eine andere Möglichkeit, private und dienstliche Bereiche auf Endgeräten zu trennen, ist, die Informationen auch bei der Verarbeitung auf den Servern der Institution zu belassen. In diesem Fall wird auf dem Client lediglich eine Oberfläche bereitgestellt, mit der über eine abgesicherte Netzverbindung die Anwendung auf einem Server der Institution bedient wird. Das entsprechende Programm auf dem Endgerät muss dabei so konfiguriert werden, dass die Daten nicht lokal gespeichert werden können. Solche Thin-Clients oder serverbasierten Lösungen sind auch im Desktop-Bereich seit Längerem im Einsatz. Damit eine serverbasierte Lösung funktionieren kann, muss jedoch zu jedem Nutzungszeitpunkt eine ausreichend dimensionierte Internetverbindung verfügbar sein. Ferner muss der Dienst auf die Randbedingungen eines Smartphones oder Tablets, zum Beispiel berührungsempfindlicher Touch-Screen statt Maus und Tastatur, angepasst sein.
- Eine weitere Option, besteht darin, die beiden Bereiche als unterschiedliche virtuelle Maschinen auf einem Gerät zu betreiben. Im Gegensatz zur Datencontainer-Variante wird bei der Virtualisierung der private und dienstliche Bereich nicht auf Anwendungsebene, sondern auf Betriebssystemebene getrennt. Dadurch werden die Schnittstellen entfernt, die sonst

zwischen den Anwendungen durch das Betriebssystem mit seinen vorhandenen Zugriffskontroll-Mechanismen bereitgestellt werden. Ein Datenaustausch zwischen beiden virtuellen Maschinen ist nur über die tiefer liegende Virtualisierungsschicht in Form des Hypervisors (auch Virtual Machine Monitor, VMM) möglich. Zudem können in den einzelnen virtuellen Bereichen jeweils eigene Anwendungen installiert und getrennt voneinander betrieben werden. So kann auch dem Bedürfnis der Benutzer Rechnung getragen werden, eigene Apps zu installieren und zu benutzen. Eine Ausschlussliste für Anwendungen ist in diesem Fall in der Regel nicht nötig, da die Anwendungen nur in einer virtuellen Maschine arbeiten und somit Anwendungen im privaten Bereich nicht auf die Daten und Anwendungen im dienstlichen Bereich zugreifen können.

Jede Institution muss prüfen, welche der dargestellten Lösungen dem Schutzbedarf der verarbeiteten Informationen entspricht und der Sicherheitsstrategie der Institution angemessen ist. Generell sollten noch folgende Vor- bzw. Nachteile in die Entscheidungsfindung einfließen:

- Eine Virtualisierungslösung bietet bei entsprechender Qualität des Hypervisors ein höheres Maß an Sicherheit als eine Container-Lösung.
- Bei einer Virtualisierungslösung muss sehr tief in das Betriebssystem eingegriffen werden oder es muss sogar ausgetauscht werden. Viele Gerätehersteller verbieten das und unterbinden es mit technischen Maßnahmen. Auch erlischt in der Regel mit einem solchen Eingriff in das Betriebssystem die Garantie auf das Endgerät.
- Eine Virtualisierungslösung erhöht oft den Stromverbrauch deutlich, sodass der Akku im Vergleich zu einem Gerät ohne Virtualisierung schneller entlädt.
- Eine Virtualisierungslösung ist nicht auf allen Endgeräten realisierbar, da einige Gerätetreiber nicht zur Verfügung stehen.
- Eine Container-Lösung bietet zwar ein geringeres Maß an Sicherheit als die Virtualisierung, aber im Gegenzug wird nicht so tief in das Betriebssystem eingegriffen, sodass die Gewährleistung für das Endgerät in der Regel nicht erlischt.
- Sowohl bei der Container- als auch bei der Virtualisierungslösung können bei Datensicherungen durch die Institution unbeabsichtigt private Daten mit einbezogen werden. Daher muss für die Umsetzung dieser Maßnahme in der Regel auch der Datenschutzbeauftragte hinzugezogen werden. Bei der Virtualisierungslösung ist das unbeabsichtigte Erheben personenbezogener Daten deutlich unwahrscheinlicher, da hier die Trennung zwischen privaten und dienstlichen Bereich strikter umgesetzt ist. Bei der Thin-Client-Lösung ist dies hingegen ausgeschlossen, da keine dienstlichen Daten auf dem Endgerät gespeichert und daher auch nicht gesichert werden müssen.
- Eine Thin-Client-Lösung setzt eine durchgehend verfügbare und ausreichend dimensionierte Internetverbindung voraus. Dies ist in Deutschland nicht flächendeckend gewährleistet, und im Ausland entstehen durch Daten-Roaming in der Regel hohe Kosten. Kurzzeitige Verbindungsausfälle können die Anwendungen auf dem Server beeinträchtigen und gegebenenfalls werden sogar Daten zerstört. Zudem steigt durch die dauerhafte Datenverbindung der Stromverbrauch erheblich an, wodurch die Betriebsdauer bis zum nächsten Aufladen verkürzt wird.

Prüffragen:

- Werden auf den mobilen Endgeräten dienstliche und private Daten durch einen geschützten Container oder durch eine Virtualisierungslösung voneinander getrennt?

- Wird der Datenschutzbeauftragte in die Umsetzung der Maßnahmen zur Trennung von dienstlichen und privaten Daten einbezogen?

M 4.469 Abwehr von eingeschleusten GSM-Codes auf Endgeräten mit Telefonfunktion

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter
Verantwortlich für Umsetzung: Leiter IT

Die Menge an GSM-Codes und ihre Funktion ist herstellerspezifisch für jedes Endgerät anders. In der Regel lassen sich GSM-Codes aber nicht generell abschalten. Damit nicht unbefugt GSM-Codes auf Endgeräten mit Telefonfunktion eingeschleust werden, müssen die folgenden Empfehlungen umgesetzt werden.

Um zu verhindern, dass ein Angreifer GSM-Codes direkt auf dem Endgerät eingibt, sollte das Endgerät nie unbeaufsichtigt sein. Außerdem muss die Code-Sperre aktiv sein.

Um zu verhindern, dass GSM-Codes von Webseiten im Internet auf dem Endgerät ausgeführt werden, müssen Programme installiert sein, die lokal die besuchten Internetseiten durchsuchen und entsprechende GSM-Codes herausfiltern. Dafür gibt es am Markt entsprechende Anwendungen. Diese Filterfunktion ist häufig auch in Virenschutzprogrammen für Smartphones, Tablets und PDAs integriert.

Um zu verhindern, dass GSM-Codes über die Near-Field-Communication-(NFC)-Schnittstelle oder über QR-Code eingeschleust werden, müssen die Applikationen auf dem Endgerät so konfiguriert sein, dass sie die über NFC oder aus QR-Code empfangenen Daten nicht sofort interpretieren und ausführen, sondern erst den Benutzer über den Inhalt der empfangenen Daten informieren und die Ausführung durch ihn bestätigen lassen. Die Benutzer müssen dahingehend sensibilisiert werden, dass sie jede Anfrage auch wirklich prüfen und GSM-Codes immer ablehnen. Dafür muss ihnen vermittelt werden, dass ein GSM-Code mit tel: beginnt und eine URL mit HTTP:// oder HTTPS://.

Prüffragen:

- Ist auf dem Endgerät eine Code-Sperre eingerichtet?
- Verfügt das Endgerät über eine Anwendung, die den Webverkehr auf GSM-Codes hin untersucht und diese Codes herausfiltert?
- Sind auf dem Endgerät nur solche Programme für NFC oder QR-Codes installiert, die den Nutzer über den Inhalt der empfangenen Daten informieren und eine Bestätigung für die Ausführung verlangen?

M 4.484 Speicherschutz bei eingebetteten Systemen

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Entwickler, Beschaffer, Planer

Wenn in einem eingebetteten System mehrere Softwarekomponenten ablaufen, kann es sinnvoll sein, diese zu separieren. Soll nicht für jede Komponente ein eigener Mikrocontroller verwendet werden, kann dies auch durch Speicherschutztechnologien erreicht werden. Ziel des Speicherschutzes ist es, Arbeitsspeicher so zu strukturieren und Bereiche so zu separieren, dass ein Programmierfehler oder Absturz eines einzelnen Programms nicht die Stabilität anderer Programme oder des Gesamtsystems beeinträchtigt. Programme sollen daran gehindert werden, auf den Speicherbereich anderer Programme zuzugreifen.

Um Daten auf dem eingebetteten System mit erhöhten Anforderungen an die Integrität und Verfügbarkeit besser abzusichern, sollen Speicherschutzmechanismen bereits im Entwurf des Systems berücksichtigt werden. Es ist eine Realisierungsform zu wählen, die das benötigte Sicherheitsniveau gewährleistet und den Einsatzerfordernissen des eingebetteten Systems nicht entgegensteht. Die beiden grundsätzlichen Realisierungen sind Hardware-Speicherschutz und Software-Speicherschutz.

Hardwareseitig kann eine Speicherverwaltungseinheit ("Memory Management Unit", MMU) oder eine einfachere Speicherschutzeinheit ("Memory Protection Unit", MPU) den Speicherschutz unterstützen. Mit einer MMU ist es möglich, mehrere virtuelle Prozessoren auf einem physikalischen Prozessor zu vereinen, der durch das Betriebssystem verwaltet wird. Jedes Programm kann seinen eigenen virtuellen Mikrocontroller erhalten, und die Ressourcen des physikalischen Mikrocontrollers lassen sich flexibel zuordnen. MMU sind standardmäßig Bestandteil von Servern, PCs und modernen Smartphones, in kleinen eingebetteten Systemen sind sie normalerweise nicht vorhanden.

Bei einer MPU nutzen alle Programme den gemeinsamen Adressraum des physikalischen Speichers. Die MPU überwacht, auf welchen Speicherbereich ein Programm zugreift. Ist ein Zugriff nicht erlaubt, so kann das Betriebssystem den Speicherzugriff abfangen, bevor die Daten im Speicher verändert werden. Theoretisch könnte jedes Programm einen separaten, sogenannten Schutzraum bekommen. Aufgrund der meist knappen Ressourcen bei eingebetteten Systemen sollten aber nur so viele Schutzräume etabliert werden wie nötig, z. B. zwei, um die Ausführung von vertrauenswürdigen Programmen gegenüber der von nicht-vertrauenswürdigen zu trennen.

Bei hardwarebasiertem Speicherschutz werden die Speicherzugriffe durch die Hardware überwacht. Dieser Ansatz funktioniert auch, wenn die nicht vertrauenswürdige Softwarekomponente direkt in einer Maschinensprache programmiert wurde. Die überwachten Speicherzugriffe umfassen nicht nur die Lade- und Speicherbefehle sondern auch Maschinenbefehle, die vor ihrer Ausführung geladen werden. Schlägt die Überprüfung beim Speicherzugriff fehl, so unterbricht die Hardware den Ablauf des aktuellen Maschinenprogramms und wechselt zu einer Unterbrechungsbehandlung in die Systemsoftware. Welche Rechte für welchen Speicherbereich gelten, wird durch spezielle, zugriffsgeschützte Register beschrieben. Eine für hardwarebasierten Speicherschutz

geeignete CPU benötigt eine Hardware, die einen privilegierten und einen unprivilegierten Betriebsmodus unterstützt.

Beim softwarebasierten Speicherschutz werden die Speicherzugriffe nicht implizit durch die Hardware überprüft, sondern vorab explizit durch die Software. Die Überprüfung kann dabei zum Teil zum Übersetzungszeitpunkt stattfinden oder auch zur Laufzeit, zum Beispiel durch automatisch generierte Überprüfungen.

Prüffragen:

- Verfügt das eingebettete System über Vorkehrungen zum Speicherschutz?
- Sind die Art des Speicherschutzes und Anzahl und Größe der Schutzräume für das System und den Einsatzzweck angemessen und ausreichend?

M 5.78 Schutz vor Erstellen von Bewegungsprofilen bei der Mobiltelefon-Nutzung

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Benutzer

Bei der Mobil-Kommunikation müssen die mobilen Kommunikationspartner aus technischen Gründen geortet werden können, um erreichbar zu sein. Sofern sie selbst eine Verbindung aufbauen, geben sie ebenfalls im Zuge des Verbindungsaufbaus Informationen über ihren Standort ab. Diese Standortinformationen könnten durch den Netz- oder Dienstbetreiber, aber eventuell auch von Dritten, zur Bildung personen- oder gerätebezogener "Bewegungsprofile" verwendet werden.

Bei modernen Mobiltelefonen besitzen gegebenenfalls einige Applikationen Zugriff auf das Internet und den eingebauten GPS-Empfänger und geben Standortinformationen weiter, mit denen Dritte ebenfalls Bewegungsprofile erstellen können. Applikationen, die diese Rechte aus nicht funktionsbezogenen Gründen anfordern, sollten nicht installiert werden. Bei allen anderen Applikationen muss zwischen der Gefahr, Bewegungsprofile zu ermöglichen, und dem Nutzen der Applikation abgewogen werden.

Werden Bewegungsprofile als Gefährdung angesehen, dann sollten, falls umsetzbar, die Mobiltelefone und auch die SIM-Karten häufiger unter den Mitarbeitern getauscht werden. So wird eine Zuordnung der Geräte und Karten zu einem bestimmten Nutzer zumindest erschwert. Lokalisierungen über das Radio Resource Location Protocol (RRLP) können damit jedoch nicht abgewehrt werden, da hierbei sowohl die Telefonnummer als auch die International Mobile Equipment Identity (IMEI) ermittelt wird.

Soll der Aufenthaltsort zu bestimmten Zeiten unentdeckt bleiben, hilft nur ein Ausschalten des Mobiltelefons. Um ganz sicher zu sein, sollte der Akku entfernt werden.

Prüffragen:

- Ist die Frage geklärt, ob Bewegungsprofile sich negativ auswirken können?

M 5.79 Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Benutzer

Im Mobilfunknetz werden in der Regel den beteiligten Kommunikationspartnern die jeweiligen Rufnummern angezeigt. Ob dies tatsächlich geschieht, hängt von der technischen Ausstattung und der Konfiguration seitens der Mobiltelefone bzw. der Netzbetreiber bzw. Mobilfunkanbieter ab.

Am Mobiltelefon kann mit der Funktion Rufnummernunterdrückung (für den nächsten bzw. alle weiteren Anrufe) verhindert werden, dass die eigene Rufnummer im Display des Angerufenen angezeigt wird. Diese Option ist in den Menüs der Mobiltelefone oft unter Bezeichnungen wie Inkognito oder Anonym zu finden. Beim SMS-Versand mit einem Mobiltelefon ist eine Rufnummernunterdrückung in der Regel nicht möglich. Das Verhalten der Voice-Mailbox sollte im Einzelfall verifiziert werden, ebenso wie das Gesamtverhalten von Rufnummernunterdrückungs-Aktionen im Ausland.

Die Rufnummernunterdrückung kann bei Geräten, die den GSM-Standard unterstützen, mit folgenden GSM-Codes für den nächsten Anruf gesteuert werden:

- Eigene Rufnummer zeigen *31#Rufnummer
- Eigene Rufnummer nicht zeigen #31#Rufnummer

Über den Netzbetreiber kann auch kontinuierlich eine Rufnummernunterdrückung aktiviert werden.

Einen gewissen Schutz gegen die Zuordnung von Rufnummern zu bestimmten Personen gewährt der Austausch von Mobiltelefonen und SIM-Karten. Damit ist keine dauerhafte Zuordnung zwischen Benutzer und Rufnummer bzw. Gerät und Nutzer möglich. Die Zuordnung z. B. zu einer Behörde oder einem Unternehmen bleibt aber bestehen.

Außer über die Signalisierung der Rufnummer kann die Mobiltelefonnummer einer bestimmten Person auch über öffentliche Telefonbücher ermittelt werden, wenn sie dort eingetragen ist. Beim Abschluss eines Mobilfunkvertrages sollte daher genau überlegt werden, ob bzw. in welcher Form eine Eintragung in öffentliche Telefonbücher sinnvoll ist. Auch in internen Telefonbüchern und bei einzelnen Datenabfragen (Formulare, Gewinnspiele, etc.) sollten Mobiltelefonnummern nicht gedankenlos preisgegeben werden.

Prüffragen:

- Wird die Rufnummer in erforderlichen Fällen für ausgehende Anrufe unterdrückt?
- Sind in öffentlichen Telefonbüchern ausschließlich die dafür vorgesehenen Rufnummern veröffentlicht?

M 5.80 Schutz vor Abhören der Raumgespräche über Mobiltelefone

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: IT-Sicherheitsbeauftragter

Wer sicher ausschließen will, dass Raumgespräche über Mobiltelefone abgehört werden, muss dafür sorgen, dass kein Mobiltelefon in den zu schützenden Raum mitgenommen wird. Wenn die Sicherheitsleitlinie einer Institution es nicht zulässt, dass Mobiltelefone mitgebracht werden, muss an allen Eingängen deutlich darauf hingewiesen werden. Ohne entsprechende Kontrollen ist ein einfacher Hinweis aber meist wirkungslos.

Es reicht als Schutz nicht aus, Mobiltelefone einfach auszuschalten bzw. in den Standby oder Flugmodus zu bringen. Sofern sie entsprechend manipuliert sind, können sie über Funk unbemerkt eingeschaltet werden.

Mobiltelefon-Detektoren

Mobiltelefon-Detektoren sind Geräte, die erkennen, wenn in einem abgegrenzten Bereich ein oder mehrere Mobiltelefone in den Sendebetrieb (Gesprächsverbindungsaufbau) gehen.

Es gibt aktive und passive Detektoren. Passive Warngeräte melden Mobiltelefone, die sich im Sendebetrieb befinden. Der Wirkungsbereich der Geräte kann so eingestellt werden, dass er auf den zu überwachenden Bereich beschränkt ist. Es wird empfohlen, bei einem entsprechenden Schutzbedarf solche Warngeräte zu installieren und diese bei Gesprächen mit vertraulichem Inhalt zu aktivieren. Moderne Mobiltelefone benötigen allerdings zum Abhören keine stehende Funkverbindung, sondern können das Gespräch aufzeichnen und die Sounddatei mit Verzögerung über das Mobilfunknetz übertragen. Daher schützen passive Mobiltelefon-Detektoren nur bedingt davor, dass Raumgespräche abgehört werden.

Um auch Mobiltelefone zu erkennen, die im Ruhebetrieb (Standby) sind, wäre ein aktiver Sendeteil für den Detektor notwendig. Mithilfe dieses Sendeteils kann das Mobiltelefon dazu gebracht werden, in den Sendebetrieb zu gehen. Danach kann es dann mit einem Detektor erkannt werden. Mithilfe dieser aktiven Detektoren lassen sich so alle eingeschalteten Mobiltelefone detektieren. Später eingeschaltete Geräte müssen sich bei der Basisstation anmelden und können bei diesem Einbuchungsvorgang ebenfalls detektiert werden. Die Störsender können auch so eingesetzt werden, dass sie in einem räumlich abgegrenzten Bereich den Funkbetrieb derart stören, dass dort kein Mobilfunkempfang möglich ist.

Derzeit können aber nur passive Mobiltelefon-Detektoren empfohlen werden. Aktive Detektoren sind zwar ebenfalls sinnvoll, sie besitzen jedoch keine Betriebsgenehmigung für Deutschland. Auch Sender, die den Mobilfunkbetrieb stören, sind in Deutschland nicht zugelassen. Mobiltelefone können auch als Diktiergeräte genutzt werden. Lautlos und in den Flugmodus geschaltete Geräte können problemlos Besprechungen aufzeichnen, selbst aktive Mobiltelefon-Detektoren sind dann keine geeignete Gegenmaßnahme.

Prüffragen:

- Ist sichergestellt, dass Mobiltelefone nicht in abhörgeschützten Räumen verwendet werden?

M 5.81 Sichere Datenübertragung über Mobiltelefone

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Benutzer, IT-Sicherheitsbeauftragter

Mobiltelefone werden für die Sprachübertragung eingesetzt, es können aber auch Daten und Faxe damit übermittelt werden. Für einige dieser Dienste wird zusätzliches Zubehör benötigt. Moderne Mobiltelefone sind in der Regel dauerhaft mit dem Internet verbunden, um Chat-Nachrichten oder E-Mails zu empfangen. Benutzen Mobiltelefone den LTE-Standard, wird jegliche Kommunikation als Datenübertragung über das Internet-Protokoll (IP) realisiert.

Kurzmitteilungen

Mit dem Kurznachrichtendienst (Short Message Service, SMS) lassen sich Texte mit maximal 160 Zeichen von einem Mobiltelefon zum anderen oder auch an E-Mail-Adressen senden. Längere Nachrichten werden dabei in der Regel automatisch vom Mobiltelefon in mehrere Kurzmitteilungen aufgeteilt. Die Übertragung von Kurzmitteilungen erfolgt immer über eine Kurzmitteilungs-Zentrale, die die Nachrichten an den jeweiligen Empfänger weiterleitet.

Kurzmitteilungen werden im Mobiltelefon gespeichert, solange Speicherplatz verfügbar ist. Wenn kein ausreichender Speicherplatz (oft bei älteren oder extrem preisgünstigen Modellen) mehr frei ist, können keine weiteren Kurzmitteilungen empfangen werden. Der Netzbetreiber versucht nur über einen begrenzten Zeitraum, weitere Nachrichten abzusetzen. Wenn nicht rechtzeitig Speicherplatz freigemacht wird, werden die Kurzmitteilungen beim Netzbetreiber gelöscht.

Teilweise kann auch über das Mobiltelefon der Zeitraum, über den Kurzmitteilungen beim Netzbetreiber zwischengespeichert werden, verändert werden. Die Voreinstellung liegt im Allgemeinen zwischen 24 und 48 Stunden. Wenn der Vertrag mit dem Netzbetreiber es nicht vorsieht, kann hierüber allerdings der Speicherungszeitraum nicht erhöht werden. Er sollte auch nicht verringert werden.

Je nach Mobilfunkanbieter besteht die Möglichkeit, dass der Absender der Kurznachricht eine automatische Empfangsbestätigung erhält. Damit sichergestellt wird, ob die Nachrichten (siehe G 5.27 *Nichtanerkennung einer Nachricht*) empfangen wurden, sollten Empfangsbestätigungen aktiviert werden. Damit lässt sich zusätzlich auch nachvollziehen, ob die Nachricht wegen zu kurzer Speicherfristen bei der Kurzmitteilungs-Zentrale womöglich nicht zugestellt wurde (siehe G 4.32 *Nichtzustellung einer Nachricht*). Die Empfangsbestätigungen sollten so lange wie nötig auf dem Mobiltelefon gespeichert werden.

Um Kurzmitteilungen verschicken zu können, muss die Rufnummer der Kurzmitteilungs-Zentrale (SMS-Gateway) über das entsprechende Menü am Mobiltelefon voreingestellt werden. Meist ist dies schon auf der SIM-Karte vom Netzbetreiber vorkonfiguriert worden.

Im Internet gibt es diverse Angebote, Kurzmitteilungen mit minimalen Kosten zu versenden. Ein Angreifer kann also ohne großen Aufwand eine große Anzahl von SMS-Nachrichten an ein Mobiltelefon versenden. SMS-Spam wirkt sich ebenso aus wie E-Mail-Spam (siehe G 5.75 *Überlastung durch eingehende E-Mails*). Die Mailbox bzw. der Speicherplatz reicht nicht aus und ernsthaf-

te Nachrichten kommen nicht durch. Darüber hinaus entstehen dem Benutzer eventuell hohe Kosten. Hiergegen hilft neben der Sperrung von Drittanbieter-Diensten durch den Provider bzw. Mobilfunkanbieter, im Vorfeld die eigene Rufnummer nicht zu breit zu streuen, also z. B. auf den Eintrag in Telefonbücher zu verzichten, bzw. im Schadensfall eine Zeit lang ganz auf SMS-Empfang zu verzichten.

Eine Identifikation des Absenders ist bei SMS nicht zuverlässig möglich. Sie erfolgt maximal über die Rufnummer des Absenders und diese wird je nach Netzbetreiber bzw. Konfiguration des Mobiltelefons nicht immer mit übertragen. Beim Versand von Kurzmitteilungen über das Internet erfolgt im Allgemeinen überhaupt keine eindeutige Identifizierung. Dies sollte allen Benutzern klar sein, um die Echtheit einer Nachricht richtig einschätzen zu können. Je nach Inhalt einer empfangenen Kurzmitteilung ist es sinnvoll nachzufragen, ob diese wirklich vom angegebenen Absender stammt.

Faxe

Es können Faxe über ein mit dem Mobiltelefon gekoppeltes IT-System (z. B. Notebook) gesendet und empfangen werden.

Dabei ist ähnlich wie bei herkömmlichen Faxgeräten (siehe Baustein B 3.402 *Faxgerät*) zu beachten, dass

- der Speicherplatz des Mobiltelefons durch empfangene Faxe überlastet werden kann,
- es je nach Bedeutung von Faxen erforderlich sein kann, davon Kopien anzufertigen, was beim Mobiltelefon unter Umständen schwierig ist,
- es sinnvoll sein kann, die Rufnummern von bestimmten Faxempfängern bzw. Absendern zu sperren.

Außerdem empfiehlt sich,

- nach dem Versand nachzufragen, ob das Fax lesbar angekommen ist,
- nach dem Empfang nachzufragen, ob das Fax wirklich vom angegebenen Absender stammt,
- ab und zu die programmierten Zieladressen zu kontrollieren.

E-Mail

Über Mobiltelefone können neben Kurzmitteilungen auch E-Mails empfangen und verschickt werden. Bei älteren Endgeräten sind E-Mails wie Kurzmitteilungen auf 160 Zeichen begrenzt. Wenn dieser Service vom Netzbetreiber eingerichtet worden ist, erhält das Mobiltelefon eine eigene E-Mail-Adresse. In der Regel besitzen Mobiltelefone heute jedoch E-Mail-Clients, die E-Mails wie ein PC verarbeiten können. Besitzen Mobiltelefone keinen E-Mail-Client aber einen Browser, so können E-Mails in der Regel über eine Web-Oberfläche verarbeitet werden.

Bei einigen Netzbetreibern können E-Mail-Dienste mit anderen Diensten kombiniert werden. So können eingehende E-Mails von einem Sprachcomputer vorgelesen werden, an ein Faxgerät oder eine andere E-Mail-Adresse weitergeleitet werden. Ausgehende E-Mails können ins Mobiltelefon gesprochen und als Audiodatei versandt werden.

Wie Kurzmitteilungen und Faxe können auch E-Mails schnell den vorhandenen Speicherplatz (bei älteren oder extrem preisgünstigen Geräten) ausschöpfen. Der E-Mail-Client sollte daher so eingestellt werden, dass Dateianhänge nur bei Bedarf, also wenn der Benutzer sie explizit anfragt, nachgeladen werden.

Potenzielle Sicherheitsprobleme und Maßnahmen für E-Mail sind in Baustein B 5.3 *Groupware* beschrieben. Dabei ist zu beachten, dass die E-Mail-Funktionalität bei Mobiltelefonen stark eingeschränkt ist gegenüber anderen E-Mail-Anwendungen. Ebenso wie SMS ist E-Mail hier eher für die Übermittlung kurzer und kurzlebiger Nachrichten gedacht. Sicherheitsmaßnahmen wie Verschlüsselung oder Signatur sind in der Regel nur mit Smartphones möglich. Alternativ gibt es noch spezielle Geräte oder zusätzliche Module, mit denen verschlüsselte oder signierte Nachrichten mit einem Mobiltelefon übermittelt werden können.

Instant Messenger

Auf einigen Mobiltelefonen und den meisten Smartphones sind Instant Messenger vorhanden oder lassen sich nachträglich installieren. Mit Instant Messengern können Nachrichten, aber auch Dateien wie z. B. Bilder, Filme, und Office-Dokumente übertragen werden. Auch Instant Messenger, die über das Internet-Relay-Chat-(IRC)-System funktionieren, sind vielfach im Einsatz. Die Kommunikation über Instant Messenger sollte, wenn möglich, Ende-zu-Ende-verschlüsselt erfolgen. Es dürfen nur vertrauenswürdige IRC-Server bzw. Instant-Message-Provider verwendet werden. In diesem Fall ist die Vertraulichkeit der Kommunikation gegenüber Kurznachrichten deutlich erhöht. Dubiose Dateiübertragungen sollten abgelehnt werden. Instant Messenger haben zudem gegenüber den Kurznachrichten den Vorteil, dass Kosten nach Datenmenge und nicht nach Anzahl der Nachrichten entstehen. Zusätzlich besitzen viele Instant Messenger die Funktion der Empfangsbestätigung, die auch genutzt werden sollte, um der Gefahr der Nichtanerkennung von Nachrichten (siehe G 5.27 *Nichtanerkennung einer Nachricht*) zu begegnen.

Datenübertragung

Ein Mobiltelefon kann je nach Modell mit einem weiteren IT-System (z. B. einem Notebook oder einem Organizer) gekoppelt werden und dann leichter auch größere Datenmengen übertragen. Dabei kann die Kopplung auf verschiedene Arten erfolgen, je nachdem, welche Techniken die beiden Geräte unterstützen.

Einsteckkarte: Eine Einsteckkarte (PC-Card, PCMCIA) ist die ursprünglich konventionelle, aber mittlerweile kaum noch eingesetzte Lösung zur Verbindung von Mobiltelefon und Notebook. Die meisten Einsteckkarten können allerdings nur an Mobiltelefone eines bestimmten Herstellers angeschlossen werden.

Softmodem: Bei dieser Lösung wird statt einer Einsteckkarte eine spezielle Software auf dem Notebook installiert. Das Mobiltelefon wird dann einfach über die serielle (oder USB) Schnittstelle mit dem Notebook verbunden. Diese Lösung ist meist preiswerter als eine Einsteckkarte.

Infrarot: Über eine Infrarot-Schnittstelle können Daten auch ohne Kabel vom Mobiltelefon zu einem anderen Gerät (z. B. Laptop oder Organizer) übertragen werden. Dazu muss sowohl das Mobiltelefon als auch das Partnergerät den Infrarot Übertragungsstandard IrDA unterstützen. IrDA ist ein weltweiter Standard für die Datenübertragung über Infrarot, wird aber für Datenübertragungen heute kaum noch eingesetzt (siehe M 4.255 *Nutzung von IrDA-Schnittstellen*).

Bluetooth: Bluetooth ist ein etablierter Standard, nach dem Geräte per Funk über Entfernungen von 1 bis 100m (je nach Bluetooth-Klasse) miteinander Daten austauschen können. (siehe B 4.8 *Bluetooth*).

WLAN: Über Wireless-LAN kann ein Mobiltelefon mit einem Rechnernetz verbunden werden oder es kann selbst als sogenannter WLAN-Hotspot fungieren ("Tethering") und eine Internetverbindung für andere IT-Systeme bereitstellen. Die WLAN-Verbindung sollte dabei über WPA kryptografisch abgesichert werden. Weitere Details zum Einsatz von WLAN sind im Baustein B 4.6 *WLAN* zu finden.

Bei der Datenübertragung z. B. von einem Laptop über das Mobilfunknetz sollten die übertragenen Daten vorher auf dem Endgerät verschlüsselt werden. Hierzu gibt es eine Vielzahl von Applikationen, die dies einfach ermöglichen. Die Verschlüsselung vor der Übertragung sichert die Informationen auf der gesamten Strecke zwischen Absender und Empfänger. Dies geht über die bei GSM standardmäßige Absicherung der Luftschnittstelle zwischen Mobiltelefon und Basisstation hinaus. Das ist notwendig, weil die Verschlüsselung über das GSM-Netz auf der Luftschnittstelle als gebrochen gilt. Bei schlechter Umsetzung bietet die Verschlüsselung bei der Übertragung mit UMTS auch keinen besseren Schutz als bei der Übertragung mit GSM. Werden die Daten hingegen mithilfe von Programmen auf dem Endgerät verschlüsselt, können die Nachrichten zudem noch digital signiert werden. Wie adäquate kryptografische Verfahren und Systeme ausgewählt und eingesetzt werden können, ist im B 1.7 *Kryptokonzept* beschrieben. Alternativ zur Verschlüsselung der Daten bieten moderne Mobiltelefone vielfach die Möglichkeit, verschlüsselte VPN-Tunnel zu etablieren, womit die Datenübertragung zwischen Mobiltelefon und anderen Netzteilnehmern ebenfalls hinreichend abgesichert werden kann. Alternativ könnte ein vorhandener Laptop auch als VPN-Endpunkt verwendet werden, über diesen das Mobiltelefon eine geschützte Datenverbindung aufbauen kann. Wird VPN verwendet, besteht überdies der Vorteil, dass die Verschlüsselung transparent ist und keine weitere Benutzerinteraktion benötigt.

Besitzt das Mobiltelefon einen Browser und E-Mail-Client, so ist es über diese Kanäle so verwundbar wie ein PC. Unbedacht heruntergeladene Dateien, Klingeltöne, aber auch Drive-by-Infektionen können die Geräte ebenso funktionsuntüchtig machen wie stationäre Computer.

Die Datenübertragung sollte in allen Organisationen klar geregelt sein. Alle Datenübertragungseinrichtungen sollten genehmigt sein und deren Nutzung klaren Regelungen unterliegen (siehe M 2.204 *Verhinderung ungesicherter Netzzugänge*).

Damit durch die Datenübertragung über GSM-Schnittstellen keine Sicherheitslücken entstehen, sollte diese restriktiv gehandhabt werden. So sollten bei IT-Systemen, auf denen sensitive Daten verarbeitet werden, keine Mobilfunkkarten zugelassen werden bzw. Verbindungen über das Mobilfunknetz immer mit verschlüsselten VPN-Tunneln abgesichert sein. Dies gilt ebenso bei allen IT-Systemen, die an einem Rechner-Netz angebunden sind, damit hier nicht der durch eine Firewall eigentlich vorhandene Schutz unterhöhlt werden kann.

Prüffragen:

- Gibt es Regelungen, welche Daten über Mobiltelefone übertragen werden dürfen?
- Gibt es Regelungen, welche Schnittstellen zu benutzen sind und wie verschlüsselt werden soll?

M 5.121 Sichere Kommunikation von unterwegs

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator, Benutzer

Über mobile Endgeräte wie Laptops, Smartphones, Tablets oder PDAs soll auch häufig unterwegs auf Daten aus dem Internet oder dem internen Netz einer Institution zugegriffen werden. Dabei werden üblicherweise öffentliche Kommunikationsnetze benutzt. Da weder die Institution noch die mobilen Mitarbeiter großen Einfluss darauf nehmen können, ob die Vertraulichkeit, Integrität und Verfügbarkeit im öffentlichen Kommunikationsnetz gewahrt werden, sind zusätzliche Maßnahmen zum Schutz der Informationen erforderlich.

Generell muss die Datenübertragung zwischen einem mobilen Endgerät und dem LAN einer Institution folgende Sicherheitsanforderungen erfüllen:

- *Sicherstellung der Vertraulichkeit der übertragenen Daten*: Die Datenübertragung muss ausreichend sicher verschlüsselt werden. Auch wer die Kommunikation abhört, soll nicht auf den Inhalt der Daten rückschließen können. Dazu gehört neben einem geeigneten Verschlüsselungsverfahren auch ein angepasstes Schlüsselmanagement mit periodischem Schlüsselwechsel.
- *Sicherstellung der Integrität der übertragenen Daten*: Die eingesetzten Übertragungsprotokolle müssen die Möglichkeit bieten, Veränderungen an den übertragenen Daten zu erkennen und eventuell sogar zu beheben. Solche Veränderungen können beispielsweise durch Übertragungsfehler (technische Probleme) oder durch absichtliche Manipulationen durch einen Angreifer entstehen. Zusätzlich kann der Einsatz digitaler Signaturen sinnvoll sein, um die Datenintegrität sicherzustellen.
- *Sicherstellung der Authentizität der Daten*: Bei der Übertragung der Daten muss vertrauenswürdig feststellbar sein, ob die Kommunikation zwischen den richtigen Teilnehmern stattfindet, sodass eine Maskerade oder ein Man-in-the-Middle-Angriff ausgeschlossen werden kann. Zu diesem Zweck muss eine gegenseitige Authentisierung der Kommunikationspartner (beispielsweise über digitale Zertifikate) erfolgen.
- *Sicherstellung der Nachvollziehbarkeit der Datenübertragung*: Um eine Kommunikation nachvollziehbar zu machen, können Protokollierungsfunktionen eingesetzt werden, durch die sich nachträglich feststellen lässt, welche Daten wann und an wen übertragen wurden.

Die Stärke der dazu erforderlichen Mechanismen richtet sich dabei nach dem Schutzbedarf der übertragenen Daten. Wie adäquate kryptografische Verfahren und Systeme ausgewählt und eingesetzt werden können, ist in Baustein B 1.7 *Kryptokonzept* beschrieben.

Wenn mit mobilen Endgeräten über öffentliche Netze auf interne Ressourcen zugegriffen werden soll, so wird der Einsatz eines Virtual Private Network (VPN) dringend empfohlen. Entsprechende Produkte sind von diversen Herstellern und für praktisch alle gebräuchlichen Plattformen verfügbar. Auf Daten oder Systeme mit hohem Schutzbedarf darf nicht ohne entsprechende Sicherungsmaßnahmen zugegriffen werden. Betreibt die Institution in ihrem Netz einen Filter für Schadsoftware, so sollte die Netzverbindung des mobilen Endgerätes durch diesen Filter geleitet werden, um so das Endgerät besser vor Schadsoftware zu schützen.

Für den Zugriff auf Internet-Anwendungen, bei denen schützenswerte Daten wie personenbezogene Daten, interne Informationen oder Kontendaten ausgetauscht werden, muss zumindest SSL zur Verschlüsselung genutzt werden (siehe auch M 5.66 *Clientseitige Verwendung von SSL/TLS*).

Kopplung mit anderen IT-Systemen

Beim Einsatz mobiler Endgeräte wie Laptops, Smartphones, Tablets oder PDAs sollen häufig auch Daten mit anderen IT-Systemen ausgetauscht werden, etwa mit Geschäftspartnern. Auch für den Zugriff auf das Internet ist häufig die Kopplung mit anderen IT-Systemen erforderlich. Dies kann auf verschiedene Arten erfolgen, je nachdem, welche Techniken die beteiligten Geräte unterstützen, beispielsweise über Infrarot-, Bluetooth-, WLAN- oder GSM-Schnittstellen. Hier müssen zum einen die Übertragungstechniken sicher eingesetzt werden, zum anderen müssen die eigenen IT-Systeme sicher konfiguriert sein. Dazu gehören bei mobilen Clients Sicherheitsmaßnahmen wie z. B. Zugriffsschutz, Benutzerauthentisierung, Virenschutz, Personal Firewall, restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene, lokale Verschlüsselung, etc.

Soll ein mobiles Endgerät an fremde Netze oder an das Internet angeschlossen werden, so sollte das System grundsätzlich über eine Personal Firewall abgesichert werden (siehe M 5.91 *Einsatz von Personal Firewalls für Clients*).

Nutzung fremder IT-Systeme

Beim Einsatz mobiler Endgeräte wie Laptops, Smartphones, Tablets oder PDAs sollen häufig auch Daten mit anderen IT-Systemen ausgetauscht werden, etwa mit Geschäftspartnern. Auch für den Zugriff auf das Internet ist häufig die Kopplung mit anderen IT-Systemen erforderlich. Dies kann auf verschiedene Arten erfolgen, je nachdem, welche Techniken die beteiligten Geräte unterstützen, beispielsweise über Infrarot-, Bluetooth-, WLAN- oder GSM-Schnittstellen. Hier müssen zum einen die Übertragungstechniken sicher eingesetzt werden, zum anderen müssen die eigenen IT-Systeme sicher konfiguriert sein. Dazu gehören bei mobilen Clients Sicherheitsmaßnahmen wie z. B. Zugriffsschutz, Benutzerauthentisierung, Virenschutz, Personal Firewall, restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene, lokale Verschlüsselung, etc.

In allen Organisationen sollte klar geregelt sein, auf welche Daten von unterwegs zugegriffen werden darf und auf welche nicht. Vor allem muss allen IT-Benutzern bekannt sein, unter welchen Randbedingungen sie Daten über externe Netze oder direkt mit fremden IT-Systemen austauschen dürfen (siehe M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen* und M 2.218 *Regelung der Mitnahme von Datenträgern und IT-Komponenten*).

Prüffragen:

- Werden bei der Datenübertragung die Daten ausreichend geschützt?
- Wird beim Datenaustausch das eigene IT-System ausreichend geschützt?

M 5.173 Nutzung von Kurz-URLs und QR-Codes

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
Verantwortlich für Umsetzung: Fachverantwortliche, Leiter IT

Webseiten werden üblicherweise über eine URL (Uniform Resource Locator) angesteuert, die daher auch Web-Adresse genannt wird. Die Komplexität vieler Webseiten führt häufig zu relativ langen Web-Adressen, die schwer zu merken sind und vor allem bei mobilen Endgeräten wie Smartphones nicht in einer Zeile dargestellt werden können. Daher haben sich verschiedene Methoden entwickelt, um den Benutzern die Nutzung von Webadressen zu erleichtern. Prominente Vertreter sind Kurz-URLs und QR-Codes.

Kurz-URLs

Kurz-URLs bezeichnen einen weitverbreiteten Dienst im Internet, bei dem lange URLs durch kürzere URLs ersetzt werden. Kurz-URLs sind vergleichbar mit einem Link-Text in HTML, der auch beliebig kurz gewählt werden kann. Anders als bei solchen Links auf Internetseiten ist die Zuordnung zwischen kurzer und langer URL dabei in einer Datenbank hinterlegt und daher nicht so leicht erkennbar. Gründe für die weite Verbreitung von Kurz-URLs sind unter anderen:

- Durch Kurz-URLs können Zeilenumbrüche von URLs in E-Mails vermieden werden. Durch einen Zeilenumbruch in einer URL bedeutet es meist mehr Aufwand, den zugeschickten Link zu öffnen. Kurz-URLs sind für gewöhnlich so kurz, dass sie nicht umgebrochen werden müssen.
- Um Links in Mikro-Blog-Einträgen wie etwa Tweets von Twitter einzubetten, können keine langen URLs benutzt werden. Mikro-Blogs besitzen eine starke Zeichenbeschränkung von in der Regel 140 Zeichen pro Eintrag, da Mikro-Blogs von den Nutzern für gewöhnlich am Handy und nicht am PC verfasst werden. Daher haben sich Kurz-URLs als die gängige Form von Links in Mikro-Blog-Einträgen durchgesetzt.
- Kurz-URLs erleichtern es, Referenzen und Verweisen in Zeitschriftenartikeln zu folgen. Viele Artikel in papiergebundenen Zeitschriften verweisen auf Quellen aus dem Internet bzw. enthalten Hinweise zu Internetseiten. Anders als bei Online-Artikeln müssen diese per Hand abgetippt werden. Kurz-URLs verringern den Aufwand dafür erheblich.

Neben all diesen Vorteilen können Kurz-URLs aber auch Gefährdungen mit sich bringen (siehe G 5.177 *Missbrauch von Kurz-URLs oder QR-Codes*). Die Mitarbeiter der Institution sollten für diese Probleme sensibilisiert werden. Alle Mitarbeiter sollten wissen, dass Kurz-URLs mit Vorsicht zu genießen sind.

Um nicht auf andere als die gewünschten Webseiten weitergeleitet zu werden, können die Vorschaudienste von Kurz-URL-Anbietern genutzt werden. Dort wird einerseits die dahinter verborgene Adresse angezeigt und andererseits ein Bild der Seite gezeigt. Diese Funktion gibt es auch direkt als Erweiterung für gängige Internetbrowser. Die Vorschaufunktion von Kurz-URLs sollte möglichst immer genutzt werden. Anbieter von Kurz-URLs ohne eine Vorschaufunktion sollten nicht verwendet werden. Allerdings kann die Vorschaufunktion durch iterative Kurz-URLs ausgehebelt werden. Iterativ heißt eine Kurz-URL, wenn sie selbst auf eine andere Kurz-URL (statt auf eine echte Seite) verweist. Es sollten daher möglichst nur Anbieter von Kurz-URLs benutzt werden, welche iterative Kurz-URLs verbieten. Schwerer zu unterbinden sind ite-

rative Kurz-URLs über mehrere Anbieter hinweg. Da iterative Kurz-URLs keinen praktischen Nutzen außer für Angreifer haben, sollten Benutzer iterative Kurz-URLs generell nicht anklicken.

Das Risiko, durch Kurz-URLs auf ungewünschte oder gefährliche Seiten im Internet geleitet zu werden, kann nur verringert, aber nicht ausgeschlossen werden. Damit schädliche Auswirkungen vermieden werden, müssen unbedingt die aktuellen Sicherheitsupdates für Browser und Betriebssystem eingespielt sein sowie ein Virenscanner aktiv sein.

Zusätzlich zu diesen Maßnahmen kann eine Institution entscheiden, dass Kurz-URLs ein zu großes Risiko darstellen und daher nicht verwendet werden dürfen. In diesem Fall kann der Zugang zu Kurz-URL-Dienstanbieter gesperrt werden, z. B. über entsprechende Filterregeln.

Nutzung von QR-Code

Um Anwendern das Abtippen von Kurz-URLs, WLAN-Zugangsdaten, Telefonnummern und anderen Informationen abzunehmen, werden vermehrt QR-Codes (Quick Response Codes) verwendet. Hierbei werden Daten in einer Abbildung, einem meist quadratischen Pixelmuster, so kodiert, dass sie zuverlässig von IT-Systeme ausgelesen werden können. Hierfür ist es erforderlich, über Endgeräte wie Smartphones mit entsprechender Ausstattung den QR-Code abzufotografieren oder einzuscannen, um die hierin kodierten Informationen auslesen zu können.

Die Spezifikation von QR-Code ist offen gelegt und QR-Codes können lizenz- und kostenfrei verwendet werden, so dass sie mittlerweile stark verbreitet sind. Klassische QR-Codes können Informationen bis zu 2.953 Byte beinhalten. QR-Codes verfügen über eine hohe Fehlertoleranz, je nach Fehlerkorrektur-Level können zwischen 7% und 30% beschädigter Informationen eines QR-Codes rekonstruiert werden. Neben den verbreiteten QR-Codes gibt es Weiterentwicklungen, in denen Informationen (teilweise) verschlüsselt abgelegt werden, die besonders kleine Abmessungen haben oder in denen Bilder, Texte oder Logos erkennbar sind.

Die in QR-Codes abgelegten Informationen können nicht ohne Weiteres von den Benutzern gelesen werden. Dadurch ergeben sich, ähnlich wie bei Kurz-URLs, einige Gefährdungen (siehe G 5.177 *Missbrauch von Kurz-URLs oder QR-Codes*). Ein Benutzer könnte beispielsweise auf seinem Endgerät einen QR-Code einlesen, der auf über die darin kodierte URL auf eine mit Schadsoftware infizierte Webseite verweist. Daher muss darauf geachtet werden, dass auf dem Endgerät nach dem Einlesen eines QR-Codes keine weiteren Aktionen automatisch ausgeführt werden. Bei einer URL sollte also zuerst die dahinter verborgene Adresse angezeigt werden, bevor die entsprechende Web-Seite geöffnet wird. Generell sollte nach dem Einlesen auch keine Telefonnummer automatisch angerufen oder eine SMS versendet werden, Benutzer sollten ausgehende Anrufe erst bestätigen, bevor gewählt wird.

Das Sicherheitsmanagement sollte deswegen die Mitarbeiter über den Umgang mit QR-Codes aufklären. Außerdem sollten auf den Endgeräten nur QR-Applikationen eingesetzt werden, bei denen nach dem Einlesen von QR-Codes keine Aktionen automatisch ausgeführt werden, sondern diese vorher vom Benutzer bestätigt werden müssen.

Sollen Informationen für einen kleinen Benutzerkreis veröffentlicht werden, kann überlegt werden, die hierin abgelegten Informationen zu verschlüsseln. Beispielsweise können hierfür Secure-QR-Codes (SQRC) verwendet werden.

Dafür müssen die eingesetzten Lesegeräte beziehungsweise IT-Systeme diese natürlich auch dekodieren können.

Prüffragen:

- Sind die Mitarbeiter für die Kurz-URL-Problematik sensibilisiert?
- Werden die Inhalte von Kurz-URLs und QR-Codes vor der Ausführung angezeigt?

M 5.176 Sichere Anbindung von Smartphones, Tablets und PDAs an das Netz der Institution

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter
Verantwortlich für Umsetzung: Leiter IT

Smartphones, Tablets und PDAs werden in der Regel kabellos mit dem Netz der Institution verbunden, z. B. über WLAN oder das mobile Telekommunikationsnetz. Grundsätzlich sollte die Verbindung zwischen Endgerät und dem Netz der Institution durchgehend verschlüsselt sein. Das lässt sich mit einem verschlüsselten VPN-Tunnel realisieren (siehe Baustein B 4.4 *VPN*), der zwischen dem Endgerät und einem VPN-Server der Institution aufgebaut wird. So wird vermieden, dass Schwächen der mobilen Telekommunikationsnetze oder einer unverschlüsselten WLAN-Verbindung die Vertraulichkeit gefährden. Greift das Endgerät über das verschlüsselte WLAN der Institution auf das Netz der Institution zu, so kann überlegt werden, ob der VPN-Tunnel entbehrlich ist.

Smartphones, Tablets und PDAs sollten innerhalb der Institution in einem eigenen Netzsegment untergebracht sein (siehe Maßnahme M 5.7 *Netzverwaltung*). Werden diese oder vergleichbare Endgeräte in einem Informationsverbund eingesetzt, sollte die Segmentierung durch eine Netzzugangskontrolle ergänzt werden. Sie sollte zusätzlich überprüfen, ob:

- auf den mobilen Endgeräten alle aktuellen Systempatches vorhanden sind,
- alle Anwendungen die neuesten Updates besitzen,
- die Virensignatur-Datenbank aktuell ist und
- alle weiteren Einstellungen am Endgerät, z. B. Passwortgestaltung und Zeitdauer bis zum automatischen Sperren, den Vorgaben entsprechen.

Sollte die Netzzugangskontrolle feststellen, dass ein Smartphone, Tablet oder PDA in einem dieser Punkte abweicht, so ist es in ein Quarantäne-Netzsegment zu verschieben. Dort kann der Agent der Netzzugangskontrolle das Gerät entsprechend den Sicherheitsvorgaben aktualisieren beziehungsweise den Benutzer anleiten, geänderte Einstellungen am Endgerät wieder rückgängig zu machen. Im Anschluss kann das Endgerät wieder aus dem Quarantäne-Bereich entfernt werden.

Sollte ein Smartphone, Tablet oder PDA gestohlen oder verloren gegangen sein und eine Meldung hierüber vorliegen, so ist der Zugang dieses Endgerätes zum Netz der Institution zu sperren (siehe Maßnahme M 6.159 *Vorsorge vor Verlust und Diebstahl von Smartphones, Tablets und PDAs*). Bei höherem Schutzbedarf muss zudem geprüft werden, ob mit dem Endgerät in der Zwischenzeit bereits unbefugt auf Informationen der Institution zugegriffen wurde und ob entsprechend den Richtlinien zur Behandlung von Sicherheitsvorfällen weitere Maßnahmen zu ergreifen sind (siehe Baustein B 1.8 *Behandlung von Sicherheitsvorfällen*). Dafür sind im Vorfeld entsprechende Protokollfunktionen der Netzzugangskontrolle zu nutzen.

Prüffragen:

- Werden Smartphones, Tablets und PDAs innerhalb der Institution in einem eigenen Netzsegment untergebracht?
- Werden auffällige Smartphones, Tablets oder PDAs in ein Quarantäne-Netzsegment verschoben?

M 6.72 Ausfallvorsorge bei Mobiltelefonen

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Benutzer, Leiter IT

Ein Mobiltelefon kann aus verschiedenen Gründen ausfallen oder in seiner Funktionsfähigkeit gestört sein. Dies ist natürlich besonders ärgerlich, wenn es dringend benötigt wird oder dadurch wichtige Daten verloren gehen. Daher sollten von vorne herein entsprechende Vorkehrungen getroffen werden, um einem Ausfall vorzubeugen bzw. die Probleme zu minimieren.

Der Ladezustand und die Funktionsfähigkeit des Mobiltelefon-Akkus sollten regelmäßig überprüft werden (siehe auch M 4.115 *Sicherstellung der Energieversorgung von Mobiltelefonen*).

Alle auf dem Mobiltelefon gespeicherten Daten wie Telefonbucheintragungen, Nachrichten, etc. sollten in regelmäßigen Abständen auf einem anderen Medium gespeichert werden, damit sie im Zweifelsfall rekonstruiert werden können. Hierzu gibt es mehrere Möglichkeiten:

- Die wichtigsten Einstellungen wie PINs und die Konfiguration von Sicherheitsmechanismen sollten schriftlich dokumentiert und entsprechend ihrem Schutzbedarf sicher aufbewahrt werden
- Alle Daten, die auf der SIM-Karte gespeichert sind, also z. B. Telefonbücher, können über SIM-Kartenleser und entsprechende Software in einen PC eingelesen und dort verwaltet werden. Dies hat außerdem den Vorteil, dass Adressdaten auf dem PC leichter gepflegt und mit anderen Adressdatenbanken synchronisiert werden können. Insbesondere wenn mehrere Mobiltelefone benutzt werden (siehe auch M 2.190 *Einrichtung eines Mobiltelefon-Pools*) ist ein Abgleich der Telefonbücher auf diesem Weg sinnvoll. Wenn nur die Daten auf der SIM-Karte gesichert werden, sind alle Benutzer darauf hinzuweisen, dass sie auch nur dort Rufnummern und Ähnliches speichern sollten. Da diese Methode in der Regel weitere Hardware (den SIM-Kartenleser) benötigt und die Speicherkapazität der SIM-Karte gegenüber dem Telefonspeicher deutlich geringer ist, sollte aber besser der Telefonspeicher für Adressbücher verwendet werden. Diese Variante hat überdies den Vorteil, dass die Kontakt-Daten dabei je nach Modell im vCard-Format vorliegen können, das von vielen verschiedenen IT-Systemen (Mobiltelefonen, Smartphones und PCs) verarbeitet werden kann.
- Das Mobiltelefon kann auch mit einem weiteren IT System, z. B. einem Notebook oder einem Organizer, gekoppelt werden, sodass die zu sichernden Daten auf diesem Weg ausgetauscht werden falls eine geeignete Synchronisations-Software für das gewählte Mobiltelefon existiert (siehe auch M 5.81 *Sichere Datenübertragung über Mobiltelefone*). Dabei können sowohl die auf der SIM-Karte als auch die im Gerät gespeicherten Daten gesichert werden.

Wenn ein Mobiltelefon kontinuierlich verfügbar sein soll, sollte ein Ersatz-Mobiltelefon oder aber ein Ersatz-Akku (wenn möglich), mitgeführt werden.

Wenn Mobiltelefone im Rahmen von Alarmierungen eingesetzt werden, also wenn z. B. die Einbruchmeldeanlage Alarmmeldungen über GSM absetzt oder Notfallpersonal über Mobiltelefone benachrichtigt werden soll, muss immer eine Ausweichmöglichkeit vorgesehen sein.

Reparatur

Bei Defekten des Mobiltelefons oder einzelner Komponenten sollten Reparaturen nur von vertrauenswürdigen Fachbetrieben durchgeführt werden. Daher sollte eine Übersicht über entsprechende Fachbetriebe vorhanden sein.

Viele Händler bieten auch für die Dauer der Reparatur Ersatzgeräte an. Bei schnelllebigen Geräten wie Mobiltelefonen lohnt sich eine Reparatur häufig nicht, sodass auch manchmal ein Tauschgerät angeboten wird. Da gerade ein Mobiltelefon kontinuierlich zur Verfügung stehen sollte, ist bei der Auswahl des Mobiltelefons bzw. des Händlers darauf zu achten, dass solche Dienstleistungen angeboten werden.

Bevor das Mobiltelefon zur Reparatur gegeben wird, sollten alle personenbezogenen Daten, also z. B. der Anrufspeicher, gespeicherte E Mails und das Telefonbuch im Gerät gelöscht werden (siehe auch M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten*), soweit das noch möglich ist. Vorher sollten sie selbstverständlich gesichert werden. Außerdem sollten die SIM-Karte und ggf. entnehmbare Speicherkarten entfernt werden. Bei vielen Mobiltelefon-Modellen empfiehlt es sich, einen dort möglichen Firmware-Reset durchzuführen.

Prüffragen:

- Werden die auf Mobiltelefonen gespeicherten Daten in regelmäßigen Abständen auf einem anderen Medium gesichert?
- Werden vor Reparaturen alle vertraulichen Daten vom Mobiltelefon gelöscht (und vorher gesichert)?

M 6.95 Ausfallvorsorge und Datensicherung bei Smartphones, Tablets und PDAs

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator, Benutzer

Ein Smartphone, Tablet oder PDA kann aus verschiedenen Gründen ausfallen oder in seiner Funktionsfähigkeit gestört sein. Dies ist natürlich besonders ärgerlich, wenn er dringend benötigt wird oder dadurch wichtige Daten verloren gehen. Daher sollten von vornherein entsprechende Vorkehrungen getroffen werden, um einem Ausfall vorzubeugen bzw. die Probleme zu minimieren.

Der Ladezustand und die Funktionsfähigkeit des Akkus sollten regelmäßig überprüft werden (siehe M 4.31 *Sicherstellung der Energieversorgung im mobilen Einsatz*).

Alle auf dem mobilen Endgerät gespeicherten Daten wie Telefonbucheintragungen, Notizen, etc. sollten in regelmäßigen Abständen auf einem anderen Medium gespeichert werden, damit sie im Zweifelsfall rekonstruiert werden können. Hierzu gibt es mehrere Möglichkeiten:

- Die wichtigsten Einstellungen wie Passwörter und die Konfiguration von Sicherheitsmechanismen sollten schriftlich dokumentiert und entsprechend ihres Schutzbedarfs sicher aufbewahrt werden. Werden die Endgeräte durch eine Mobile-Device-Management-Software zentral gesteuert und konfiguriert, so sind die entsprechenden Profile der Endgeräte zu sichern, sodass sie zügig wieder eingespielt werden können.
- Die Daten auf dem Smartphone, Tablet oder PDA sollten regelmäßig mit einer anderen Stelle, wie z. B. mit einem PC, einem Serverdienst der Institution oder gegebenenfalls mit einem externen Dienstleister synchronisiert werden. Das ersetzt allerdings keine vollständige Datensicherung.
- Es sollte daher regelmäßig auch eine komplette Datensicherung des Smartphones, Tablets oder PDAs auf einem weiteren IT-System, z. B. einem Notebook oder einem Desktop-PC, durchgeführt werden. Besonders empfehlenswert ist die komplette Datensicherung durch ein vollständiges Systemabbild (Snapshot). Die Lösung ist komfortabel und verringert die Zeit für die Installation und Konfiguration eines neuen Gerätes erheblich. Wenn für diese Lösung das IT-System tiefer gehend manipuliert werden muss, wie beispielsweise durch Rooten oder die Installation eines alternativen Recovery bei Android-basierten Geräten, so sollte das Risiko der Manipulation gegen den Vorteil der schnelleren Wiederverfügbarkeit sorgsam abgewogen werden. Gegebenenfalls sind die zusätzlichen Maßnahmen für die Informationssicherheit, die durch das Rooten oder sonstige Maßnahmen nötig werden, so hoch, dass kein Vorteil gegenüber der weniger komfortablen Sicherungsmethode ohne Systemabbild besteht.
- Da bei Smartphones, Tablets und PDAs der vorhandene Speicherplatz beschränkt ist, können die meisten Modelle mit externen Speichermedien erweitert werden (siehe auch M 4.232 *Sichere Nutzung von Zusatzspeicherkarten*). Verbreitet sind hierfür Speicherkarten, z. B. Memory-Cards, die schnell austauschbar sind, sodass sie sich gut eignen, um auch unterwegs Backups durchzuführen. Das ist vor allem dann sinnvoll, wenn ein Benutzer häufig lange abwesend ist und dadurch für längere Zeit keine Synchronisation zwischen IT-System und Smartphone, Tablet oder PDA stattfindet. Wie generell für Datensicherungen gilt auch hier, dass diese sicher verwahrt werden müssen. Wenn die Memory-Cards im Endgerät oder

anderswo unbeaufsichtigt liegen bleiben, können Unbefugte die darauf gespeicherten Daten kopieren. Legen sie anschließend die Memory-Card wieder zurück, werden dabei nicht einmal Spuren hinterlassen.
- Alle Daten, die auf austauschbaren Speicherkarten gespeichert sind, müssen ebenfalls gesichert werden, spätestens bei der nächsten Synchronisation.

Bei den meisten Smartphones, Tablets oder PDAs liegt das Betriebssystem in einem Flash-Speicher, der häufig auch genügend Platz für eine Datensicherung wenigstens der wichtigsten Daten wie der Inhalte des Personal Information Manager (PIM) bietet. Um das komfortabel durchzuführen, gibt es je nach Hersteller mitgelieferte oder zusätzliche Tools. Hierbei sollte beachtet werden, dass nach einem kompletten Reset alle Daten außerhalb des Flash-Speichers gelöscht werden, also auch alle Passwörter zum Zugriffsschutz. Ein Angreifer kann dadurch leicht Zugriff auf den Flash-Speicher und die dort gespeicherten Daten erhalten. Bevor ein Smartphone, Tablet oder PDA weitergegeben wird, z. B. zur Reparatur oder an andere Benutzer, sollten daher alle Daten, auch aus dem Flash-Speicher, gelöscht werden.

Wenn ein Smartphone, Tablet oder PDA kontinuierlich verfügbar sein soll, sollte immer ein Ersatz-Akku mitgeführt werden.

Reparatur

Bei Defekten des Smartphones, Tablets, PDAs oder einzelner Komponenten sollten Reparaturen nur von vertrauenswürdigen Fachbetrieben durchgeführt werden. Daher sollte eine Übersicht über entsprechende Fachbetriebe vorhanden sein.

Viele Händler bieten auch für die Dauer der Reparatur Ersatzgeräte an. Bei schnelllebigen Geräten wie Smartphones, Tablets oder PDAs lohnt sich eine Reparatur häufig nicht, sodass auch manchmal ein Tauschgerät angeboten wird. Da gerade ein Smartphone, Tablet oder PDA kontinuierlich zur Verfügung stehen sollte, ist bei der Auswahl des jeweiligen Endgerätes bzw. des Händlers darauf zu achten, dass solche Dienstleistungen angeboten werden.

Bevor ein Smartphone, Tablet oder PDA zur Reparatur gegeben wird, sollten alle personenbezogenen Daten, also z. B. gespeicherte E Mails und das Telefonbuch im Gerät gelöscht werden (siehe auch M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten*), soweit das noch möglich ist. Vorher sollten sie selbstverständlich gesichert werden. Außerdem sollten Zusatzkarten entfernt werden.

Prüffragen:

- Werden der Ladezustand und die Funktionsfähigkeit der PDA-Akkus regelmäßig überprüft?
- Werden die auf PDAs gespeicherten Daten regelmäßig gesichert?
- Werden vor der Weitergabe von PDAs alle Daten gelöscht?

M 6.159 Vorsorge vor Verlust und Diebstahl von Smartphones, Tablets und PDAs

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter
Verantwortlich für Umsetzung: Leiter IT

Damit beim Diebstahl oder Verlust eines Smartphones, Tablets oder PDAs nicht gleichzeitig alle Kontaktdaten, Zugangsdaten zum Netz der Institution und sonstige schützenswerte Informationen auf dem Endgerät verloren gehen oder missbraucht werden, müssen entsprechende Empfehlungen umgesetzt werden.

Es sollten nur Endgeräte eingesetzt werden, die eine vollständige Verschlüsselung der Daten unterstützen. Sofern das Endgerät eine externe Speicherkarte besitzt, sollte auch sie möglichst vollständig verschlüsselt werden. Dafür ist ein sicheres Passwort auszuwählen (siehe M 2.11 *Regelung des Passwortgebrauchs*). Für die Datensicherung sollte dann zusätzlich M 6.56 *Datensicherung bei Einsatz kryptographischer Verfahren* herangezogen werden.

Bei Verlust oder Diebstahl von Smartphones, Tablets und PDAs sollte es möglich sein, aus der Ferne Maßnahmen zum Sperren, Löschen und Lokalisieren der mobilen Endgeräte einzuleiten. Dafür gibt es Anwendungen, die ausgesucht und auf den Geräten installiert werden müssen. Da die meisten Mobile Device Management (MDM) Lösungen oder Virenschutzprogramme (siehe M 4.230 *Zentrale Administration von Smartphones, Tablets und PDAs* oder M 4.466 *Einsatz von Viren-Schutzprogrammen bei Smartphones, Tablets und PDAs*) diese Funktionen mit anbieten, sollte überprüft werden, ob die bereits verwendeten Lösungen alle benötigten Funktionen enthalten. Werden neue MDM-Lösungen oder Antivirenschutzprogramme eingekauft, ist sicherzustellen, dass sie alle Funktionen enthalten, die nötig sind, um auf Diebstahl oder Verlust zu reagieren.

Es sollte ein klarer Verfahrensablauf bei Diebstahl oder Verlust von dienstlich genutzten Smartphones, Tablets oder PDAs definiert werden. Alle betroffenen Mitarbeiter müssen die entsprechenden Abläufe, Kontaktdaten und sonstigen Informationen kennen.

Bei einem Verlust oder Diebstahl von Smartphones, Tablets oder PDAs ist umgehend eine Stelle in der Institution zu informieren, die alle weitere Schritte veranlassen kann. Zuerst sollte jeglicher Zugang dieses Endgerätes zum Informationsverbund, beispielsweise durch E-Mail oder VPN, abgeschaltet werden. Dann sollten aus der Ferne alle schützenswerten Informationen vom Endgerät gelöscht und das Gerät gesperrt werden. Vielfach kann der Sperrbildschirm mit einer frei wählbaren Nachricht versehen werden. Hier sollten für den ehrlichen Finder alle nötigen Kontaktdaten hinterlegt werden, damit er das Endgerät der Institution zurückgeben kann.

Ein Dieb wird in der Regel versuchen zu verhindern, dass das Endgerät geortet wird, indem er die SIM-Karte entfernt. Es ist daher zu empfehlen, solche Anwendungen zum Orten, Löschen und Sperren des Endgerätes zu verwenden, die diese Aktionen auch ereignisbasiert ausführen können. So sollten automatisch alle schützenswerten Informationen vom Endgerät gelöscht werden, wenn eine andere SIM-Karte eingesetzt oder die SIM-Karte entfernt wird. Um den Dieb besser identifizieren zu können, ist es sinnvoll, wenn die Anwendung automatisch die Telefonnummer der neuen SIM-Karte und die GPS-Koordi-

naten an die Institution übermittelt. Wenn solche automatisierten Nachrichten eintreffen, sollte zusätzlich der Zugang zu Informationen der Institution für dieses Endgerät gesperrt werden. Eine solche Meldung ersetzt jedoch nicht die persönliche Verlustmeldung des Benutzers.

Wenn verlorene Geräte wieder auftauchen, sollten sie auf eventuelle Manipulationen an Hard- und Software untersucht werden, z. B. ob Schrauben geöffnet, Siegel entfernt wurden oder sich das Gewicht gegenüber dem Auslieferungszustand geändert hat. Besteht ein Verdacht, sollte das Gerät entweder gleich entsorgt oder von einem Spezialisten weiter untersucht werden. Um sicherzustellen, dass sich keine manipulierten Programme auf den wiedererlangten Smartphones, Tablets oder PDAs befinden, müssen alle Daten vom Endgerät gelöscht und das Endgerät danach komplett neu installiert werden.

Prüffragen:

- Existiert ein Ablaufplan für Verlust oder Diebstahl eines Smartphones, Tablets oder PDAs?
- Ist auf dem Endgerät ein Programm installiert und konfiguriert, das es erlaubt, das Endgerät aus der Ferne zu sperren, zu löschen und zu orten?
- Ist dieses Programm so konfiguriert, dass es bei Austausch der SIM-Karte das Endgerät sperrt, löscht, ortet und die neue Telefonnummer an die Institution schickt?
- Wurde definiert, in welcher Weise wiedererlangte Endgeräte auf Manipulationen an Hard- und Software zu untersuchen sind, bevor sie wieder eingesetzt werden?