DSGVo: Themen bezüglich Mitarbeiter und Personal anhand der IT-Grundschutzkataloge des BSI und des österreichischen Informationssicherheitshandbuchs

Dieses Paper ist eine Zusammenfassung von möglichen Gefahren und Maßnahmen bezüglich Mitarbeiter und Personal.

Es basiert auf den zutreffenden Bausteinkatalogen, den Gefährungskatalogen und den Maßnahmenkatalogen aus dem Dokument „IT-Grundschutz-Kataloge“ in der Version 15. Ergänzungslieferung – 2016 („BSI“ - 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) sowie auf dem Österreichischen Informationssicherheitshandbuch in der Version 4.0.1 vom 19.01.2016 („ISHB“ - https://www.sicherheitshandbuch.gv.at/).

Inhalt

Informationssicherheitshandbuch

Regelungen für MitarbeiterInnen

7.1.1 Verpflichtung der MitarbeiterInnen zur Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen (siehe auch BSI M 3.2)
7.1.2 Aufnahme der sicherheitsrelevanten Aufgaben und Verantwortlichkeiten in die Stellenbeschreibung
7.1.3 Vertretungsregelungen (siehe auch BSI M 3.3)
7.1.4 Geregelte Verfahrensweise beim Ausscheiden von MitarbeiterInnen (siehe auch BSI M 3.6)
7.1.5 Geregelte Verfahrensweise bei Versetzung von MitarbeiterInnen
7.1.6 Gewährleistung eines positiven Betriebsklimas (siehe auch BSI M 3.8 und BSI M 3.9)
7.1.7 Clear-Desk-Policy
7.1.8 Benennung vertrauenswürdiger AdministratorInnen und VertreterInnen (siehe auch BSI M 3.10)
7.1.9 Verpflichtung der PC-BenutzerInnen zum Abmelden (siehe auch BSI M 3.18)
7.1.10 Kontrolle der Einhaltung der organisatorischen Vorgaben
7.1.11 Geregelte Verfahrensweise bei vermuteten Sicherheitsverletzungen

Regelungen für den Einsatz von Fremdpersonal

7.2.1 Regelungen für den kurzfristigen Einsatz von Fremdpersonal (siehe auch BSI M 2.226)
7.2.2 Verpflichtung externer MitarbeiterInnen zur Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
7.2.3 Beaufsichtigung oder Begleitung von Fremdpersonen
7.2.4 Information externer MitarbeiterInnen über die IT-Sicherheitspolitik

Sicherheitssensibilisierung und –schulung

7.3.1 Geregelte Einarbeitung/Einweisung neuer MitarbeiterInnen (siehe auch BSI M 3.1)
7.3.2 Schulung vor Programmnutzung (siehe auch BSI M 3.4)
7.3.3 Schulung und Sensibilisierung zu IT-Sicherheitsmaßnahmen
7.3.4 Betreuung und Beratung von IT-BenutzerInnen
7.3.5 Aktionen bei Auftreten von Sicherheitsproblemen
7.3.6 Schulung des Wartungs- und Administrationspersonals (siehe auch BSI M 3.11)
7.3.7 Einweisung in die Regelungen der Handhabung von Kommunikationsmedien
7.3.8 Einweisung in die Bedienung von Schutzschränken

Anhang B.4 Muster: Verpflichtungserklärung betreffend die Benutzung von IT-Systemen
Anhang B.7 Muster: Verpflichtungserklärung zur Einhaltung des DSG
Anhang B.8 Muster: Verpflichtungserklärung zur Nutzung von dienstlich beigestellten mobilen Arbeitsplatzrechnern
8.1.3.1 Herausgabe einer PC-Richtlinie

BSI-Bausteinkataloge

B 1.2 Personal

BSI-Gefährdungskataloge

G 1.1 Personalausfall
G 1.2 Ausfall von IT-Systemen
G 2.2 Unzureichende Kenntnis über Regelungen
G 2.7 Unerlaubte Ausübung von Rechten
G 2.16 Ungeordneter Benutzerwechsel bei tragbaren PCs
G 2.21 Mangelhafte Organisation des Wechsels zwischen den Benutzern
G 2.36 Ungeeignete Einschränkung der Benutzerumgebung
G 2.41 Mangelhafte Organisation des Wechsels von Datenbank-Benutzern
G 2.103 Unzureichende Schulung der Mitarbeiter
G 2.201 Unzureichende Berücksichtigung von Veränderungen im Arbeitsumfeld von Mitarbeitern
G 3.1 Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten
G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
G 3.3 Nichtbeachtung von Sicherheitsmaßnahmen
G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
G 3.8 Fehlerhafte Nutzung von IT-Systemen
G 3.9 Fehlerhafte Administration von IT-Systemen
G 3.17 Kein ordnungsgemäßer PC-Benutzerwechsel
G 3.36 Fehlinterpretation von Ereignissen
G 3.37 Unproduktive Suchzeiten
G 3.38 Konfigurations- und Bedienungsfehler
G 3.43 Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen
G 3.44 Sorglosigkeit im Umgang mit Informationen
G 3.77 Mangelhafte Akzeptanz von Informationssicherheit
G 5.1 Manipulation oder Zerstörung von Geräten oder Zubehör
G 5.2 Manipulation an Informationen oder Software
G 5.16 Gefährdung bei Wartungs-/Administrierungsarbeiten
G 5.19 Missbrauch von Benutzerrechten
G 5.20 Missbrauch von Administratorrechten
G 5.23 Schadprogramme
G 5.42 Social Engineering
G 5.80 Hoax
G 5.104 Ausspähen von Informationen

BSI-Maßnahmenkataloge

Mitarbeiter

M 2.12 Betreuung und Beratung von IT-Benutzern
M 2.29 Bedienungsanleitung der TK-Anlage für die Benutzer
M 2.41 Verpflichtung der Mitarbeiter zur Datensicherung
M 2.197 Integration der Mitarbeiter in den Sicherheitsprozess
M 2.198 Sensibilisierung der Mitarbeiter für Informationssicherheit
M 2.558 Sensibilisierung der Mitarbeiter zur Informationssicherheit bei Mobiltelefonen, Smartphones, Tablets und PDAs
M 3.2 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen (siehe auch ISHB 7.1.1)
M 3.18 Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung (siehe auch ISHB 7.1.9)
M 3.55 Vertraulichkeitsvereinbarungen
M 3.78 Korrektes Auftreten im Internet
M 6.115 Integration der Mitarbeiter in den Notfallmanagement-Prozess

Organisation

M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen
M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile
M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung
M 2.40 Rechtzeitige Beteiligung des Personal-/Betriebsrates
M 2.65 Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
M 2.113 Regelungen für Telearbeit
M 2.132 Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen
M 2.226 Regelungen für den Einsatz von Fremdpersonal (siehe auch ISHB 7.2.1)
M 2.398 Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten
M 2.519 Geregelte Benutzer- und Berechtigungsverwaltung im Cloud Computing
M 3.3 Vertretungsregelungen (siehe auch ISHB 7.1.3)
M 3.6 Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern (siehe auch ISHB 7.1.4)
M 3.7 Anlaufstelle bei persönlichen Problemen
M 3.8 Vermeidung von Störungen des Betriebsklimas (siehe auch ISHB 7.1.6)
M 3.9 Ergonomischer Arbeitsplatz
M 3.10 Auswahl eines vertrauenswürdigen Administrators und Vertreters (siehe auch ISHB 7.1.8)
M 3.33 Sicherheitsüberprüfung von Mitarbeitern
M 3.44 Sensibilisierung des Managements für Informationssicherheit
M 3.46 Ansprechpartner zu Sicherheitsfragen
M 3.50 Auswahl von Personal
M 3.51 Geeignetes Konzept für Personaleinsatz und –qualifizierung
M 3.79 Einführung in Grundbegriffe und Funktionsweisen von Bluetooth
M 3.83 Analyse sicherheitsrelevanter personeller Faktoren
M 3.90 Allgemeine Grundlagen für die zentrale Protokollierung
M 3.92 Grundlegende Begriffe beim Einsatz von Speicherlösungen
M 3.93 Analyse der Zielgruppen für Sensibilisierungs und Schulungsprogramme
M 3.96 Unterstützung des Managements für Sensibilisierung und Schulung
M 4.16 Zugangsbeschränkungen für Benutzer-Kennungen und / oder Terminals

Schulungsmaßnahmen

M 2.506 Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten
M 3.1 Geregelte Einarbeitung/Einweisung neuer Mitarbeiter (siehe auch ISHB 7.3.1)
M 3.4 Schulung vor Programmnutzung (siehe auch ISHB 7.3.2)
M 3.5 Schulung zu Sicherheitsmaßnahmen
M 3.11 Schulung des Wartungs- und Administrationspersonals (siehe auch ISHB 7.3.6)
M 3.12 Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und –töne
M 3.13 Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen
M 3.14 Einweisung des Personals in den geregelten Ablauf der Informationsweitergabe und des Datenträgeraustausches
M 3.15 Informationen für alle Mitarbeiter über die Faxnutzung
M 3.17 Einweisung des Personals in die Modem-Benutzung
M 3.20 Einweisung in die Bedienung von Schutzschränken
M 3.21 Sicherheitstechnische Einweisung der Telearbeiter
M 3.23 Einführung in kryptographische Grundbegriffe
M 3.26 Einweisung des Personals in den sicheren Umgang mit IT
M 3.28 Schulung zu Sicherheitsmechanismen für Benutzer bei Windows Client-Betriebssystemen
M 3.32 Schulung zu Sicherheitsmechanismen von Outlook für Benutzer
M 3.35 Einweisung der Benutzer in die Bedienung des Archivsystems
M 3.43 Schulung der Administratoren des Sicherheitsgateways
M 3.45 Planung von Schulungsinhalten zur Informationssicherheit
M 3.47 Durchführung von Planspielen zur Informationssicherheit
M 3.54 Schulung der Administratoren des Speichersystems
M 3.56 Schulung der Administratoren für die Nutzung von VoIP
M 3.59 Schulung zum sicheren WLAN-Einsatz
M 3.60 Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern und Geräten
M 3.67 Einweisung aller Mitarbeiter über Methoden zur Löschung oder Vernichtung von Daten

M 3.69 Einführung in die Bedrohung durch Schadprogramme
M 3.76 Einweisung der Benutzer in den Einsatz von Groupware und E-Mail
M 3.77 Sensibilisierung zur sicheren Internet-Nutzung
M 3.80 Sensibilisierung für die Nutzung von Bluetooth
M 3.81 Schulung zum sicheren Terminalserver-Einsatz
M 3.82 Schulung zur sicheren Nutzung von TK-Anlagen
M 3.97 Schulung des Projektteams für die Software-Entwicklung
M 3.98 Einweisung aller Mitarbeiter in den Umgang mit Authentisierungsverfahren und –mechanismen
M 6.129 Schulung der Mitarbeiter des Service Desk zur Behandlung von Sicherheitsvorfällen

Informationssicherheitshandbuch

7.1.1 Verpflichtung der MitarbeiterInnen zur Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen

Bei der Einstellung von MitarbeiterInnen sind diese zur Einhaltung einschlägiger Gesetze (z. B. Bundesgesetz über den Schutz personenbezogener Daten - Datenschutzgesetz i.d.F. vom 25.05.2018, insbesondere § 6 „Datengeheimnis“), Vorschriften und interner Regelungen zu verpflichten.

Damit sollen neue MitarbeiterInnen mit den bestehenden Vorschriften und Regelungen zur IT-Sicherheit bekannt gemacht und gleichzeitig zu deren Einhaltung motiviert werden. Dabei ist es sinnvoll, nicht nur die Verpflichtung durchzuführen, sondern auch die erforderlichen Exemplare der Vorschriften und Regelungen auszuhändigen und gegenzeichnen zu lassen bzw. für die MitarbeiterInnen an zentraler Stelle zur Einsichtnahme vorzuhalten.

Neben der Verpflichtung zur Einhaltung von Gesetzen und Vorschriften empfiehlt es sich insbesondere, Regelungen zu folgenden Bereichen zu treffen, die dann auch in eine entsprechende Verpflichtungserklärung aufzunehmen sind:

- Clear-Desk-Policy, falls vorgesehen (vgl. 7.1.7 Clear-Desk-Policy)
- Einhaltung von PC-Benutzungsregeln (vgl. 8.1.3.1 Herausgabe einer PC-Richtlinie)
- Einhaltung der Regeln für die Benutzung des Internet

7.1.2 Aufnahme der sicherheitsrelevanten Aufgaben und Verantwortlichkeiten in die Stellenbeschreibung

Bei der Erstellung von Stellenbeschreibungen ist dafür Sorge zu tragen, dass alle sicherheitsrelevanten Aufgaben und Verantwortlichkeiten explizit in diese Beschreibungen aufgenommen werden. Anzuführen sind dabei sowohl die allgemein aus der organisationsweiten IT-Sicherheitspolitik abzuleitenden Verpflichtungen als auch spezielle Verantwortlichkeiten auf Grund der Tätigkeit.

Dies gilt in besonderem Maße für MitarbeiterInnen mit speziellen Sicherheitsaufgaben (Mitglieder des IT-Sicherheitsmanagement-Teams, Datenschutzbeauftragte, IT-Sicherheitsbeauftragte, Bereichs-IT-Sicherheitsbeauftragte, Applikations-/Projektverantwortliche).

7.1.3 Vertretungsregelungen

Vertretungsregelungen haben den Sinn, für vorhersehbare (Urlaub, Dienstreise) und auch unvorhersehbare Fälle (Krankheit, Unfall, Kündigung) des Personenausfalls die Fortführung der Aufgabenwahrnehmung zu ermöglichen. Daher muss vor Eintritt eines solchen Falles geregelt sein, wer wen in welchen Angelegenheiten mit welchen Kompetenzen vertritt. Dies ist besonders im Bereich der Informationsverarbeitung von Bedeutung, da dafür meist Spezialwissen sowie eine zeitgerechte Einarbeitung unkundiger MitarbeiterInnen unbedingt erforderlich sind.

Für die Vertretungsregelungen sind folgende Randbedingungen einzuhalten:

- Die Übernahme von Aufgaben im Vertretungsfall setzt voraus, dass der Verfahrens- oder Projektstand hinreichend dokumentiert ist.
- Die VertreterInnen müssen so geschult werden, dass sie die Aufgaben jederzeit übernehmen können. Stellt sich heraus, dass es Personen gibt, die aufgrund ihres Spezialwissens nicht kurzfristig ersetzbar sind, so bedeutet deren Ausfall eine gravierende Gefährdung des Normalbetriebes. Hier ist es von besonders großer Bedeutung, VertreterInnen zu schulen.
- Es muss festgelegt sein, welcher Aufgabenumfang im Vertretungsfall von wem wahrgenommen werden soll.
- Die VertreterInnen dürfen die erforderlichen Zugangs- und Zutrittsberechtigungen nur im Vertretungsfall erhalten.
- Ist es in Ausnahmefällen nicht möglich, für Personen kompetente VertreterInnen zu benennen oder zu schulen, sollte frühzeitig überlegt werden, welche externen Kräfte für den Vertretungsfall eingesetzt werden können.
- Es sollte vermieden werden, dass Vertretungsregeln u.U. vorgesehene Mehraugenprinzipien unterlaufen, z. B. wenn sich zwei kollektiv Berechtigte wechselseitig vertreten.
- Im Zusammenhang mit der Verwendung von kryptographischen Systemen ist auch über ein Verfahren zur Offenlegung von kryptographischen Schlüsseln im Rahmen des Kryptokonzeptes zu achten.

7.1.4 Geregelte Verfahrensweise beim Ausscheiden von MitarbeiterInnen

Scheiden MitarbeiterInnen aus, so sollten einige Punkte beachtet werden. Dies wären:

- Vor dem Ausscheiden ist eine Einweisung der NachfolgerInnen durchzuführen.
- Von den Ausscheidenden sind sämtliche Unterlagen, ausgehändigte Schlüssel, ausgeliehene IT-Geräte (z. B. tragbare Rechner, Speichermedien, Dokumentationen) zurückzufordern. Insbesondere sind die Behörden- bzw. Firmenausweise einzuziehen.
- Es sind sämtliche für die Ausscheidenden eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Dies betrifft auch die externen Zugangsberechtigungen via Datenübertragungseinrichtungen. Wurde in Ausnahmefällen eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt (z. B. mittels eines gemeinsamen Passwortes), so ist nach Ausscheiden einer der Personen die Zugangsberechtigung zu ändern.
- Es ist sicherzustellen, dass bei Ausscheidenden keine Unterlagen, Betriebsmittel oder Zugangsmöglichkeiten verbleiden, und diese Nachfolgenden für ihre Tätigkeiten zur Verfügung stehen.
- Vor der Verabschiedung sollte noch einmal explizit darauf hingewiesen werden, dass alle Verschwiegenheitserklärungen weiterhin in Kraft bleiben und keine im Rahmen der Tätigkeit erhaltenen Informationen weitergegeben werden dürfen.
- Nach Möglichkeit sollte eine Neuvergabe der User-IDs an andere MitarbeiterInnen vermieden/ausgeschlossen werden.
- Sind die ausscheidenden Personen FunktionsträgerInnen in einem Notlaufplan, so ist der Notlaufplan zu aktualisieren.
- Sämtliche mit Sicherheitsaufgaben betrauten Personen, insbesondere der Portierdienst, sind über das Ausscheiden der MitarbeiterInnen zu unterrichten.
- Ausgeschiedenen MitarbeiterInnen ist der unkontrollierte Zutritt zum Behördenoder Firmengelände, insbesondere zu Räumen mit IT-Systemen zu verwehren.
- Optional kann sogar für den Zeitraum zwischen Aussprechen der Kündigung und dem Ausscheiden der Entzug sämtlicher Zugangs- und Zugriffsrechte auf IT-Systeme sowie darüber hinaus auch das Verbot, schützenswerte Räume zu betreten, ausgesprochen werden.
- Als ein praktikables Hilfsmittel haben sich Laufzettel erwiesen, auf denen die einzelnen Aktivitäten der Ausscheidenden vorgezeichnet sind, die sie vor Verlassen der Behörde bzw. des Unternehmens zu erledigen haben

7.1.5 Geregelte Verfahrensweise bei Versetzung von MitarbeiterInnen

Bei Versetzung von MitarbeiterInnen oder einer wesentlichen Änderung ihrer Tätigkeit sind ihre Zugangsberechtigungen sowie Zugriffsrechte auf Übereinstimmung mit den neuen Anforderungen zu überprüfen und gegebenenfalls anzupassen.

7.1.6 Gewährleistung eines positiven Betriebsklimas

Ein positives Betriebsklima motiviert die MitarbeiterInnen einerseits zur Einhaltung von IT-Sicherheitsmaßnahmen und bewirkt andererseits die Reduzierung von fahrlässigen oder vorsätzlichen Handlungen (vgl. § 126a Datenbeschädigung (StGB)), die eine Störung des IT-Betriebs herbeiführen können. Daher sollte auch unter IT-Sicherheitsaspekten versucht werden, ein positives Betriebsklima zu erreichen.

Dazu gehört auch die ergonomische Gestaltung des Arbeitsplatzes. Hierzu besteht eine Reihe von Regelungen und Normen, deren Nichtbeachtung u. a. eventuell zu Sicherheitsproblemen führen kann. Ergonomie ist nicht Gegenstand dieses Handbuches, die Wichtigkeit einer ergonomischen Gestaltung des Arbeitsplatzes sei aber hier nochmals betont.

Weiters ist bei der Ausstattung von Arbeitsplätzen darauf zu achten, dass die Einhaltung von IT-Sicherheitsmaßnahmen unterstützt wird. Dazu gehören etwa verschließbare Schreibtische oder Schränke, in denen Datenträger, Dokumentationen, Unterlagen und Zubehör verschlossen werden können. Ursache für eine unzureichende Aufgabenerfüllung können oftmals persönliche Probleme von ArbeitnehmerInnen sein. Daher ist es für jede Organisation wichtig, ihre MitarbeiterInnen und eventuelle potenzielle Probleme zu kennen („Know your Employee“). In vielen Fällen kann es hilfreich sein, wenn eine Anlaufstelle zur Verfügung steht, die bei solchen Problemen konkrete Hilfe und Lösungsmöglichkeiten anbieten kann.

7.1.7 Clear-Desk-Policy

Alle MitarbeiterInnen sollten vor ihrer Abwesenheit ihre Unterlagen und den persönlichen Arbeitsbereich verschließen: Schreibtisch, Schrank, PC und Telefon. Dies gilt insbesondere für Großraumbüros, aber auch in den anderen Fällen ist dafür Sorge zu tragen, dass keine unberechtigten Personen (BesucherInnen, Reinigungspersonal, unbefugte MitarbeiterInnen, ...) Zugriff zu Schriftstücken, Datenträgern und IT-Komponenten haben.

Ist eine „Clear-Desk-Policy"-Regelung in einer Organisation vorgesehen, so sollte die Einhaltung dieser Regelung in die Verpflichtungserklärung aller MitarbeiterInnen (vgl. 7.1.1 Verpflichtung der MitarbeiterInnen zur Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen) aufgenommen werden.

7.1.8 Benennung vertrauenswürdiger AdministratorInnen und VertreterInnen

AdministratorInnen von IT-Systemen und ihren VertreterInnen müssen vom Betreiber großes Vertrauen entgegengebracht werden können. Sie haben – in Abhängigkeit vom eingesetzten System - weitgehende und oftmals allumfassende Befugnisse. AdministratorInnen und ihre VertreterInnen sind in der Lage, auf alle gespeicherten Daten zuzugreifen, sie ggf. zu verändern und Berechtigungen so zu vergeben, dass erheblicher Missbrauch möglich wäre.

Das hierfür eingesetzte Personal muss sorgfältig ausgewählt werden. Es soll regelmäßig darüber belehrt werden, dass die Befugnisse nur für die erforderlichen Administrationsaufgaben verwendet werden dürfen. Eine regelmäßige Kontrolle von AdministratorInnen - etwa durch Auswertung von Protokollen durch Revisoren – ist vorzusehen.

Darüber hinaus sollte geprüft werden, inwieweit durch technische Maßnahmen - etwa die Verschlüsselung von ausgewählten Daten oder Zugriffsbeschränkungen zu Protokollfiles - die Befugnisse von AdministratorInnen eingeschränkt werden können, ohne deren Aufgabenerfüllung zu beeinträchtigen.

7.1.9 Verpflichtung der PC-BenutzerInnen zum Abmelden

Wird ein PC von mehreren BenutzerInnen genutzt und besitzen die einzelnen BenutzerInnen unterschiedliche Zugriffsrechte auf im PC gespeicherte Daten oder Programme, so kann der erforderliche Schutz mittels einer Zugriffskontrolle nur dann erreicht werden, wenn alle BenutzerInnen sich nach Aufgabenerfüllung bzw. bei Verlassen des Arbeitsplatzes am PC abmelden. Ist es Dritten möglich, an einem PC unter der Identität von Anderen weiterzuarbeiten, so ist jegliche sinnvolle Zugriffskontrolle unmöglich. Daher sind alle PC-BenutzerInnen zu verpflichten, sich bei Verlassen des Arbeitsplatzes abzumelden.

Ist keine Zugriffskontrolle realisiert, so ist die Abmeldung der BenutzerInnen aus Gesichtspunkten der Ordnungsmäßigkeit dennoch vorzuschreiben. Ist absehbar, dass nur eine kurze Unterbrechung der Arbeit erforderlich ist, kann an Stelle des Abmeldens auch eine manuelle oder nach einer gewissen Zeit automatische Aktivierung der Bildschirmsperre erfolgen.

7.1.10 Kontrolle der Einhaltung der organisatorischen Vorgaben

Mittels Protokollauswertung oder durch Stichproben ist in angemessenen Zeitabständen zu überprüfen, ob die BenutzerInnen eines IT-Systems die organisatorischen Vorgaben (etwa Verpflichtung zur Abmeldung nach Aufgabenerfüllung oder Verbot der Weitergabe von Passwörtern) auch tatsächlich einhalten.

Kontrollen sollten vor allen Dingen darauf ausgerichtet sein, Mängel abzustellen. Für die Akzeptanz von Kontrollen ist es wichtig, dass dies allen Beteiligten als Ziel der Kontrollen erkennbar ist und dass dabei keine Personen bloßgestellt werden oder als „Schuldige" identifiziert werden. Wenn die MitarbeiterInnen dies befürchten müssen, besteht die Gefahr, dass sie nicht offen über ihnen bekannte Schwachstellen und Sicherheitslücken berichten, sondern versuchen, bestehende Probleme zu vertuschen. Es ist daher sinnvoll, während einer Kontrolle mit den Beteiligten über mögliche Problemlösungen zu sprechen und entsprechende Abhilfen vorzubereiten

Wenn MitarbeiterInnen eine Regelung ignorieren oder umgehen, ist das meist ein Zeichen dafür, dass diese nicht mit den Arbeitsabläufen vereinbar ist oder durch die MitarbeiterInnen nicht umgesetzt werden kann. Beispielsweise ist eine Anweisung, vertrauliche Schreiben nicht unbeaufsichtigt am Drucker liegen zu lassen, unsinnig, wenn zum Drucken nur ein weit entfernter Netzdrucker zur Verfügung steht.

Wenn bei Kontrollen Mängel festgestellt werden, kommt es nicht darauf an, nur die Symptome zu beseitigen. Vielmehr ist es wichtig, die Ursachen für diese Probleme festzustellen und Lösungen aufzuzeigen. Diese können beispielsweise in der Änderung bestehender Regelungen oder in der Hinzunahme technischer Maßnahmen bestehen.

7.1.11 Geregelte Verfahrensweise bei vermuteten Sicherheitsverletzungen

Die Vorgehensweise zur Untersuchung angeblicher (bewusster oder versehentlicher) Verletzungen von Sicherheitsvorgaben sowie potenzielle Konsequenzen - im Falle interner MitarbeiterInnen können dies beispielsweise disziplinäre Maßnahmen sein, im Falle externer MitarbeiterInnen etwa vertraglich abgeleitete Konsequenzen - sollen festgelegt, vom Management verabschiedet und allen MitarbeiterInnen bekannt sein.

Eine derartig geregelte Verfahrensweise kann einerseits infolge der abschreckenden Wirkung zur Prävention von Sicherheitsverletzungen dienen und gewährleistet andererseits eine korrekte und faire Behandlung von Personen, denen Sicherheitsverletzungen angelastet werden.

7.2.1 Regelungen für den kurzfristigen Einsatz von Fremdpersonal

Kurzfristig oder einmalig zum Einsatz kommendes Fremdpersonal ist wie BesucherInnen zu behandeln, d. h. dass also etwa der Aufenthalt in sicherheitsrelevanten Bereichen nur in Begleitung von MitarbeiterInnen der Behörde bzw. des Unternehmens erlaubt ist etc.

7.2.2 Verpflichtung externer MitarbeiterInnen zur Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen

Externe MitarbeiterInnen, die über einen längeren Zeitraum in einer oder für eine Organisation tätig sind und evtl. Zugang zu vertraulichen Unterlagen und Daten bekommen könnten, sind ebenfalls schriftlich zur Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen zu verpflichten.

7.2.3 Beaufsichtigung oder Begleitung von Fremdpersonen

Fremde (BesucherInnen, HandwerkerInnen, Wartungs- und Reinigungspersonal) sollten, außer in Räumen, die ausdrücklich dafür vorgesehen sind, nicht unbeaufsichtigt sein.

Wird es erforderlich, Fremde allein im Büro zurückzulassen, sollte man KollegInnen ins Zimmer oder die BesucherInnen zu KollegInnen bitten. Ist es nicht möglich, Fremdpersonen (z. B. Reinigungspersonal) ständig zu begleiten oder zu beaufsichtigen, sollte zumindest der persönliche Arbeitsbereich abgeschlossen werden: Schreibtisch, Schrank und PC (Schloss für Diskettenlaufwerk, Tastaturschloss). Siehe auch 7.1.7 Clear-Desk-Policy.

Für den häuslichen Arbeitsplatz gilt, dass Familienmitglieder und BesucherInnen sich nur dann alleine im Arbeitsbereich aufhalten dürfen, wenn alle Arbeitsunterlagen verschlossen aufbewahrt sind und die IT über einen aktivierten Zugangsschutz gesichert ist.

Die Notwendigkeit dieser Maßnahmen ist den MitarbeiterInnen zu erläutern und ggf. in einer Dienstanweisung festzuhalten. Eine Dokumentation über den Aufenthalt von Fremdpersonen kann in einem Besucherbuch geführt werden.

7.2.4 Information externer MitarbeiterInnen über die IT-Sicherheitspolitik

Externe MitarbeiterInnen sind - so weit es zur Erfüllung ihrer Aufgaben und Verpflichtungen erforderlich ist - über hausinterne Regelungen und Vorschriften zur IT-Sicherheit sowie die organisationsweite IT-Sicherheitspolitik zu unterrichten.

7.3.1 Geregelte Einarbeitung/Einweisung neuer MitarbeiterInnen

Neuen MitarbeiterInnen müssen interne Regelungen, Gepflogenheiten und Verfahrensweisen im IT-Einsatz bekannt gegeben werden. Ohne eine entsprechende Einweisung kennen sie ihre AnsprechpartnerInnen bzgl. IT-Sicherheit nicht. Sie wissen nicht, welche IT-Sicherheitsmaßnahmen durchzuführen sind und welche IT-Sicherheitspolitik die Behörde bzw. das Unternehmen betreibt. Daraus können Störungen und Schäden für den IT-Einsatz erwachsen. Daher kommt der geregelten Einarbeitung neuer MitarbeiterInnen eine entsprechend hohe Bedeutung zu.

Die Einarbeitung bzw. Einweisung sollte zumindest folgende Punkte umfassen:

- Planung der notwendigen Schulungen; arbeitsplatzbezogene Schulungsmaßnahmen (siehe auch 7.3.2 Schulung vor Programmnutzung und 7.3.3 Schulung und Sensibilisierung zu IT-Sicherheitsmaßnahmen),
- Vorstellung aller AnsprechpartnerInnen, insbesondere zu IT-Sicherheitsfragen,
- Erläuterung der hausinternen Regelungen und Vorschriften zur IT-Sicherheit und der organisationsweiten IT-Sicherheitspolitik.

7.3.2 Schulung vor Programmnutzung

Durch unsachgemäßen Umgang mit IT-Anwendungen hervorgerufene Schäden können vermieden werden, wenn die BenutzerInnen eingehend in die IT-Anwendungen eingewiesen werden. Daher ist es unabdingbar, dass die BenutzerInnen vor der Übernahme IT-gestützter Aufgaben ausreichend geschult werden.

Dies betrifft sowohl die Nutzung von Standardprogrammpaketen als auch von speziell entwickelten IT-Anwendungen. Darüber hinaus müssen auch bei umfangreichen Änderungen in einer IT-Anwendung Schulungsmaßnahmen durchgeführt werden.

Stehen leicht verständliche Handbücher zu IT-Anwendungen bereit, so kann an Stelle der Schulung auch die Aufforderung stehen, sich selbstständig einzuarbeiten. Eine wesentliche Voraussetzung dazu ist allerdings die Bereitstellung ausreichender Einarbeitungszeit.

7.3.3 Schulung und Sensibilisierung zu IT-Sicherheitsmaßnahmen

Umfassende IT-Sicherheit kann nur dann gewährleistet werden, wenn alle beteiligten und betroffenen Personen einen angemessenen Kenntnisstand über IT-Sicherheit allgemein und insbesondere über die Gefahren und Gegenmaßnahmen in ihrem eigenen Arbeitsgebiet haben. Es liegt in der Verantwortung der Organisationsleitung, durch geeignete Schulungsmaßnahmen hierfür die nötigen Voraussetzungen zu schaffen. Darüber hinaus sollte alle BenutzerInnen dazu motiviert werden, sich auch in Eigeninitiative Kenntnisse anzueignen.

Angesichts des Umfangs der möglichen Schulungsthemen und der Bedeutung der IT-Sicherheit ist bei der Auswahl der Schulungsinhalte ein koordiniertes Vorgehen erforderlich. Dieses ist in Schulungskonzepten darzulegen und zu dokumentieren.

Es sollte versucht werden, Schulungsthemen zur IT-Sicherheit soweit möglich in andere Schulungskonzepte der betreffenden Organisation, etwa in die IT-Anwenderschulung, zu integrieren. Eine solche Einbindung hat den Vorteil, dass IT-Sicherheit unmittelbar als Bestandteil des IT-Einsatzes wahrgenommen wird.

Insbesondere sollen folgende Themen in der Schulung zu IT-Sicherheitsmaßnahmen vermittelt werden:

- Sensibilisierung für IT-Sicherheit: Die überwiegende Zahl von Schäden im IT-Bereich entsteht durch Nachlässigkeit. Um dies zu verhindern, ist jede/r Einzelne zum sorgfältigen Umgang mit der IT zu motivieren. Zusätzlich sind Verhaltensregeln zu vermitteln, die Verständnis für die IT-Sicherheitsmaßnahmen wecken. Alle MitarbeiterInnen sind auf die Notwendigkeit der IT-Sicherheit hinzuweisen. Das Aufzeigen der Abhängigkeit der Organisation und damit der Arbeitsplätze von dem reibungslosen Funktionieren der IT-Systeme ist ein geeigneter Einstieg in die Sensibilisierung. Darüber hinaus ist der Wert von Informationen herauszuarbeiten, insbesondere unter den Gesichtspunkten Vertraulichkeit, Integrität und Verfügbarkeit. Diese Sensibilisierungsmaßnahmen sind in regelmäßigen Zeitabständen zu wiederholen, evtl. auch durch praktische Hinweise z. B. in hausinternen Publikationen, im Intranet oder am „Schwarzen Brett“.

- Die mitarbeiterInnenbezogenen IT-Sicherheitsmaßnahmen: Zu diesem Thema sollen die IT-Sicherheitsmaßnahmen vermittelt werden, die in einem IT-Sicherheitskonzept erarbeitet wurden und von den einzelnen MitarbeiterInnen umzusetzen sind. Dieser Teil der Schulungsmaßnahmen hat große Bedeutung, da viele IT-Sicherheitsmaßnahmen erst nach einer entsprechenden Schulung und Motivation effektiv umgesetzt werden können.

- Die produktbezogenen IT-Sicherheitsmaßnahmen: Zu diesem Thema sollen die IT-Sicherheitsmaßnahmen vermittelt werden, die inhärent mit einem Softwareprodukt verbunden sind und bereits im Lieferumfang enthalten sind. Dies können neben Passwörtern zur Anmeldung, der Pausenschaltung durch Bildschirmschoner auch Möglichkeiten der Verschlüsselung von Dokumenten oder Datenfeldern sein. Hinweise und Empfehlungen über die Strukturierung und Organisation von Dateien, die anwendungsspezifische Daten enthalten, können die Vergabe von Zugriffsrechten erleichtern und den Aufwand für die Datensicherung deutlich reduzieren.

- Das Verhalten bei Auftreten eines Schadprogramms auf einem PC: Hier soll den MitarbeiterInnen vermittelt werden, wie mit Viren umzugehen ist. Mögliche Inhalte dieser Schulung sind
    - Wirkungsweise und Arten von Schadprogrammen
    - Vorbeugende Maßnahmen
    - Erkennen des Schadprogrammbefalls
    - Sofortmaßnahmen im Verdachtsfall
    - Maßnahmen zur Eliminierung des Schadprogrammes

- Der richtige Einsatz von Zugangscodes und Zugangskontrollmedien: Hierbei sollen die Bedeutung von Zugangscodes (Passwörtern, PINs, Zugangscodes für Voicemail etc.) und Zugangskontrollmedien (Karten, Token, Bürgerkarte, ...) für die IT-Sicherheit erläutert werden. Ebenso sind die Randbedingungen, die einen wirksamen Einsatz von Zugangscodes und Zugangskontrollmedien erst ermöglichen, herauszuarbeiten

- Die Bedeutung der Datensicherung und deren Durchführung: Die regelmäßige Datensicherung ist eine der wichtigsten IT-Sicherheitsmaßnahmen in jedem IT-System. Vermittelt werden sollen das Datensicherungskonzept der Organisation und die von jeder/jedem Einzelnen durchzuführenden Datensicherungsaufgaben. Besonders bedeutend ist dies für den PC-Bereich, in dem alle BenutzerInnen selbst die Datensicherung verantwortlich durchführen muss.

- Der geregelte Ablauf eines Datenträgeraustausches: Die Festlegung, wann welchen KommunikationspartnerInnen welche Datenträger übermittelt werden dürfen, ist allen Beteiligten bekannt zu geben. Werden bestimmte IT-gestützte Verfahren zum Schutz der Daten während des Austausches eingesetzt (wie etwa Verschlüsselung, digitale Signaturen oder Checksummenverfahren), so sind die MitarbeiterInnen in die Handhabung dieser Verfahren ausreichend einzuarbeiten.

- Der Umgang mit personenbezogenen Daten: An den Umgang mit personenbezogenen Daten sind besondere Anforderungen zu stellen. MitarbeiterInnen, die mit personenbezogenen Daten (sowohl in IT-Systemen als auch in Akten) arbeiten müssen, sind für die gesetzlich erforderlichen Sicherheitsmaßnahmen zu schulen. Dies betrifft etwa Meldepflichten, den Umgang mit den Rechten von Betroffenen (Auskunft, Richtigstellung, Löschung, Widerspruch, ...), Datensicherheitsmaßnahmen sowie Übermittlung und Überlassung von Daten.

- Die Einweisung in Notfallmaßnahmen: Sämtliche MitarbeiterInnen (auch nicht unmittelbar mit IT befasste Personen wie Portier oder Wachpersonal) sind in bestehende Notfallmaßnahmen einzuweisen. Dazu gehören die Erläuterung der Fluchtwege, die Verhaltensweisen bei Feuer, der Umgang mit Feuerlöschern, das Notfallmeldesystem (wer als Erstes wie zu benachrichtigen ist) und der Umgang mit dem Disaster Recovery-Handbuch.

- Richtiges Verhalten bei Auftreten von Sicherheitsproblemen (IHP): Die in den Incident Handling-Plänen (IHPs) festgelegten Aufgaben und Verantwortlichkeiten aller MitarbeiterInnen bei Auftreten sicherheitsrelevanter Ereignisse sind allen betroffenen MitarbeiterInnen bekannt zu machen, regelmäßige Schulungen und gegebenenfalls praktische Übungen sind vorzusehen (vgl. auch 7.3.5 Aktionen bei Auftreten von Sicherheitsproblemen (Incident Handling-Pläne))

- Vorbeugung gegen „Social Engineering“: Die MitarbeiterInnen sollen auf die Gefahren des „Social Engineerings“ hingewiesen werden. Die typischen Muster solcher Versuche, über gezieltes Aushorchen an vertrauliche Informationen zu gelangen, ebenso wie die Methoden, sich dagegen zu schützen, sollten bekannt gegeben werden. Da „Social Engineering“ oft mit der Vorspiegelung einer falschen Identität einhergeht, sollten MitarbeiterInnen regelmäßig darauf hingewiesen werden, die Identität von GesprächspartnerInnen zu überprüfen und insbesondere am Telefon keine vertraulichen Informationen weiterzugeben

7.3.4 Betreuung und Beratung von IT-BenutzerInnen

Neben der Schulung, die die IT-BenutzerInnen in die Lage versetzt, die vorhandene Informationstechnik sachgerecht einzusetzen, bedarf es einer Betreuung und Beratung der IT-BenutzerInnen für die im laufenden Betrieb auftretenden Probleme. Diese Probleme können aus Hardwaredefekten, fehlerhaften Softwareinstallationen, aber auch aus Bedienungsfehlern resultieren.

In größeren Behörden bzw. Unternehmen kann es daher sinnvoll sein, eine zentrale Stelle mit der Betreuung der IT-BenutzerInnen zu beauftragen und diese allen MitarbeiterInnen bekannt zu geben („Helpdesk“). Dabei hat sich die Wahl einer besonders leicht zu merkenden Telefonnummer besonders bewährt. Die Einrichtung eines Helpdesk kann sich insbesondere bei einer hohen Zahl dezentraler Systeme wie PCs als vorteilhaft erweisen. Es muss für alle BenutzerInnen klar ersichtlich sein, an wen sie sich in Problemfällen zu wenden haben.

7.3.5 Aktionen bei Auftreten von Sicherheitsproblemen

(Incident Handling-Pläne)
Die Aufgaben und Verantwortlichkeiten aller MitarbeiterInnen bei Auftreten von sicherheitsrelevanten Ereignissen sollten im Rahmen der organisationsweiten IT-Sicherheitspolitik (High-Level-Beschreibung) sowie spezieller „Incident Handling-Pläne“ (IHPs) sowohl für einzelne Bereiche als auch für die gesamte Organisation festgelegt werden (vgl. dazu auch 16.1.3 Erstellung eines Incident Handling-Plans und Richtlinien zur Behandlung von Sicherheitsvorfällen).

Unter sicherheitsrelevanten Ereignissen sind dabei zu verstehen:

- Angriffe und (vermutete) Angriffsversuche gegen ein IT-System
- (vermutete) Sicherheitsschwächen
- Funktionsstörungen von Systemen (etwa durch maliziöse Software)

Incident Handling-Pläne sollen in schriftlicher Form und verbindlich festlegen:

- wie auf sicherheitsrelevante Ereignisse zu reagieren ist,
- die Verantwortlichkeiten für die Meldung bzw. Untersuchung sicherheitsrelevanter Vorfälle,
- die einzuhaltenden Meldewege,
- die Protokollierung und Dokumentation sicherheitsrelevanter Vorfälle sowie
- die Ausbildung von Personen, die sicherheitsrelevante Vorfälle behandeln bzw. Gegenmaßnahmen treffen müssen.

IHPs sind allen betroffenen MitarbeiterInnen bekannt zu machen.

7.3.6 Schulung des Wartungs- und Administrationspersonals

Das Wartungs- und Administrationspersonal sollte mindestens so weit geschult werden, dass

- alltägliche Administrationsarbeiten selbst durchgeführt,
- einfache Fehler selbst erkannt und behoben,
- Datensicherungen selbsttätig durchgeführt
- Tätigkeiten im Normalbetrieb bis zur Erkennung von Problemen eigenhändig durchgeführt,
- die Eingriffe von externem Wartungspersonal nachvollzogen und
- Manipulationsversuche oder unbefugte Zugriffe auf die Systeme erkannt

werden können.

7.3.7 Einweisung in die Regelungen der Handhabung von Kommunikationsmedien

Der Einsatz neuer Medien und Geräte - dazu zählen Fax und Router genauso wie etwa Anrufbeantworter und Voice Mail - erleichtert die Kommunikation, bringt aber auch neue potenzielle Gefährdungen der Vertraulichkeit und Integrität von Informationen mit sich. Alle MitarbeiterInnen sind daher auf die Besonderheiten der Handhabung von solchen Geräten hinzuweisen und für potenzielle Gefahren zu sensibilisieren.

Verständliche Bedienungsanleitungen, Sicherheitshinweise und ggf. auch Dienstanweisungen sind den MitarbeiterInnen zur Kenntnis zu bringen und verfügbar zu halten.

Im Folgenden werden einige Beispiele angeführt, was solche Regelungen umfassen sollten. Sie sind den jeweiligen technischen Anforderungen und Möglichkeiten anzupassen.

Fax (Stand-alone-Gerät):

- Festlegung von Fax-Verantwortlichen, die für die Verteilung eingehender Fax-Sendungen zuständig sind und als AnsprechpartnerInnen in Fax-Problemfällen fungieren,
- Festlegung, wer das Faxgerät benutzen darf,
- Verbot des Versendens von vertraulichen Informationen per Fax (oder besondere technische und organisatorische Vorkehrungen für diesen Fall, wie etwa telefonische Ankündigung eines derartigen Fax),
- Verwendung einheitlicher Fax-Deckblätter,
- ggf. Kontrolle von Einzelsendenachweisen

Fernzugänge:

- Information über mögliche Gefährdungen, einzuhaltende Sicherheitsmaßnahmen und Regelungen beim Betrieb eines Modems oder Routers,
- Auswirkungen verschiedener Konfigurationen auf die Betriebssicherheit des Modems oder Routers.

Anrufbeantworter:

- Regelung über den Einsatz von Sicherungscodes für die Fernabfrage
- Vermeidung schutzbedürftiger Informationen auf Anrufbeantwortern,
- Regelmäßiges Abhören und Löschen aufgezeichneter Gespräche,
- Abschalten nicht benötigter Leistungsmerkmale.

7.3.8 Einweisung in die Bedienung von Schutzschränken

Nach der Beschaffung eines Schutzschrankes (Serverschrank oder Datensicherungsschrank) sind die BenutzerInnen in die korrekte Bedienung einzuweisen. Dies sollte auch bei Neuübertragung einer Aufgabe erfolgen, die die Nutzung eines Schutzschrankes umfasst.

Beispiele für zu vermittelnde Punkte sind:

- Korrekter Umgang mit dem Schloss des Schutzschrankes: Dabei ist auf typische Fehler hinzuweisen, wie zum Beispiel das Nichtverwerfen von Codeschlössern. Die Regelungen zur Schlüsselverwaltung, Schlüsselhinterlegung und Vertretungsregelung sind aufzuzeigen. Insbesondere ist einzufordern, dass der Schutzschrank bei - auch nur kurzfristiger - Nichtbenutzung verschlossen wird.
- Im Falle eines Serverschrankes ist darauf hinzuweisen, dass unnötige brennbare Materialien (Ausdrucke, überzählige Handbücher, Druckerpapier) nicht im Serverschrank aufbewahrt werden sollen.
- Datensicherungsträger des Servers sollten in einem anderen Brandabschnitt bzw. bei Bedarf disloziert gelagert werden. Eine Aufbewahrung im Serverschrank ist daher ungeeignet und nur dann zulässig, wenn eine Kopie der Datensicherungsbestände in einem anderen Brandabschnitt bzw. disloziert ausgelagert ist.
- Wird ein klimatisierter Serverschrank eingesetzt, sollten dessen Öffnungszeiten minimiert werden. Gegebenenfalls ist sporadisch zu kontrollieren, ob im Serverschrank Wasser kondensiert ist.

8.1.3.1 Herausgabe einer PC-Richtlinie

Um einen sicheren und ordnungsgemäßen Einsatz von Personalcomputern in größeren Organisationen zu gewährleisten, sollte eine PC-Richtlinie erstellt werden, in der verbindlich vorgeschrieben wird, welche Randbedingungen eingehalten werden müssen und welche IT-Sicherheitsmaßnahmen zu ergreifen sind. Diese PC-Richtlinie soll zumindest den Einsatz von unvernetzten PCs regeln; werden PCs vernetzt betrieben oder als intelligente Terminals genutzt, ist die Richtlinie um diese meist weiter einschränkenden Punkte zu erweitern. Im Folgenden wird grob umrissen, welche Inhalte für eine solche PC-Richtlinie sinnvoll sind.

Möglicher inhaltlicher Aufbau einer PC-Richtlinie:

- Zielsetzung und Begriffsdefinitionen: Dieser erste Teil der PC-Richtlinie soll dazu dienen, die PC-AnwenderInnen für IT-Sicherheit zu sensibilisieren und zu motivieren. Gleichzeitig werden die für das gemeinsame Verständnis notwendigen Begriffe definiert und eine einheitliche Sprachregelung geschaffen.
- Geltungsbereich: In diesem Teil muss verbindlich festgelegt werden, für welche Teile des Unternehmens bzw. der Behörde die PC-Richtlinie gilt.
- Rechtsvorschriften und interne Regelungen: Hier wird auf wichtige Rechtsvorschriften (z. B. das Datenschutzgesetz und das Urheberrechtsgesetz) hingewiesen. Darüber hinaus kann diese Stelle genutzt werden, um alle relevanten betriebsinternen Regelungen aufzuführen.
- Verantwortungsverteilung: In diesem Teil wird definiert, wer im Zusammenhang mit dem PC-Einsatz welche Verantwortung trägt. Dabei sind insbesondere die Funktionen IT-BenutzerInnen, Vorgesetzte, PC-AdministratorInnen, Datenschutz-/IT-Sicherheitsbeauftragte, Bereichs-IT-Sicherheitsbeauftragte und Applikations-/Projektverantwortliche zu unterscheiden.
- Umzusetzende und einzuhaltende IT-Sicherheitsmaßnahmen: Im letzten Teil der PC-Richtlinie ist festzulegen, welche IT-Sicherheitsmaßnahmen von den IT-BenutzerInnen einzuhalten bzw. umzusetzen sind. Es kann je nach Schutzbedarf auch über die IT-Grundschutzmaßnahmen hinausgehen.

Die PC-Richtlinie muss regelmäßig - insbesondere im Hinblick auf die IT-Sicherheitsmaßnahmen - aktualisiert werden.

Es ist dafür Sorge zu tragen, dass alle PC-BenutzerInnen ein Exemplar dieser Richtlinie besitzen und dass die Einhaltung regelmäßig überprüft wird. Sind TelearbeiterInnen im Unternehmen bzw. in der Behörde beschäftigt, sollte die PC-Richtlinie um die dafür spezifischen Regelungen ergänzt werden.

ISHB Anhang B.4 - Verpflichtungserklärung betreffend die Benutzung von IT-Systemen (Muster)

Verpflichtungserklärung betreffend die Benutzung der IT-Systeme des *(Unternehmen)*

Name, Titel: .....Organisationseinheit: .....

Als Bedienstete(r) des *(Unternehmens)* nehme ich hiermit zur Kenntnis, dass

- das unbefugte Kopieren und die unbefugte Weitergabe von Software strafrechtlich verfolgbar ist;
- die unbefugte Installation, Nutzung und Weitergabe von Software als Verletzung der Dienstpflichten geahndet wird;
- zur Beschaffung von Hardware und Software nur die geschäftseinteilungsmäßig berechtigten Bediensteten der Abteilung „XX“ *(z.B. IT-Abteilung)* berechtigt sind;
- zur Installation, Reparatur und Veränderung von Hardware und Software nur Bedienstete der Abteilung „XX“ *(z.B. IT-Abteilung)* im Rahmen ihrer dienstlichen Obliegenheiten bzw. Personen im Auftrag der Abteilung „XX“ *(z.B. IT-Abteilung)* berechtigt sind;
- die Abteilung „XX“ *(z.B. IT-Abteilung)* berechtigt ist, alle EDV-Systeme auf Kopien von unbefugt eingespielter Software zu prüfen, solche Softwarekopien zu löschen und verpflichtet ist, den Vorfall der Abteilung „YY“ *(z.B. Personalabteilung)* zu melden.

Ich nehme weiters nachstehende urheberrechtliche Bestimmungen zur Kenntnis:

- Originalsoftware darf ausschließliche insofern vervielfältigt und bearbeitet werden, als dies für ihre bestimmungsgemäße Benutzung durch die/den zu Benutzung Berechtigte/n notwendig ist (Arbeits- und Sicherungskopien);
- dem *(Unternehmen)* als Dienstgeber steht gemäß § 40b des Urheberrechtsgesetzes, BGBl. Nr. 111/1936, in der geltenden Fassung, ein unbeschränktes Werknutzungsrecht an allen von mir in Erfüllung meiner dienstlichen Obliegenheiten geschaffenen Computerprogrammen zu.

Um die Sicherheit des Computernetzwerkes und die Einhaltung der Software-Lizenzbestimmungen gewährleisten zu können, bestätige ich die Einhaltung folgender Benutzungsregeln:

- für die Vertraulichkeit der „Benutzerkennung“, die mir von einer/einem Bediensteten der Abteilung „XX“ *(z.B. IT-Abteilung)* mitgeteilt wurde, ist Sorge zu tragen;
- die Anwender/innen dürfen keine zusätzliche Hardware und Software auf dem PC installieren bzw. verwenden; die von der Abteilung „XX“ *(z.B. IT-Abteilung)* vorgegebene Konfiguration (Hard- und Software) darf nicht verändert werden, eine Änderung aus Versehen ist zum Schutz des gesamten Systems unverzüglich der Abteilung „XX“ *(z.B. IT-Abteilung)* zu melden;
- die Sicherung der lokal auf einem (nicht vernetzten) Einzelplatz-PC gehaltenen Daten hat in Eigenverantwortung zu erfolgen.

(Datum, Unterschrift)

ISHB Anhang B.7 - Verpflichtungserklärung zur Einhaltung des Datenschutzgesetzes (Muster)

Diese Verpflichtungserklärung betrifft:

Familienname: _____ (in BLOCKSCHRIFT)
Vornamen: _____ (in BLOCKSCHRIFT)

1) VERPFLICHTUNGSERKLÄRUNG
Im Zuge Ihres Dienstverhältnisses erhalten Sie voraussichtlich Kenntnis über Personen und personenbezogene Umstände und Daten sowie über technische Daten betreffend die technische Infrastruktur und den strukturellen Aufbau von Datenanwendungen.

Alle diese Daten sind absolut vertraulich zu behandeln und unterliegen den Bestimmungen des österreichischen Datenschutzgesetzes.

Mit Ihrer Unterschrift verpflichten Sie sich daher:

- das Datengeheimnis gemäß den Bestimmungen des Datenschutzgesetzes i.d.F. vom 25.05.2018 und später, insbesondere § 6 DSG (Datengeheimnis) zu wahren. (*Anmerkung: für Österreich ab 25.05.2018*)
- zu absoluter Verschwiegenheit über alle, Ihnen anlässlich Ihrer Tätigkeit bekannt gewordenen, nicht von den zuständigen Personen ausdrücklich als unbedenklich bezeichneten Dienst- und Amtsvorgänge.

Mit Ihrer Unterschrift verpflichten Sie sich weiters:

- unbefugten Personen oder unzuständigen Stellen die Kenntnisnahme von Daten, die Ihnen in Ausübung Ihres Dienstes bekannt geworden sind, nicht zu ermöglichen, sowie solche Daten nicht zu einem anderen als dem zum jeweiligen rechtmäßigen Aufgabenvollzug gehörenden Zweck zu verwenden,
- automationsunterstützt oder manuell verarbeitete Daten, die Ihnen auf Grund Ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger Verschwiegenheitspflichten, nur auf Grund einer ausdrücklichen mündlichen oder schriftlichen Zustimmung des Bundesministeriums für Inneres oder dessen Beauftragten zu verwenden,
- diese Verpflichtung auch nach Beendigung Ihres Mitarbeiterverhältnisses und dem Ausscheiden aus der Firma einzuhalten

Sie nehmen durch Ihre Unterschrift zur Kenntnis,

- dass weiterreichende andere Bestimmungen über die Geheimhaltungspflicht von der oben angeführten Verpflichtung unberührt bleiben, sofern sie nicht mit dem Datenschutzgesetz im Widerspruch stehen,
- dass als Dienst- und Amtsvorgänge insbesondere jene zur Kenntnis gelangten Vorgänge zu verstehen sind, die dienstinterner Natur sind, oder die Rechte Dritter berühren;
- dass Verstöße gegen die oben angeführte Verpflichtung zu entsprechender strafrechtlicher Verfolgung führen können, schadenersatzpflichtig machen und auch arbeitsrechtliche Folgen haben können (z.B. Entlassung gemäß § 27 Angestelltengesetz).

_____ _____
Ort, Datum Unterschrift des/der Verpflichteten

2) VERPFLICHTUNGSBESTÄTIGUNG
Herr/Frau ..... hat die oben stehende Verpflichtung in meiner Gegenwart unterschrieben.

Dem/Der Verpflichteten sind vor der Unterschriftleistung folgende Vorschriften ausgehändigt worden:

.....

_____ _____
Ort, Datum Unterschrift des/der Verpflichtenden

ISHB Anhang B.8 - Verpflichtungserklärung zur Nutzung von dienstlich beigestellten mobilen Arbeitsplatzrechnern (Muster)

Der/Die Notebook-Benutzer/in verpflichtet sich,

- das zugeteilte Notebook und den Zugang zu den organisationseigenen Ressourcen mittels Datenfernübertragungseinrichtung ausschließlich für dienstliche Zwecke zu verwenden;
- die unzulässige Verwendung des zugeteilten Notebooks und die zugeteilten Verbindungsparameter durch dritte Personen auf geeignete Art und Weise zu verhindern;
- mit dem zur Verfügung gestellten technischen Equipment nur von der Dienstgeberin bzw. vom Dienstgeber vorkonfigurierten bzw. bekannt gegebenen Verbindungen zu nutzen und keine Verbindungen zu anderen IT-Providern bzw. IT-Systemen, weder über Wählleitungsverbindungen noch über sonstige lokale Verbindungsmöglichkeiten (z.B. USB, Bluetooth, RS232, Ethernet, usw.), herzustellen;
- niemals gleichzeitig zwei oder mehrere DFÜ-Verbindungen zu unterschiedlichen IT-Systemen zu betreiben;
- bei Verbindungen zu Fremdsystemen erhöhte Vorsicht in sicherheitstechnischer Hinsicht walten zu lassen;
- für den Zugang zu den organisationseigenen Ressourcen mittels Datenfernübertragungseinrichtungen nur ein von der Arbeitgeberin bzw. vom Arbeitgeber zur Verfügung gestelltes, speziell gesichertes, technisches Equipment zu nutzen;
- in das Notebook von extern eingebrachte Daten unverzüglich und bestmöglich auf Computerviren zu prüfen und die Prüfsoftware in kürzestmöglichen Abständen auf Aktualität zu überprüfen und gegebenenfalls die Aktualität des Systems herzustellen;
- sich nach den Grundsätzen der Zweckmäßigkeit und Sparsamkeit zu bemühen, die Kosten für Verbindungen möglichst gering zu halten und nur jene Daten abzurufen, die für den dienstlichen Gebrauch nötig sind;
- bei der Verwendung von nicht durch die EDV-Abteilung zur Verfügung gestellten Programmen alle lizenzrechtlichen Bestimmungen zu beachten;
- Service und Reparaturen nur durch den Arbeitgeber bzw. von diesem benannte Fachwerkstätten durchführen zu lassen.

Die IT-Sicherheits-Verantwortlichen behalten sich das Recht vor, aktive Netzwerkverbindungen einer Benutzerin bzw. eines Benutzers sofort zu unterbrechen, wenn eine unzulässige Verwendung entdeckt wird.

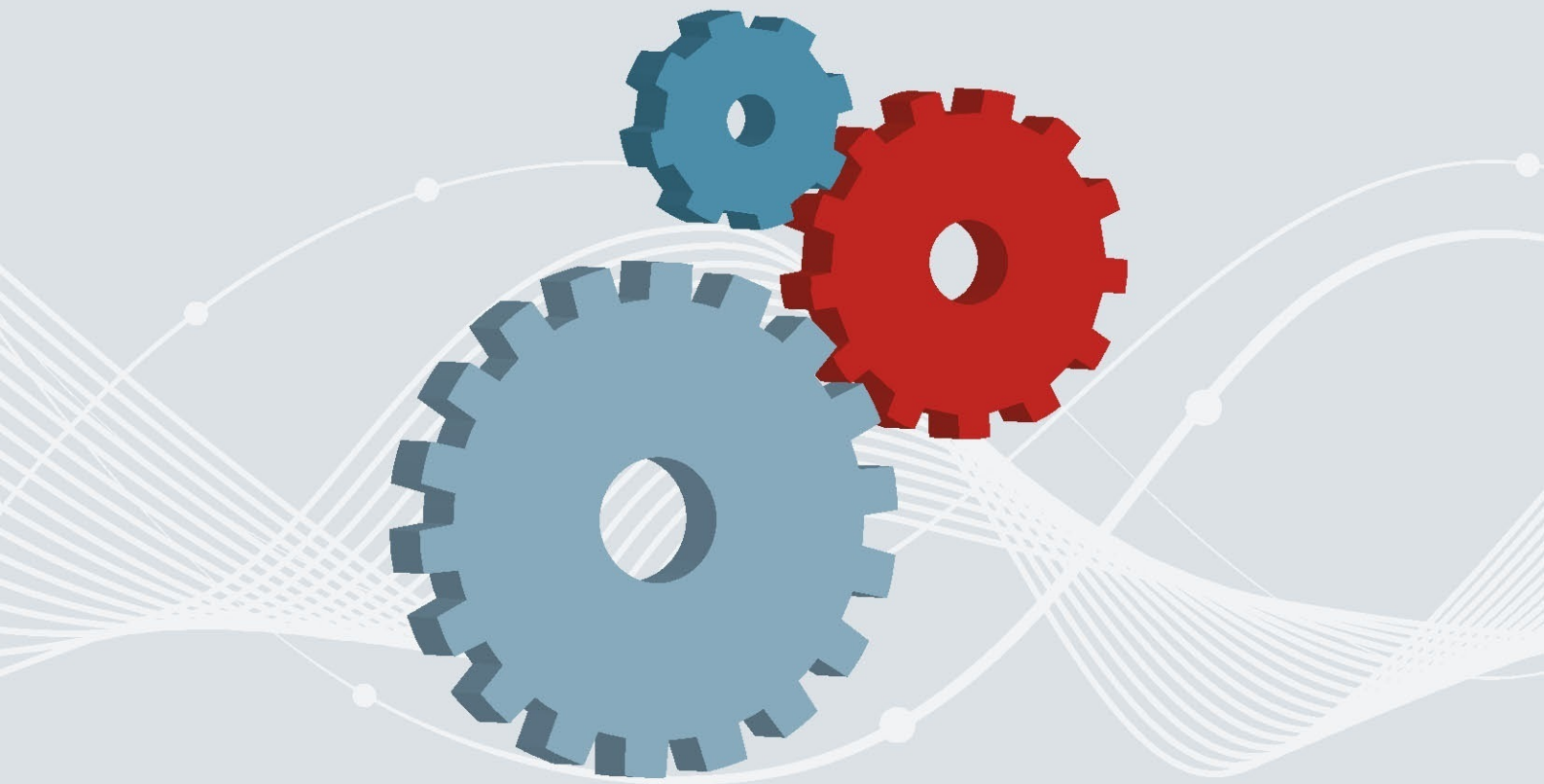
_____

Name der/des Bediensteten

_____

Datum und Unterschrift der/des Bediensteten

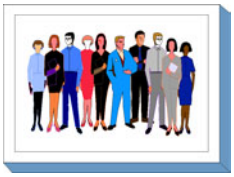
Bundesamt
für Sicherheit in der
Informationstechnik



IT-Grundschutz-Kataloge

15. Ergänzungslieferung - 2016

B 1.2 Personal



Beschreibung

In diesem Baustein werden die übergeordneten IT-Grundschutz-Maßnahmen erläutert, die im Bereich Personalwesen standardmäßig durchgeführt werden sollten. Beginnend mit der Einstellung von Mitarbeitern bis hin zu deren Weggang ist eine Vielzahl von Maßnahmen erforderlich. Auch für den Umgang mit Externen, wie z. B. Besuchern oder Wartungstechnikern, müssen angemessene Sicherheitsmaßnahmen vorhanden sein. Personelle Empfehlungen, die an eine bestimmte Funktion gebunden sind, wie z. B. die Ernennung des Systemadministrators eines LAN, werden in den Bausteinen angeführt, die sich mit dem jeweiligen Themengebiet beschäftigen.

Gefährdungslage

In diesem Baustein werden für den IT-Grundschutz die folgenden typischen Gefährdungen betrachtet:

Höhere Gewalt

- G 1.1 *Personalausfall*
- G 1.2 *Ausfall von IT-Systemen*

Organisatorische Mängel

- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.7 *Unerlaubte Ausübung von Rechten*

Menschliche Fehlhandlungen

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.36 *Fehlinterpretation von Ereignissen*
- G 3.37 *Unproduktive Suchzeiten*
- G 3.43 *Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen*
- G 3.44 *Sorglosigkeit im Umgang mit Informationen*
- G 3.77 *Mangelhafte Akzeptanz von Informationssicherheit*

Vorsätzliche Handlungen

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.20 *Missbrauch von Administratorrechten*
- G 5.23 *Schadprogramme*
- G 5.42 *Social Engineering*
- G 5.80 *Hoax*
- G 5.104 *Ausspähen von Informationen*

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 das in einem Unternehmen oder einer Behörde tätige Personal sind eine Reihe von Maßnahmen umzusetzen, beginnend mit einer geregelten Einarbeitung neuer Mitarbeiter, über Schulungen, bis hin zu einem geregelten Ausscheiden eines Mitarbeiters. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Umsetzung

Das Unternehmen bzw. die Behörde muss neuen Mitarbeitern bestehende Regelungen und Handlungsanweisungen bekannt machen (siehe M 3.1 *Geregelte Einarbeitung/Einweisung neuer Mitarbeiter*), damit diese zügig in die bestehenden Prozesse integriert werden können. Ebenso ist es unerlässlich, alle Mitarbeiter über Veränderungen dieser Regelungen und ihre spezifischen Auswirkungen auf einen Prozess oder auf den einzelnen Mitarbeiter zu unterrichten. Insbesondere bei sicherheitskritischen Betriebsumgebungen empfiehlt es sich, die Mitarbeiter entsprechend zu verpflichten und die Vertrauenswürdigkeit von Mitarbeitern bestätigen zu lassen (siehe M 3.33 *Sicherheitsüberprüfung von Mitarbeitern*). Besonderes Gewicht ist hierbei auf die Vertrauenswürdigkeit von Personen mit besonderen Funktionen und Berechtigungen zu legen (siehe M 3.10 *Auswahl eines vertrauenswürdigen Administrators und Vertreters*).

Betrieb

Die Motivation aller Mitarbeiter, Informationssicherheit in den Betriebsprozessen zu akzeptieren und auch eigenverantwortlich umzusetzen, muss durch geeignete Schulungen (siehe M 3.5 *Schulung zu Sicherheitsmaßnahmen*) und durch detaillierte Kenntnisse der Anwendungen (siehe M 3.4 *Schulung vor Programmnutzung*) auf fachlicher Ebene motiviert und gefördert werden. Hierbei kommt der Ausbildung des Administrations- und Wartungspersonals (siehe M 3.11 *Schulung des Wartungs- und Administrationspersonals*) ein besonderer Stellenwert zu, da dieser Personenkreis aufgrund seiner weitgehenden Rechte im Umgang mit der IT eine hohe Verantwortung trägt.

Um eine kontinuierliche Verfügbarkeit wichtiger Prozesse zu erreichen, muss dafür gesorgt werden, dass Schlüsselpositionen immer besetzt sind, wenn dies von den Abläufen her gefordert wird (siehe M 3.3 *Vertretungsregelungen*).

Kommunikationsprobleme, persönliche Probleme, schlechtes Betriebsklima, weitreichende organisatorische Veränderungen und Ähnliches sind ebenfalls Faktoren, die zu Sicherheitsrisiken führen können. Für solche Fälle sollten Vertrauenspersonen und Anlaufstellen eingerichtet sein (siehe M 3.7 *Anlaufstelle bei persönlichen Problemen*).

Funktionsänderungen

Bei Mitarbeitern, die die Institution verlassen oder andere Funktionen übernehmen, müssen bestehende Regelungen mit erhöhter Sorgfalt umgesetzt werden (siehe M 3.6 *Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern*). Bei kurzfristig ausscheidenden Mitarbeitern kann ein potentielles Risiko vorhanden sein, dass unberechtigterweise vertrauliche Informationen mitgenommen werden oder erst im nachhinein gezielte Manipulationen an Einrichtungen, IT-Systemen oder Daten bemerkt werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Personal" vorgestellt:

Planung und Konzeption
- M 2.226 (A) *Regelungen für den Einsatz von Fremdpersonal*
- M 3.51 (Z) *Geeignetes Konzept für Personaleinsatz und -qualifizierung*
- M 3.83 (Z) *Analyse sicherheitsrelevanter personeller Faktoren*

Beschaffung
- M 3.50 (Z) *Auswahl von Personal*

Umsetzung
- M 3.1 (A) *Geregelte Einarbeitung/Einweisung neuer Mitarbeiter*
- M 3.10 (A) *Auswahl eines vertrauenswürdigen Administrators und Vertreters*
- M 3.33 (Z) *Sicherheitsüberprüfung von Mitarbeitern*
- M 3.55 (C) *Vertraulichkeitsvereinbarungen*

Betrieb
- M 3.3 (A) *Vertretungsregelungen*
- M 3.4 (A) *Schulung vor Programmnutzung*
- M 3.5 (A) *Schulung zu Sicherheitsmaßnahmen*
- M 3.7 (Z) *Anlaufstelle bei persönlichen Problemen*
- M 3.8 (Z) *Vermeidung von Störungen des Betriebsklimas*

- M 3.11 (A) *Schulung des Wartungs- und Administrationspersonals*

Aussonderung

- M 3.6 (A) *Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern*

G 1.1 Personalausfall

Der Ausfall von Personal kann erhebliche Auswirkungen auf eine Institution und deren Geschäftsprozesse haben. Personal kann beispielsweise durch Krankheit, Unfall, Tod oder Streik unvorhergesehen ausfallen. Des weiteren ist auch der vorhersagbare Personalausfall bei Urlaub, Fortbildung oder einer regulären Beendigung des Arbeitsverhältnisses zu berücksichtigen, insbesondere wenn die Restarbeitszeit z. B. durch einen Urlaubsanspruch verkürzt wird.

In allen Fällen kann die Konsequenz sein, dass entscheidende Aufgaben aufgrund des Personalausfalls nicht mehr wahrgenommen werden können. Dies ist besonders dann kritisch, wenn die betroffene Person in einem Geschäftsprozess eine Schlüsselstellung einnimmt und aufgrund fehlenden Fachwissens anderer nicht ersetzt werden kann. Störungen des IT-Betriebs können die Folge sein. Dadurch können auch andere Bereiche und Prozesse der Institution massiv gestört werden.

Ein Personalausfall kann zusätzlich einen empfindlichen Verlust von Wissen und Geheimnissen nach sich ziehen, der die nachträgliche Übertragung der Tätigkeiten auf andere Personen unmöglich macht.

Beispiele:

- Aufgrund längerer Krankheit blieb der Netzadministrator einer Firma vom Dienst fern. In der betroffenen Firma lief das Netz zunächst fehlerfrei weiter. Nach zwei Wochen jedoch war nach einem Systemabsturz niemand in der Lage, den Fehler zu beheben, da es nur diesen in den Netzbetrieb eingearbeiteten Administrator gab. Dies führte zu einem Ausfall des Netzes über mehrere Tage.
- Während des Urlaubs eines Administrators musste in einer Institution für Datensicherungszwecke auf die Backupbänder im Datensicherungstresor zurückgegriffen werden. Der Zugangscode zum Tresor wurde erst kurz zuvor kürzlich geändert und ist war nur diesem Administrator bekannt. Erst nach mehreren Tagen konnte die Datenrestaurierung durchgeführt werden, da der Administrator nicht schneller im Urlaub erreicht werden konnte.
- Im Falle eine Pandemie fällt nach und nach längerfristig immer mehr Personal aus, sei es durch die Krankheit selbst, durch die Notwendigkeit Angehörige zu pflegen oder Kinder zu betreuen, die nicht mehr zur Schule oder in Kindergarten können, oder einfach aus Angst vor Ansteckung in öffentlichen Verkehrsmitteln oder in der Institution. Nur noch die notwendigsten Arbeiten können erledigt werden. Die erforderliche Wartung der Systeme, sei es der zentrale Server oder die notwendige Klimaanlage im Rechenzentrum, ist nicht mehr zu leisten. Nach und nach fallen dadurch immer mehr Systeme aus.

G 1.2 Ausfall von IT-Systemen

Der Ausfall einer Komponente eines IT-Systems kann zu einem Ausfall des gesamten IT-Betriebs und damit dem Ausfall wichtiger Geschäftsprozesse führen. Insbesondere zentrale Komponenten eines IT-Systems sind geeignet, solche Ausfälle herbeizuführen, z. B. LAN-Server oder Netzkoppelelemente. Auch der Ausfall von einzelnen Komponenten der technischen Infrastruktur, beispielsweise Klima- oder Stromversorgungseinrichtungen, kann zu einem Ausfall des gesamten Informationsverbunds beitragen.

Ursache für den Ausfall eines IT-Systems ist nicht immer technisches Versagen (z. B. G 4.1 *Ausfall der Stromversorgung*). Ausfälle lassen sich auch oft auf menschliches Fehlverhalten (z. B. G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*) oder vorsätzliche Handlungen (z. B. G 5.4 *Diebstahl*, G 5.102 *Sabotage*) zurückführen. Auch mangelnde Wartung, beispielsweise durch Ausfall des Wartungspersonals, kann zu technischem Versagen führen. Auch durch höhere Gewalt (z. B. Feuer, Blitzschlag, Chemieunfall) können Schäden eintreten, allerdings sind diese Schäden meist um ein Vielfaches höher.

Werden auf einem IT-System zeitkritische Anwendungen betrieben, sind die Folgeschäden nach einem Systemausfall entsprechend hoch, wenn es keine Ausweichmöglichkeiten gibt.

Beispiele:

- Durch Spannungsspitzen in der Stromversorgung wird das Netzteil eines wichtigen IT-Systems zerstört. Da es sich um ein älteres Modell handelt, steht nicht unmittelbar ein Ersatz bereit. Die Reparatur nimmt einen Tag in Anspruch, in dieser Zeit ist der gesamte IT-Betrieb nicht verfügbar.
- Es wird eine Firmware in ein IT-System eingespielt, die nicht für diesen Systemtyp vorgesehen ist. Das IT-System startet daraufhin nicht mehr fehlerfrei und muss vom Hersteller wieder betriebsbereit gemacht werden.
- Bei einem Internet Service Provider (ISP) führte ein Stromversorgungsfehler in einem Speichersystem dazu, dass dieses abgeschaltet wurde. Obwohl der eigentliche Fehler schnell behoben werden konnte, ließen sich die betroffenen IT-Systeme anschließend nicht wieder hochfahren, da Inkonsistenzen im Dateisystem auftraten. Bis alle Folgeprobleme behoben waren, waren mehrere der vom ISP betriebenen Webserver tagelang nicht erreichbar.
- In elektronischen Archiven kann der Zeitpunkt der erstmaligen Archivierung als Entstehungszeitpunkt von Dokumenten fehlinterpretiert werden, wenn keine anderweitigen Beweisverfahren, z. B. Zeitstempeldienste, zur Beglaubigung eingesetzt werden. Dies gilt vor allem für Geschäftsprozesse, in denen die elektronische Archivierung von massenhaft anfallenden Belegdaten transparent eingebunden ist. Im vorliegenden Fall konnte aufgrund des Ausfalls einer Archivkomponente ein Teil von Belegdaten erst um einen Tag verzögert archiviert werden. Durch die Verwendung von WORM-Medien wurde die Reihenfolge der physischen Archivierung der Geschäftsbelege trotzdem nachweisbar dokumentiert. Es wurde jedoch kein Nachweis für die ansonsten nicht auftretende Verzögerung durch die ausgefallene Archivkomponente geführt. Dadurch entstand bei einer späteren Prüfung der Eindruck einer nachträglichen Manipulation.

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 2.7 Unerlaubte Ausübung von Rechten

Rechte wie Zutritts-, Zugangs- und Zugriffsberechtigungen werden als organisatorische Maßnahmen eingesetzt, um Informationen, Geschäftsprozesse und IT-Systeme vor unbefugtem Zugriff zu schützen. Werden solche Rechte an die falsche Person vergeben oder wird ein Recht unautorisiert ausgeübt, kann sich eine Vielzahl von Gefahren für die Vertraulichkeit und Integrität von Daten oder die Verfügbarkeit von Rechnerleistung ergeben.

Beispiele:

- Der Arbeitsvorbereiter, der keine Zutrittsberechtigung zum Datenträgerarchiv besitzt, entnimmt in Abwesenheit des Archivverwalters Magnetbänder, um Sicherungskopien einspielen zu können. Durch die unkontrollierte Entnahme wird das Bestandsverzeichnis des Datenträgerarchivs nicht aktualisiert, die Bänder sind für diesen Zeitraum nicht auffindbar. Der Arbeitsvorbereiter, der keine Zutrittsberechtigung zum Datenträgerarchiv besitzt, entnimmt in Abwesenheit des Archivverwalters Magnetbänder, um Sicherungskopien einspielen zu können. Durch die unkontrollierte Entnahme wird das Bestandsverzeichnis des Datenträgerarchivs nicht aktualisiert, die Bänder sind für diesen Zeitraum nicht auffindbar.
- Ein Mitarbeiter ist erkrankt. Ein Zimmerkollege weiß aufgrund von Beobachtungen, wo dieser sein Passwort auf einem Merkzettel aufbewahrt und verschafft sich Zugang zum Rechner des anderen Mitarbeiters. Da er erst kürzlich durch ein Telefonat mitbekommen hat, dass der Kollege noch eine fachliche Stellungnahme abzugeben hatte, nimmt er hier unberechtigterweise diese Aufgabe im Namen seines Kollegen wahr, obwohl er zu der Thematik nicht auf dem aktuellen Sachstand ist. Eine daraus folgende Erstellung einer Ausschreibungsunterlage in der Verwaltungsabteilung fordert im Pflichtenheft daher eine längst veraltete Hardwarekomponente, weil die dortigen Mitarbeiter der fachlichen Stellungnahme des erfahrenen Kollegen uneingeschränkt vertraut haben.

G 2.16 Ungeordneter Benutzerwechsel bei tragbaren PCs

Der Benutzerwechsel bei tragbaren PC wie Laptops oder Notebooks wird oftmals durch die einfache Übergabe des Gerätes vorgenommen. Dies hat zur Folge, dass meist nicht sichergestellt wird, dass auf dem Gerät keine schutzbedürftigen Daten mehr gespeichert sind und dass das Gerät nicht mit einem Computer-Virus verseucht ist. Zudem ist nach einiger Zeit nicht mehr nachvollziehbar, wer den tragbaren PC wann genutzt hat oder wer ihn zurzeit benutzt. Der ungeordnete Benutzerwechsel ohne Speicherkontrollen und ohne entsprechende Dokumentation kann damit zur Einschränkung der Verfügbarkeit des Geräts und zum Vertraulichkeitsverlust von Restdaten der Festplatte führen.

G 2.21 Mangelhafte Organisation des Wechsels zwischen den Benutzern

Arbeiten mehrere Benutzer zeitlich versetzt an einem Einzelplatz-IT-System, so findet zwangsläufig ein Wechsel zwischen den Benutzern statt. Ist dieser nicht ausreichend organisiert und geregelt, wird er unter Umständen nicht sicherheitsgerecht durchgeführt. Hierdurch können Missbrauchsmöglichkeiten entstehen, wenn z. B.

- laufende Anwendungen nicht korrekt abgeschlossen werden,
- aktuelle Daten nicht gespeichert werden,
- Restdaten im Hauptspeicher oder in temporären Dateien verbleiben,
- der vorhergehende Benutzer sich nicht am IT-System abmeldet und
- der neue Benutzer sich nicht ordnungsgemäß am IT-System anmeldet.

G 2.36 Ungeeignete Einschränkung der Benutzerumgebung

Die meisten Betriebssysteme bieten die Möglichkeit, die Benutzerumgebung individuell für jeden Benutzer einzuschränken. Wo dies nicht der Fall ist, können hierfür im Allgemeinen spezielle Sicherheitsprodukte eingesetzt werden. Dabei bestehen prinzipiell zwei Möglichkeiten:

- Bestimmte Funktionalitäten werden erlaubt, alle anderen sind verboten.
- Bestimmte Funktionalitäten werden verboten, alle anderen sind erlaubt.

In beiden Fällen besteht die Möglichkeit, den Benutzer derart einzuschränken, dass dieser wesentliche Funktionen nicht mehr ausführen kann oder dass sogar ein sinnvolles und effizientes Arbeiten mit dem IT-System nicht mehr möglich ist.

Eine weitere Form, die Benutzerumgebung einzuschränken, besteht in der Begrenzung des nutzbaren Speicherplatzes. Reicht der zur Verfügung stehende Speicherplatz nicht mehr aus, so können keine weiteren Informationen gespeichert werden. Je nach Art und Aufteilung des betroffenen IT-Systems können hiervon eine Vielzahl von Benutzern und Anwendungen betroffen sein. Wenn dabei auf eine Trennung zwischen Daten- und Systempartition verzichtet wurde, kann das gesamte IT-System ausfallen, weil beispielsweise kein Speicherplatz für Auslagerungen des Arbeitsspeichers ("Swap") mehr vorhanden ist.

Beispiele:

- In einer Firma hatte der Administrator den Benutzern durch enge Quotas nur sehr wenig Speicherplatz auf dem Mailserver zur Verfügung gestellt, um die Benutzer zu disziplinieren. Diese sollten angehalten werden, die Mails nicht in den Eingangspostfächern, sondern in den jeweiligen Arbeitsverzeichnissen zu speichern. Dadurch liefen die E-Mail-Postfächer allerdings schon nach wenigen Mails über und die Benutzer konnten keine weiteren E-Mails empfangen.
- In einer Behörde war festgelegt worden, dass bestimmte sicherheitsrelevante Informationen wie Anmeldeversuche ein Jahr lang protokolliert werden sollten. Da für die Protokoll-Daten aber zu wenig Platz auf dem Server vorhanden war, wurden diese immer automatisch nach einer Woche gelöscht. Als auffiel, dass geschäftsrelevante Daten manipuliert worden waren, konnte zwar eine Sicherheitslücke entdeckt werden, es ließ sich aber nicht mehr nachvollziehen, wie und durch wen diese ausgenutzt worden war.

G 2.41 Mangelhafte Organisation des Wechsels von Datenbank-Benutzern

Teilen sich mehrere Benutzer einer Datenbank den gleichen Arbeitsplatz, so besteht die Gefahr von ungewollten oder gezielten Datenmanipulationen, wenn der Wechsel zwischen den Benutzern nicht organisiert ist bzw. der Wechsel nicht ordnungsgemäß durchgeführt wird. Auch ist dann die Vertraulichkeit der Daten nicht mehr gewährleistet.

Beispiel:

Wird eine Anwendung, die auf eine Datenbank zugreift, vor einem Benutzerwechsel nicht ordnungsgemäß verlassen, so führen die unterschiedlichen Berechtigungsprofile der betroffenen Benutzer zu den oben genannten Gefährdungen. Auch wird dabei der Protokollmechanismus der Datenbank unterlaufen, da dieser die Datenmodifikationen und Aktivitäten der aktiven Benutzer-Kennung festhält. Diese Kennung stimmt aber in einem solchen Fall nicht mit dem tatsächlichen Benutzer überein. Dadurch können Datenmodifikationen nicht mehr eindeutig einem Benutzer zugeordnet werden.

G 2.103 Unzureichende Schulung der Mitarbeiter

IT-Benutzer aller Art werden häufig zu wenig in der Bedienung der von ihnen eingesetzten IT-Systeme geschult. Dies trifft leider sogar öfters auf Administratoren und Benutzerbetreuer zu. Vielfach werden teure Systeme und Anwendungen angeschafft, aber keine oder nur unzureichend Mittel für die Schulung der IT-Benutzer bereitgestellt.

Dies kann durch unabsichtliche Fehlbedienungen, falsche Konfiguration und ungeeignete Betriebsmittel zu gravierenden Sicherheitsproblemen führen. Häufig wenden Benutzer neu eingeführte Sicherheitsprogramme deswegen nicht an, weil sie nicht wissen, wie sie bedient werden und eine selbstständige Einarbeitung oft als zu zeitaufwendig im täglichen Arbeitsablauf gesehen wird. Daher reicht die Beschaffung und Installation einer Sicherheitssoftware noch lange nicht aus.

Beispiele:

- Während der Datenerfassung erschien eine dem Benutzer nicht bekannte Fehlermeldung. Da bei den meisten Fehlermeldungen das Anklicken von "ok" bisher keinen Schaden verursachte, wählte er an diesem Fall auch "ok". Nur diesmal bewirkte dies das Herunterfahren des Systems und folglich den Verlust der bis dahin eingegebenen Daten.
- Ein teures Firewall-System wurde beschafft. Der Administrator eines anderen IT-Systems wurde "durch Handauflegen" zum Administrator dieses Firewall-Systems bestimmt. Da er als unabkömmlich galt und alle verfügbaren Mittel für die System-Beschaffung verwendet worden waren, wurde er aber weder in der Bedienung der System-Plattform noch für den eingesetzten Firewall-Typ ausgebildet. Externe Seminare wurden aus Geldmangel verweigert, nicht einmal zusätzliche Handbücher angeschafft. Zwei Monate nach Inbetriebnahme des Firewall-Systems stellte sich heraus, dass durch eine Fehlkonfiguration der Firewall interne Systeme aus dem Internet frei zugänglich waren.
- In einem Unternehmen wurde die Migration auf ein neues Betriebssystem vorbereitet. Der dafür verantwortliche Mitarbeiter war zwar ein ausgezeichneter Kenner der bis dahin eingesetzten Plattform, kannte sich aber mit den diskutierten neuen Systemen nicht aus und erhielt auch keine dem entsprechende Schulung. Daher besuchte er einige kostenfreie Veranstaltungen eines Herstellers, dessen Produkte er auch danach favorisierte. Dies führte zu einer kostenintensiven Fehlentscheidung durch Einführung eines ungeeigneten Produktes.
- Für die Internet-Nutzung während der Dienstreisen wurden auf den Notebooks der Mitarbeiter Personal Firewalls installiert. Die Mitarbeiter wurden nicht dazu geschult, eine Abstimmung der Einstellungen der Firewall mit den Bedürfnissen der Mitarbeiter fand nicht statt. Viele Mitarbeiter haben daraufhin die Firewall abgeschaltet, um problemlos alle Internet-Seiten zu erreichen, die sie brauchten. Das Ergebnis war, dass schon nach einigen Wochen viele der Rechner mit Schadprogrammen verseucht waren. Neben dem Datenverlust war der Ansehensschaden erheblich, da sich ein Schadprogramm über Mails an Kunden weitergesendet hatte.

G 2.201 Unzureichende Berücksichtigung von Veränderungen im Arbeitsumfeld von Mitarbeitern

Institutionen müssen sich regelmäßig an veränderte Anforderungen und Rahmenbedingungen anpassen, um ihre Geschäftsziele zu erreichen und ihre Wettbewerbsfähigkeit zu behaupten. Damit unterliegen auch ihre Prozesse und eingesetzten IT-Systeme einem ständigen organisatorischen und technischen Wandel.

Eine vergleichbare Situation liegt auch für die Mitarbeiter vor: Sie erleben als Teil der Institution diesen Wandel mit und müssen sich an Veränderungen in den Arbeitsaufgaben, in den bekleideten Positionen sowie an Arbeiten mit unterschiedlichen technischen Systemen anpassen. Dies kann für Mitarbeiter eine Chance sein sich weiterzuentwickeln, aber auch demotivierend wirken. Dadurch können Veränderungen dazu führen, dass Sicherheitsvorgaben nicht wie vorgesehen beachtet werden.

Veränderungen für die Mitarbeiter ergeben sich vor allem aus folgenden Ereignissen:

- persönliche Entwicklung der Mitarbeiter innerhalb der Institution (Versetzung, Beförderung, Weggang etc.),
- Änderungen in der oder für die Institution (Umstrukturierungen, Übernahmen etc.),
- Einführung neuer oder geänderter Geschäftsprozesse oder IT-Verfahren.

Damit sich dabei der Umgang der Mitarbeiter mit Informationen und mit der Informationssicherheit verändern kann, müssen diese Ereignisse zielgruppenspezifisch in institutionsweite Sensibilisierungs- und Schulungsmaßnahmen eingebunden werden.

Beispiele:

- Ein Praktikant wird nach Abschluss des Studiums in die Institution übernommen und einer Fachabteilung zugewiesen. Seine IT-Berechtigungen sind aber auch jetzt noch sehr weitreichend, da er im Rahmen seines Praktikums in verschiedenen Abteilungen der Institution eingesetzt wurde. So kann er weiterhin auf Informationen aus der Personalabteilung zugreifen, obwohl dies nicht für die Erfüllung seiner neuen Aufgabe erforderlich ist.
- In einer Abrechnungsabteilung wird das Abrechnungssystem durch das Produkt eines neuen Herstellers ersetzt. Die Administratoren werden zwar zum neuen Abrechnungssystem geschult, aber nur zu allgemeinen Grundlagen, nicht zu Sicherheitsaspekten. Dadurch werden wichtige Sicherheitseinstellungen nicht vorgenommen.
- Ein Mitarbeiter wird in den Ruhestand verabschiedet. Die im Laufe seiner Organisationszugehörigkeit unterzeichneten Richtlinien und Vereinbarungen zur Informationssicherheit werden als bekannt und präsent vorausgesetzt. Der Mitarbeiter wird bei seinem Weggang nicht explizit auf weiterhin noch bestehende Verschwiegenheitspflichten hingewiesen. Daher nutzt er die gewonnene Freizeit, um sich in Internetforen und bei persönlichen Treffen mit anderen Personen über das Arbeitsleben auszutauschen und dabei vertrauliche Informationen über die Institution preiszugeben.

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 3.2 Fahrlässige Zerstörung von Gerät oder Daten

Durch Fahrlässigkeit, aber auch durch ungeschulten Umgang kann es zu Zerstörungen an Geräten und Daten kommen, die den Betrieb des IT-Systems empfindlich stören können. Dies ist auch durch die unsachgemäße Verwendung von IT-Anwendungen möglich, wodurch fehlerhafte Ergebnisse entstehen oder Daten unabsichtlich verändert oder zerstört werden. Durch unachtsames Benutzen eines einzigen Löschbefehls können ganze Dateistrukturen gelöscht werden.

Beispiele:

- Benutzer, die aufgrund von Fehlermeldungen den Rechner ausschalten, statt ordnungsgemäß alle laufenden Anwendungen zu beenden bzw. einen Sachkundigen zu Rate zu ziehen, können hierdurch schwerwiegende Integritätsfehler in Datenbeständen hervorrufen.
- Durch umgestoßene Kaffeetassen oder beim Blumengießen eindringende Feuchtigkeit können in einem IT-System Kurzschlüsse hervorrufen werden.
- In einem z/OS-System verfügte ein Systemprogrammierer über die Berechtigung, das Programm *ICKDSF* zum Formatieren von Festplatten aufzurufen. Als er zur Ausübung seiner Tätigkeit dringend eine Festplatte benötigte, wählte er aus dem vorhandenen Pool eine freie Festplatte aus, gab jedoch aufgrund eines Tippfehlers eine falsche Adresse an. Den im System-Log anstehenden Reply las er nur flüchtig und beantwortete ihn sofort. Die Formatierung einer bereits belegten Festplatte wurde dadurch freigegeben und wichtige Produktionsdaten zerstört.
- Ein Benutzer, der es sich zur Gewohnheit gemacht hat, unter Unix den Löschbefehl *rm* grundsätzlich ohne den Parameter für die Sicherheitsabfragen (*-i*) durchzuführen oder gar mit *-f* die Sicherheitsabfragen grundsätzlich ausschaltet, riskiert in hohem Maße das versehentliche Löschen von Dateien.

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 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal

Es ist bereits nicht immer ganz einfach, eigene Mitarbeiter ausreichend zum richtigen Umgang mit geschäftskritischen Informationen und mit IT-Systemen zu schulen. Bei Betriebsfremden kann grundsätzlich nicht vorausgesetzt werden, dass sie mit ihnen zugänglichen Informationen und der Informationstechnik entsprechend den Vorgaben der besuchten Institution umgehen, vor allem, da sie diese in den seltensten Fällen kennen.

Besucher, Reinigungs- und Fremdpersonal können interne Informationen, Geschäftsprozesse und IT-Systeme auf verschiedene Art und Weise gefährden, angefangen von der unsachgemäßen Behandlung der technischen Einrichtungen, über den Versuch des "Spielens" an IT-Systemen bis zum Diebstahl von Unterlagen oder IT-Komponenten.

Beispiele:

- Besucher können, wenn sie unbegleitet sind, Zugriff auf Unterlagen, Datenträger oder Geräte haben, diese beschädigen oder unbefugt Kenntnis von schützenswerten Informationen erlangen.
- Durch Reinigungspersonal kann versehentlich eine Steckverbindung gelöst werden, Wasser kann in Geräte gelangen, Unterlagen können verlegt oder sogar mit dem Abfall entfernt werden.
- Ein externer Mitarbeiter hatte auf seinem Laptop Unterlagen gespeichert, die vor einer Besprechung in einer Behörde noch ausgedruckt werden sollten. Dafür wurden diese schnell per USB-Stick auf einen Rechner im LAN der Behörde kopiert. Dabei wurde allerdings auch Schadsoftware mitübertragen.
- In einem Rechenzentrum sollten in den Maschinenräumen Malerarbeiten durchgeführt werden. Der Maler stieß mit der Leiter versehentlich an den zentralen Notausschalter der Stromversorgung und löste diesen aus. Die gesamte Stromversorgung der z/OSin diesem Rechenzentrum war sofort unterbrochen. Durch den Stromausfall waren mehrere Platten (DASD - Direct Access Storage Device) nicht sofort verfügbar. Der hinzugezogene Techniker benötigte mehrere Stunden, bis die Produktion wieder anlaufen konnte.

G 3.8 Fehlerhafte Nutzung von IT-Systemen

Eine fehlerhafte oder nicht ordnungsgemäße Nutzung von IT-Systemen kann deren Sicherheit beeinträchtigen, wenn dadurch Sicherheitsmaßnahmen missachtet oder umgangen werden.

Beispielsweise können zu großzügig vergebene Rechte, leicht zu erratende Passwörter, nicht ausreichend geschützte Datenträger mit Sicherungskopien oder bei vorübergehender Abwesenheit nicht gesperrte Terminals zu Sicherheitsvorfällen führen.

Gleichermaßen können durch die fehlerhafte Bedienung von IT-Systemen oder Anwendungen Daten versehentlich gelöscht oder verändert werden. Dadurch könnten aber auch vertrauliche Informationen an die Öffentlichkeit gelangen, beispielsweise wenn Zugriffsrechte falsch gesetzt werden.

G 3.9 Fehlerhafte Administration von IT-Systemen

Eine Administration beeinträchtigt die Sicherheit eines IT-Systems, wenn dadurch Sicherheitsmaßnahmen missachtet oder umgangen werden. Jede Modifikation von Sicherheitseinstellungen und die Erweiterung von Zugriffsrechten stellt eine potenzielle Gefährdung der Gesamtsicherheit dar.

Durch die fehlerhafte Installation von Software können Sicherheitsprobleme entstehen. Standard-Installationen von Betriebssystemen oder Systemprogrammen weisen in den seltensten Fällen alle Merkmale einer sicheren Konfiguration auf. Mangelnde Anpassungen an die konkreten Sicherheitsbedürfnisse können hier ein erhebliches Risiko darstellen. Die Gefahr von Fehlkonfigurationen besteht insbesondere bei komplexen Sicherheitssystemen, bei denen sich Systemfunktionen oft gegenseitig beeinflussen.

Die Ursachen für fehlerhaft ausgeführte Administrationstätigkeiten können vielfältigen Ursprungs sein. Denkbar sind hier beispielsweise Fehlbedienungen, die durch nachfolgende Aspekte hervorgerufen werden.

- Die Prozessdokumentation fehlt oder ist nicht aktualisiert. Sie gibt dem Administrator keinen Aufschluss über die Handhabung notwendiger Sicherheitseinstellungen.
- Die hohe technische Komplexität des IT-Systems führt dazu, dass der Administrator die Auswirkungen seiner Tätigkeiten in ihrer Gesamtheit nicht mehr überschauen kann. Durch die Anpassung eines Systemparameters werden weitere Parameter beeinflusst, die unter Umständen ursprünglich nicht im Zusammenhang standen.
- Die fehlende Standardisierung eines IT-Systems oder seiner Komponenten führt dazu, dass dieses auf die Einstellungen eines Administrators anders reagiert als gewünscht.
- Bedingt durch die fehlende Umsetzung des 4-Augen-Prinzips bleibt der Bedienungsfehler eines Administrators zunächst unentdeckt.
- Die eingesetzten Administratoren verfügen über unzureichende Kenntnisse im Zusammenhang mit der Bedienung der eingesetzten IT-Systeme.
- Die falsche Interpretation von aufgezeichneten Ereignissen führt zur Ausführung administrativer Arbeiten, die sich in der Folge als fehlerhaft erweisen. Die tatsächliche Ursache für das Ereignis wird dadurch zunächst nicht untersucht.

Die Durchführung von Wartungs- bzw. Betriebsarbeiten erfolgt in der Regel auf Basis administrativer Berechtigungen. Mögliche Gefährdungen für die Institution ergeben sich hierbei beispielsweise durch:

- die Nichteinhaltung von Standard-Arbeitsanweisungen (*Standard Operating Procedures,*SOP),
- eine falsche Patch-Reihenfolge,
- das Einspielen von Patches ohne das Durchlaufen eines vorherigen Test- und Freigabeverfahrens,
- die Nichtbeachtung der Kompatibilitätsmatrix des Herstellers.

Die Erstellung und Pflege eines entsprechenden Betriebshandbuchs ist die Voraussetzung für die Nachvollziehbarkeit der Konfiguration und Funktionsweise der eingesetzten IT-Systeme. Fehlt dieses, können Fehler unter Umständen verzögert nachvollzogen und beseitigt werden.

G 3.17 Kein ordnungsgemäßer PC-Benutzerwechsel

Arbeiten mehrere Benutzer an einem PC, so kann es aufgrund von Nachlässigkeit oder Bequemlichkeit dazu kommen, dass sich bei einem Wechsel der vorhergehende Benutzer nicht abmeldet und der neue sich nicht ordnungsgemäß anmeldet. Dies wird von den Betroffenen meist damit begründet, dass die Zeit, die das IT-System zum Neustarten benötigt, sehr lang ist und als nicht akzeptabel empfunden wird.

Dieses Fehlverhalten führt jedoch dazu, dass die Protokollierung von An- und Abmeldevorgängen und damit ein Teil der Beweissicherung unwirksam wird. Es lässt sich anhand der Protokolle nicht mehr zuverlässig feststellen, wer den Rechner zu einem bestimmten Zeitpunkt genutzt hat.

Beispiele:

- Ein PC wird abwechselnd von drei Benutzern eingesetzt, um Reisekostenabrechnungen durchzuführen. Nachdem der erste Benutzer den Anmeldevorgang durchgeführt hat, erfolgt kein ordnungsgemäßer PC-Benutzerwechsel mehr, weil die damit verbundenen Ab- und Anmeldevorgänge aus Bequemlichkeit nicht durchgeführt werden.
- Aufgrund von Unregelmäßigkeiten wird geprüft, wer welchen Vorgang am Rechner bearbeitet hat. Da nach Protokollierung nur ein Benutzer am PC gearbeitet hat, kann der Verursacher im Nachhinein nicht mehr festgestellt werden bzw. der einzige angemeldete Benutzer muss die Konsequenzen tragen.

G 3.36 Fehlinterpretation von Ereignissen

Beim Einsatz eines Managementsystems ist es eine Aufgabe des jeweils verantwortlichen Systemadministrators, die Meldungen des Managementsystems zu analysieren und zu interpretieren, um dann geeignete Maßnahmen einzuleiten. In der Regel basieren die Meldungen des Managementsystems auf Überwachungsmechanismen, die Systemprotokolle unterschiedlichster Art automatisch nach gewissen Regeln durchsuchen. Es ist dabei nicht einfach, aus der Fülle der anfallenden Protokolldaten automatisiert Anomalien, die auf Systemfehler hindeuten, zu erkennen und entsprechende Meldungen an den Systemadministrator zu erzeugen. Darüber hinaus kann ein Fehler hier sogar unentdeckt bleiben. Die eingehenden Meldungen müssen daher immer vom Systemadministrator gesichtet und interpretiert werden, da die Meldungen (im Fehlerfall) auf Fehlersymptome und deren (automatischer) Interpretation beruhen. Ein Systemadministrator muss hier auch Fehlalarme und Falschmeldungen erkennen können. Werden Systemmeldungen vom Administrator falsch interpretiert, so führen vermeintlich korrigierende Gegenmaßnahmen u. U. zu einer Verschlimmerung der Situation.

G 3.37 Unproduktive Suchzeiten

Im Internet werden Millionen von Informationsseiten, Dokumenten und Dateien angeboten. Zum Navigieren in diesem riesigen Informationsangebot wird eine durch einfachen Mausklick zu bedienende Querverweistechnik verwendet. Sie erlaubt den schnellen Wechsel auf weiterführende Informationsseiten, die ihrerseits wieder neue Querverweise auf weitere Seiten beinhalten. Das Springen über Querverweise von einer Informationsseite zu weiteren wird als "Surfen" bezeichnet und kann zu sehr langen Suchzeiten führen.

In vielen Organisationen wurden Internet-Dienste eingeführt, ohne die damit verbundenen Ziele und erwarteten Auswirkungen vorher konkret zu untersuchen. Die Schulungen und Hilfen für die Benutzer sind häufig nicht ausreichend, so dass es zu unproduktiven Suchzeiten im vielfältigen Angebot des Internets kommt. Die Kosten für diese Abfragen sind oft weder den Benutzern noch den Verantwortlichen bekannt. Nach Schätzung einer Unternehmensberatung entstehen durch Surfen sowie unnötige und langatmige Recherchen im Internet vermeidbare Personal- und Kommunikationskosten in mehrstelliger Millionenhöhe je Jahr.

G 3.38 Konfigurations- und Bedienungsfehler

Konfigurationsfehler entstehen durch eine falsche oder nicht vollständige Einstellung von Parametern und Optionen, mit denen ein Programm gestartet wird. In diese Gruppe fallen unter anderem falsch gesetzte Zugriffsrechte für Dateien. Bei Bedienungsfehlern sind nicht einzelne Einstellungen falsch, sondern die IT-Systeme oder IT-Anwendungen werden falsch behandelt. Ein Beispiel hierfür ist das Starten von Programmen, die für den Einsatzzweck des Rechners nicht notwendig sind, aber von einem Angreifer missbraucht werden können.

Beispiele für aktuelle Konfigurations- bzw. Bedienungsfehler sind das Speichern von Passwörtern auf einem PC, auf dem ungeprüfte Software aus dem Internet ausgeführt wird, oder das Laden und Ausführen von schadhaften ActiveX-Controls. Diese Programme, die unter anderem, die Aufgabe haben, Webseiten durch dynamische Inhalte attraktiver zu machen, werden mit den gleichen Rechten ausgeführt, die auch der Benutzer hat. Sie können beliebig Daten löschen, verändern oder versenden.

Viele Programme, die für die ungehinderte Weitergabe von Informationen in einem offenen Umfeld gedacht waren, können bei falscher Konfiguration potenziellen Angreifern Daten zu Missbrauchszwecken liefern. So kann beispielsweise der *finger*-Dienst darüber informieren, wie lange ein Benutzer bereits am Rechner sitzt. Aber auch Browser übermitteln bei jeder Abfrage einer Datei eine Reihe von Informationen an den Webserver (z. B. die Version des Browsers und des verwendeten Betriebssystems, den Namen und die Internet-Adresse des PCs). In diesem Zusammenhang sind auch die Cookies zu nennen. Hierbei handelt es sich um Dateien, in denen Webserver-Betreiber Daten über den Benutzer auf dessen Rechner speichern. Diese Daten können beim nächsten Besuch des Servers abgerufen und vom Server-Betreiber für eine Analyse, der vom Benutzer vorher auf dem Server besuchten Webseiten, verwendet werden.

Der Einsatz eines Domain Name Systems stellt eine weitere Gefahrenquelle dar. Zum einen ermöglicht ein falsch konfigurierter DNS-Server die Abfrage von vielen Informationen über ein lokales Netz. Zum anderen hat ein Angreifer durch die Übernahme dieses Servers die Möglichkeit, gefälschte IP-Adressen zu verschicken, sodass jeglicher Verkehr von ihm kontrolliert werden kann.

Eine große Bedrohung geht auch von den automatisch ausführbaren Inhalten (*Executable Content*) in E-Mails oder HTML-Seiten aus. Dies ist unter dem Stichwort Content-Security-Problem bekannt. Dateien, die aus dem Internet geholt werden, können Code enthalten, der bereits beim "Betrachten" und ohne Rückfrage beim Benutzer ausgeführt wird. Dies ist z. B. bei Makros in Office-Dateien der Fall und wurde zum Erstellen von sogenannten Makro-Viren ausgenutzt. Auch Programmiersprachen und -schnittstellen wie ActiveX, Javascript oder Java, die für Anwendungen im Internet entwickelt worden sind, besitzen bei falscher Implementierung der Kontrollfunktionen ein Schadpotenzial.

Die Verfügbarkeit des Sicherheitssystems RACF ist bei z/OS-Betriebssystemen von zentraler Bedeutung für die Verfügbarkeit des gesamten Systems. Durch unsachgemäßen Einsatz von z/OS-Utilities bei der RACF-Datenbanksicherung oder fehlerhafte Bedienung der RACF-Kommandos kann diese eingeschränkt werden.

G 3.43 Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen

Selbst die Nutzung von durchdachten Authentikationsverfahren hilft wenig, wenn die Benutzer nicht sorgfältig mit den benötigten Zugangsmitteln umgehen. Unabhängig davon, ob Passwörter, PINs oder Authentikationstoken eingesetzt werden, werden diese immer wieder weitergegeben oder unsicher aufbewahrt.

Benutzer geben oft aus Bequemlichkeit Passwörter an andere Benutzer weiter. Häufig werden Passwörter innerhalb von Arbeitsgruppen geteilt, um jedem Mitarbeiter den Zugriff auf gemeinsam zu bearbeitende Dateien zu erleichtern. Der Zwang zur Passwortbenutzung wird oft als lästig empfunden und dadurch unterlaufen, dass Passwörter nie gewechselt werden oder alle Mitarbeiter dasselbe Passwort benutzen.

Immer wieder finden sich IT-Systeme und Anwendungen, bei denen die vom Hersteller voreingestellten Passwörter nicht geändert wurden. Häufig betrifft dies sogar die Administrator-Passwörter, die nicht geändert wurden, um sie nicht vergessen zu können. Standard-Passwörter sind jedoch allgemein bekannt und stellen damit ein hohes Sicherheitsrisiko dar.

Wird zur Benutzer-Authentisierung ein Token-basiertes Verfahren eingesetzt (z. B. Chipkarte oder Einmalpasswortgenerator), so ergibt sich bei Verlust die Gefahr, dass das Token unberechtigt verwendet wird. Ein unberechtigter Benutzer kann mit diesem Token unter Umständen erfolgreich eine Remote-Access-Verbindung aufbauen.

Wegen der Vielzahl verschiedener Passwörter und PINs können sich Benutzer diese oftmals nicht alle merken. Daher werden Passwörter immer wieder vergessen, was teilweise zu hohem Aufwand führt, um mit dem System weiterarbeiten zu können. Authentikationstoken können ebenso verloren werden. Bei sehr sicheren IT-Systemen kann der Verlust von Passwörtern oder Token sogar dazu führen, dass alle Benutzerdaten verloren sind.

Passwörter werden oft notiert, damit sie nicht vergessen werden. Dies ist solange kein Problem, wie sie sorgfältig, also vor unbefugtem Zugriff geschützt, aufbewahrt werden. Dies ist nicht immer der Fall. Ein klassisches Beispiel ist das Passwort unter der Tastatur oder auf einem Klebezettel am Bildschirm. Auch Authentikationstoken finden sich oft unter der Tastatur.

Ein anderer Trick, um Passwörter nicht zu vergessen, ist die "geeignete" Auswahl. Wenn Benutzer Passwörter selber auswählen können und nicht ausreichend für die Probleme hierbei sensibilisiert sind, werden in vielen Fällen Trivialpasswörter wie "4711" oder Namen von Freunden gewählt.

Beispiele:

- In einem Unternehmen wurde bei Stichproben festgestellt, dass viele Passwörter zu schlecht gewählt bzw. zu selten gewechselt wurden. Es wurde technisch erzwungen, dass die Passwörter monatlich gewechselt wurden und außerdem Zahlen oder Sonderzeichen enthalten mussten. Es stellte sich heraus, dass ein Administrator seine Passwörter wie folgt auswählte:
  Januar-2008, Februar-2008, Maerz-2008,

Diese Passwörter entsprachen zwar den Vorgaben, waren aber leicht zu erraten.

- In einer Behörde zeigte sich, dass einige der Benutzer, die ihre Büros zur Straßenseite hatten, dasselbe Passwort benutzten: den Namen des gegenüberliegenden Hotels, der in großen Leuchtbuchstaben die Aussicht dominierte.

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 5.1 Manipulation oder Zerstörung von Geräten oder Zubehör

Außentäter, aber auch Innentäter, können aus unterschiedlichen Beweggründen (Rache, Böswilligkeit, Frust) heraus versuchen, Geräte, Zubehör, Schriftstücke und andere Datenträger zu manipulieren oder zu zerstören. Die Angriffe können umso wirkungsvoller sein, je später sie entdeckt werden, je umfassender die Kenntnisse des Täters sind und je tief greifender die Folgen für einen Arbeitsvorgang sind. Die Manipulationen reichen von der unerlaubten Einsichtnahme in schützenswerte Daten bis hin zur Zerstörung von Datenträgern oder IT-Systemen. Erhebliche Ausfallzeiten können die Folge sein.

Beispiel:

- In einem Unternehmen nutzte ein Innentäter seine Kenntnis darüber, dass ein wichtiger Server empfindlich auf zu hohe Betriebstemperaturen reagiert, und blockierte die Lüftungsschlitze für den Netzteillüfter mit einem hinter dem Server versteckt aufgestellten Gegenstand. Zwei Tage später erlitt die Festplatte im Server einen temperaturbedingten Defekt und der Server fiel für mehrere Tage aus. Hinterher behauptete der Angreifer, dass es sich um ein Versehen gehandelt habe.
- Ein Mitarbeiter hatte sich über das wiederholte Abstürzen des Systems so stark geärgert, dass er seine Wut an seinem Arbeitsplatzrechner ausließ. Er trat mehrmals gegen den Rechner und beschädigte dabei die Festplatte so stark, dass sie unbrauchbar wurde. Die darauf gespeicherten Daten konnte die IT-Abteilung nur teilweise wieder durch ein Backup vom Vortag rekonstruieren.

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 5.16 Gefährdung bei Wartungs-/ Administrierungsarbeiten

Ein IT-System kann bei Wartungsarbeiten auf jedwede Weise manipuliert werden. Die Gefahr besteht in erster Linie darin, dass der Eigentümer oft nicht in der Lage ist, die vorgenommenen Modifikationen sofort zu erkennen und nachzuvollziehen. Darüber hinaus haben externe sowie interne Wartungstechniker üblicherweise auch vollen Zugriff auf alle auf den betreuten IT-Systemen gespeicherten Daten.

Externe Wartungstechniker könnten versuchen, sich unbefugt interne Informationen zu verschaffen oder sich Hintertüren einzubauen, um jederzeit Zugriff auf die IT-Systeme zu haben.

Zum eigenen Vorteil oder aus Gefälligkeit für Kollegen könnte bei Wartungs- oder Administrationsarbeiten durch internes Personal versucht werden, Berechtigungen (z. B. Auslandsberechtigung für Telefongespräche oder Zugriff auf Internetdienste) zu ändern oder weitere Leistungsmerkmale zu aktivieren. Dabei können durch Unkenntnis Systemabstürze verursacht werden oder weitere Sicherheitslücken durch Konfigurationsfehler eröffnet werden.

Das Wartungspersonal hat außerdem häufig vollen Zugriff auf die gespeicherten Daten auf den betreuten IT-Systemen (lesend und schreibend). Selbst wenn der Zugriff auf bestimmte Speicherbereiche oder bestimmte Zeiten eingeschränkt ist, lässt dies Spielraum, auf die gespeicherten Daten zuzugreifen und diese eventuell unbefugt weiterzugeben oder zu manipulieren.

Auch die eigenhändige Steuerung oder zeitweilige Deaktivierung von Regel- oder Alarmtechnik bei der Wartung birgt ein hohes Gefährdungspotential. Dies betrifft auch Gefahrenmeldeanlagen und Leitsysteme.

Beispiele:

- Eine kurzfristig eingestellte Aushilfe, die die Aufgabe hatte, nicht mehr genutzte Accounts zu sperren, nutzt ihre umfassende Berechtigung, um sich urheberrechtlich geschützte Software vom zentralen Applikationsserver für private Zwecke herunterzuladen. Um das Programm auch gleich an Freunde verteilen zu können, nutzt er dienstliche CD-ROM-/DVD-Brenner und Datenträger.
- Damit eine Kollegin auch während der Dienstzeit ihre privaten Homebanking-Transaktionen ausführen kann, wird ihr aus Gefälligkeit ein exklusiver Zugang zu ihrem Internet-Provider via ISDN zugänglich gemacht. Als sie sich zu Ostern einen Bildschirmschoner aus dem Internet herunterlädt, infiziert sie ihren PC mit einem Virus. Da der Rechner mit dem Hausnetz verbunden ist, verbreitet sich der Virus sehr schnell. Das Unternehmensnetz ist bis zur Behebung des Problems für mehrere Stunden nicht nutzbar.
- Einbruchmeldeanlagen haben in vielen Fällen einen integrierten Protokollierungsdrucker. Es kommt immer wieder vor, dass die Einbruchmeldeanlage zum Auswechseln des hierzu erforderlichen Druckerpapiers "vorsorglich" abgeschaltet wird. Beim anschließenden Wiedereinschalten besteht die Gefahr, dass das System unsachgemäß gestartet wird und sich dadurch Fehlfunktionen ergeben.

G 5.19 Missbrauch von Benutzerrechten

Eine missbräuchliche Nutzung liegt vor, wenn man vorsätzlich recht- oder unrechtmäßig erworbene Möglichkeiten ausnutzt, um dem System oder dessen Benutzern zu schaden.

In nicht wenigen Fällen verfügen Anwender aus systemtechnischen Gründen über höhere oder umfangreichere Zugriffsrechte, als sie für ihre Tätigkeit benötigen. Diese Rechte können zum Ausspähen von Daten verwendet werden, auch wenn Arbeitsanweisungen den Zugriff verbieten.

Beispiele:

- Auf vielen Unix-Systemen ist die Datei */etc/passwd* für jeden Benutzer lesbar, so dass er sich Informationen über dort eingetragene persönliche Daten verschaffen kann. Außerdem kann er mit Wörterbuchattacken (siehe G 5.18 *Systematisches Ausprobieren von Passwörtern*) versuchen, die verschlüsselten Passwörter zu erraten. Bei zu großzügiger Vergabe von Gruppenrechten, insbesondere bei den Systemgruppen wie z. B. *root, bin, adm, news* oder *daemon*, ist ein Missbrauch wie z. B. das Verändern oder Löschen fremder Dateien leicht möglich.
- Ein für die Verwaltung der Festplatten in z/OS-Systemen zuständiger Storage-Administrator konnte dank des Attributes *Operations*, das er für die Ausführung seiner Tätigkeit von der RACF-Administration erhalten hatte, Kundendateien einsehen. Er nutzte dieses Zugriffsrecht aus, um unerlaubt Kopien zu erstellen.

G 5.20 Missbrauch von Administratorrechten

Eine missbräuchliche Administration liegt vor, wenn man vorsätzlich recht- oder unrechtmäßig erworbene Super-User- (*root*-) Privilegien ausnutzt, um dem System oder dessen Benutzern zu schaden.

Beispiele:

- Da *root* auf Unix-Anlagen keinerlei Beschränkungen unterliegt, kann der Administrator unabhängig von Zugriffsrechten jede Datei lesen, verändern oder löschen. Außerdem kann er die Identität jedes Benutzers seines Systems annehmen, ohne dass dies von einem anderen Benutzer bemerkt wird, es ist ihm also z. B. möglich, unter fremden Namen Mails zu verschicken oder fremde Mails zu lesen und zu löschen.
- Es gibt verschiedene Möglichkeiten, missbräuchlich Super-User-Privilegien auszunutzen. Dazu gehören der Missbrauch von falsch administrierten Super-User-Dateien (Dateien mit Eigentümer *root* und gesetztem s-Bit) und des Befehls *su*.
- Die Gefährdung kann auch durch automatisches Mounten von austauschbaren Datenträgern entstehen: Sobald das Medium in das Laufwerk gelegt wird, wird es gemountet. Dann hat jeder Zugriff auf die dortigen Dateien. Mit sich auf dem gemounteten Laufwerk befindenden s-Bit-Programmen kann jeder Benutzer Super-User-Rechte erlangen.
- In Abhängigkeit von der Unix-Variante und der zugrunde liegenden Hardware kann bei Zugangsmöglichkeit zur Konsole der Monitor-Modus aktiviert oder in den Single-User-Modus gebootet werden. Das ermöglicht die Manipulation der Konfiguration.
- Durch Softwarefehler kann es möglich sein, dass eine Anwendung nur eine begrenzt große Menge an Daten verarbeiten kann. Werden dieser Anwendung übergroße Datenmengen oder Parameter übergeben, können Bereiche im Hauptspeicher mit fremdem Code überschrieben werden. Dadurch können Befehle mit den Rechten der Anwendung ausgeführt werden. Dies war unter anderem mit dem Befehl *eject* unter SunOS 5.5 möglich, der mit SetUID-Rechten ausgestattet ist, also bei der Ausführung Super-User-Rechte besitzt.

G 5.23 Schadprogramme

Ein Schadprogramm ist eine Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Zu den typischen Arten von Schadprogrammen gehören unter anderem Viren, Würmer und Trojanische Pferde. Schadprogramme werden meist heimlich, ohne Wissen und Einwilligung des Benutzers aktiv.

Schadprogramme bieten heutzutage einem Angreifer umfangreiche Kommunikations- und Steuerungsmöglichkeiten und besitzen eine Vielzahl von Funktionen. Unter anderem können Schadprogramme gezielt Passwörter ausforschen, Systeme fernsteuern, Schutzsoftware deaktivieren und Daten ausspionieren.

Als Schaden ist hier insbesondere der Verlust oder die Verfälschung von Informationen oder Anwendungen von größter Tragweite. Aber auch der Imageverlust und der finanzielle Schaden, der durch Schadprogramme entstehen kann, ist von großer Bedeutung.

Beispiele:

- In der Vergangenheit verbreitete sich das Schadprogramm W32/Bugbear auf zwei Wegen: Es suchte in lokalen Netzen nach Computern mit Freigaben, auf die schreibender Zugriff möglich war, und kopierte sich darauf. Zudem schickte es sich selbst als HTML-E-Mail an Empfänger im E-Mail-Adressbuch von befallenen Computern. Durch einen Fehler in der HTML-Routine bestimmter E-Mail-Programme wurde das Schadprogramm dort beim Öffnen der Nachricht ohne weiteres Zutun des Empfängers ausgeführt.
- Das Schadprogramm W32/Klez verbreitete sich in verschiedenen Varianten. Befallene Computer schickten den Virus an alle Empfänger im E-Mail-Adressbuch des Computers. Hatte dieser Virus einen Computer befallen, verhinderte er durch fortlaufende Manipulationen am Betriebssystem die Installation von Viren-Schutzprogrammen verbreiteter Hersteller und erschwerte so die Desinfektion der befallenen Computer erheblich.
- Auch gewisse Arten von eingebetteten Systemen können von Schadsoftware befallen werden. Prominentester Vertreter ist "Stuxnet", eine auf Prozesssteuerungssysteme spezialisierte Schadsoftware, welche dort unter anderem Prozessdaten manipuliert. Die Schadsoftware "Duqu" ist eine vermutete Weiterentwicklung von Stuxnet und soll vermutlich vor allem dazu dienen, Informationen zur Vorbereitung von Angriffen zu sammeln. Ebenfalls im Verdacht Industrieanlagen anzugreifen steht der Trojaner "Havex Remote Access Trojan". Er versucht Netzwerkverkehr mitzulesen und ein infiziertes System unter administrative Kontrolle zu bringen und fernzusteuern.

G 5.42 Social Engineering

Social Engineering ist eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch "Aushorchen" zu erlangen. Beim Social Engineering werden menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Dadurch können Mitarbeiter so manipuliert werden, dass sie unzulässig handeln. Ein typischer Fall von Angriffen mit Hilfe von Social Engineering ist das Manipulieren von Mitarbeitern per Telefonanruf, bei dem sich der Angreifer z. B. ausgibt als:

- Vorzimmerkraft, deren Vorgesetzter schnell noch etwas erledigen will, aber sein Passwort vergessen hat und es jetzt dringend braucht,
- Administrator, der wegen eines Systemfehlers anruft, da er zur Fehlerbehebung noch das Passwort des Benutzers benötigt,
- Telefonentstörer, der einige technische Details wissen will, z. B. unter welcher Rufnummer ein Modem angeschlossen ist und welche Einstellungen es hat,
- Externer, der gerne Herrn X sprechen möchte, der aber nicht erreichbar ist. Die Information, dass Herr X drei Tage abwesend ist, sagt ihm auch gleichzeitig, dass der Account von Herrn X in dieser Zeit nicht benutzt wird, also unbeobachtet ist.

Wenn kritische Rückfragen kommen, ist der Neugierige angeblich "nur eine Aushilfe" oder eine "wichtige" Persönlichkeit.

Eine weitere Strategie beim systematischen Social Engineering ist der Aufbau einer längeren Beziehung zum Opfer. Durch viele unwichtige Telefonate im Vorfeld kann der Angreifer Wissen sammeln und Vertrauen aufbauen, das er später ausnutzen kann.

Solche Angriffe können auch mehrstufig sein, indem in weiteren Schritten auf Wissen und Techniken aufgebaut wird, die in vorhergehenden Stufen erworben wurden.

Beispiel:

- Ein Angreifer hat leichteres Spiel, wenn er das Opfer dazu bringt, ihn von sich aus zu kontaktieren. Beispielsweise kann der Angreifer die Telefonanlage der Ziel-Organisation so manipulieren, dass alle Anrufe an den Administrator an ihn weitergeleitet werden. Dies kann zum Beispiel nach einem erfolgreichen Social-Engineering-Angriff auf den Telefontechniker oder einer erfolgreichen Kompromittierung einer unsicher konfigurierten Telefonanlage von außen geschehen. Gelingt es dem Angreifer dann beispielsweise, einen Denial-of-Service-Angriff durchzuführen, wird das Opfer des Angriffes den Administrator verständigen. Durch die Manipulation der Telefonanlage erreicht das Opfer aber nur den Angreifer. Dass dieser kein "echter" Administrator ist, wird aber normalerweise niemand im normalen Tagesgeschäft hinterfragen.

Viele Anwender wissen, dass sie Passwörter an niemanden weitergeben dürfen. Social Engineers wissen dies und müssen daher über andere Wege an das gewünschte Ziel gelangen. Beispiele hierfür sind:

- Ein Angreifer kann das Opfer bitten, ihm unbekannte Befehle oder Applikationen auszuführen, z. B. weil dies bei einem IT-Problem helfen soll. Dies kann eine versteckte Anweisung für eine Änderung von Zugriffsrechten sein. So kann der Angreifer an sensible Informationen gelangen.
- Viele Benutzer verwenden zwar starke Passwörter, aber dafür werden diese für mehrere Konten genutzt. Wenn ein Angreifer einen nützlichen Netzdienst (wie ein E-Mail-Adressensystem) betreibt, an dem die Anwender

sich authentisieren müssen, kann er an die gewünschten Passwörter und Logins gelangen. Viele Benutzer werden die Anmeldedaten, die sie für diesen Dienst benutzen, auch bei anderen Diensten verwenden.

Beim Social Engineering tritt der Angreifer nicht immer sichtbar auf, es gibt auch diverse Varianten, bei denen er im Hintergrund bleibt. Oft erfährt das Opfer niemals, dass es ausgenutzt wurde. Ist dies erfolgreich, muss der Angreifer nicht mit einer Strafverfolgung rechnen und besitzt außerdem eine Quelle, um später an weitere Informationen zu gelangen.

Die Nutzung von E-Mail und Internet-Diensten bietet viele Möglichkeiten, unter Vorspiegelung falscher Tatsachen an Informationen zu gelangen. Ist erst einmal das Vertrauen des Opfers gewonnen, ist es für den Angreifer leicht, dem Opfer eine E-Mail z. B. mit einem Trojanischen Pferd als Anhang zu übersenden. Da das Opfer den Angreifer kennt und als vertrauenswürdig einstuft, wird es meist auch die E-Mail und den Anhang als vertrauenswürdig einstufen und den Anhang öffnen.

Soziale Netzwerke

Soziale Netzwerke im Internet bieten eine gute Ausgangsbasis für Social Engineering. Über diese Plattformen können eine Vielzahl von Hintergrundinformationen über Personen gefunden werden. Die Informationen, die sie über ihr Profil preisgeben, können gesammelt und als Grundlage für die weitere Informationsbeschaffung genutzt werden.

G 5.80 Hoax

Ein Hoax (englisch für Streich, Trick, falscher Alarm) ist eine Nachricht, die eine Warnung vor neuen spektakulären Computer-Viren oder anderen IT-Problemen enthält und Panik verbreitet, aber nicht auf realen technischen Fakten basiert. Meist werden solche Nachrichten über E-Mails verbreitet. Beispielsweise wird dabei vor Computer-Viren gewarnt, die Hardware-Schäden verursachen können oder durch das bloße Öffnen einer E-Mail (nicht eines Attachments) zu Infektionen und Schäden führen können und die durch keine Antiviren-Software erkannt werden. Neben dieser Warnung wird darum gebeten, die Warnmeldung an Freunde und Bekannte weiterzuleiten. Noch wirksamer wird ein solcher Hoax, wenn als Absender eine gefälschte Adresse angegeben wird, wie zum Beispiel die eines namhaften Herstellers.

Ein solcher Hoax ist nicht zu verwechseln mit einem Computer-Virus, der tatsächlich Manipulationen am IT-System vornehmen kann. Vielmehr handelt es sich um eine irreführende Nachricht, die ohne Schaden gelöscht werden kann und sollte. Die einzigen Schäden, die ein Hoax herbeiführt, sind die Verunsicherung und Irritation der Empfänger und ggf. die Kosten an Zeit und Geld für den Weiterversand des Hoax.

Im Bereich des Mobilfunks gab es eine ganze Reihe solcher Hoax-Nachrichten, bei denen davor gewarnt wurde, dass an Mobiltelefonen die Eingabe bestimmter Tastenkombinationen oder die Wahl bestimmter Rufnummern dazu führen könnten, Gespräche abzuhören oder auf Kosten anderer zu telefonieren. Durch die Nennung bestimmter Mobiltelefon-Marken und einiger technischer Ausdrücke wird der Anschein von Seriosität erweckt. Solche Gerüchte halten sich hartnäckig und verunsichern die Benutzer.

Beispiel:

- Im Frühjahr 2000 kursierte folgende Falschmeldung per E-Mail (und teilweise sogar per Brief):
  "Wenn Sie eine Nachricht auf Ihr Handy erhalten, dass Sie unter der Nummer 0141-455xxx zurückrufen sollen, antworten Sie auf keinen Fall darauf. Ihre Rechnung steigt sonst ins Unermessliche.
  Diese Information wurde von der "Zentralstelle zur Unterdrückung von betrügerischen Machenschaften" (Office Central de Repression du Banditisme) herausgegeben."

G 5.104 Ausspähen von Informationen

Neben einer Vielzahl technisch komplexer Angriffe gibt es oft auch viel einfachere Methoden, um an wertvolle Informationen zu kommen. Da sensitive Daten oft nicht ausreichend geschützt werden, können diese oft auf optischem, akustischem oder elektronischen Weg ausgespäht werden.

Beispiele:

- Die meisten IT-Systeme sind durch Identifikations- und Authentisierungsmechanismen gegen eine unberechtigte Nutzung geschützt, z. B. in Form von Benutzer-ID- und Passwort-Prüfung. Wenn das Passwort allerdings unverschlüsselt über die Leitung geschickt wird, ist es einem Angreifer möglich, dieses auszulesen.
- Um mit einer ec- oder Kreditkarte Geld an einem Geldausgabeautomaten abheben zu können, muss die korrekte PIN eingegeben werden. Leider ist der Sichtschutz an diesen Geräten häufig unzureichend, so dass ein Angreifer einem Kunden bei der Eingabe der PIN ohne Mühe über die Schulter schauen kann. Wenn er ihm hinterher die Karte stiehlt, kann er damit das Konto plündern. Der Kunde hat anschließend außerdem das Problem, dass er nachweisen muss, nicht fahrlässig mit seiner PIN umgegangen zu sein, sie also beispielsweise nicht auf der Karte notiert hat.
- Um Zugriffsrechte auf einem Benutzer-PC zu erhalten oder diesen anderweitig zu manipulieren, kann ein Angreifer dem Benutzer ein Trojanisches Pferd schicken, das er als vorgeblich nützliches Programm einer E-Mail beigefügt hat. Erfahrungsgemäß öffnen Benutzer trotz aller Aufklärung sogar dann E-Mail-Anhänge, wenn diese nicht erwartet wurden oder merkwürdige Namen tragen. Neben unmittelbaren Schäden können über Trojanische Pferde Informationen nicht nur über den einzelnen Rechner, sondern auch über das lokale Netz ausspäht werden. Insbesondere verfolgen viele Trojanische Pferde das Ziel, Passwörter oder andere Zugangsdaten auszuspähen.
- In vielen Büros sind die Arbeitsplätze akustisch nicht gut gegeneinander abgeschirmt. Dadurch können Kollegen, aber auch Besucher unter Umständen Gespräche mitgehören und dabei Kenntnis von Informationen erlangen, die nicht für sie bestimmt oder sogar vertraulich sind.