STUDIENSKRIPT

Einführung in Datenschutz und IT-Sicherheit

DLBISIC01

INTERNATIONALE HOCHSCHULE

Studienskript

Einführung in Datenschutz und IT-Sicherheit

DLBISIC01

INTERNATIONALE HOCHSCHULE

Impressum

Herausgeber:
IU Internationale Hochschule GmbH
IU International University of Applied Sciences
Juri-Gagarin-Ring 152
D-99084 Erfurt

Postanschrift:
Albert-Proeller-Straße 15-19
D-86675 Buchdorf

media@iu.org
www.iu.de

DLBISIC01
Version Nr.: 002-2023-0206

Wissenschaftliche Leitung

Prof. Dr. Ralf Kneuper

Herr Kneuper unterrichtet seit 2016 im Bereich der Wirtschaftsinformatik und Informatik an der IU Internationale Hochschule und ist in erster Linie verantwortlich für Module mit den Schwerpunkten Softwareentwicklung, IT-Management, IT-Governance und IT-Sicherheit.

Herr Kneuper studierte Mathematik in Mainz, Manchester (UK) und Bonn und promovierte in Informatik an der Universität Manchester. Danach war er rund 15 Jahre bei einem Softwarehaus sowie im IT-Bereich eines Anwenderunternehmens verantwortlich für Aufgaben im Bereich des Qualitätsmanagements, der Softwareprozesse und der Prozessverbesserung sowie als Projektleiter tätig.

Seit 2004 ist er als freiberuflicher Berater tätig und unterstützt Unternehmen bei Aufgaben zu Softwarequalitätsmanagement, Prozessverbesserung und Datenschutz. Er ist Experte für Vorgehensmodelle sowie für Datenschutz und hat mehrere Fachbücher zu diesen Themen veröffentlicht. Daneben ist er Mitglied des Leitungsgremiums und war langjähriger Sprecher der Fachgruppe „Vorgehensmodelle für die betriebliche Anwendungsentwicklung“ der Gesellschaft für Informatik e. V. (GI).

Inhaltsverzeichnis

Einführung in Datenschutz und IT-Sicherheit

Einleitung

Einführung in Datenschutz und IT-Sicherheit

INTERNATIONALE HOCHSCHULE

Wegweiser durch das Studienskript

Herzlich willkommen!

Dieses Studienskript bildet die Grundlage Ihres Kurses. Ergänzend zum Studienskript stehen Ihnen weitere Medien aus unserer Online-Bibliothek sowie Videos zur Verfügung, mit deren Hilfe Sie sich Ihren individuellen Lern-Mix zusammenstellen können. Auf diese Weise können Sie sich den Stoff in Ihrem eigenen Tempo aneignen und dabei auf lerntypspezifische Anforderungen Rücksicht nehmen.

Die Inhalte sind nach didaktischen Kriterien in Lektionen aufgeteilt, wobei jede Lektion aus mehreren Lernzyklen besteht. Jeder Lernzyklus enthält jeweils nur einen neuen inhaltlichen Schwerpunkt. So können Sie neuen Lernstoff schnell und effektiv zu Ihrem bereits vorhandenen Wissen hinzufügen.

In der IU Learn App befinden sich am Ende eines jeden Lernzyklus die Interactive Quizzes. Mithilfe dieser Fragen können Sie eigenständig und ohne jeden Druck überprüfen, ob Sie die neuen Inhalte schon verinnerlicht haben.

Sobald Sie eine Lektion komplett bearbeitet haben, können Sie Ihr Wissen auf der Lernplattform unter Beweis stellen. Über automatisch auswertbare Fragen erhalten Sie ein direktes Feedback zu Ihren Lernfortschritten. Die Wissenskontrolle gilt als bestanden, wenn Sie mindestens 80 % der Fragen richtig beantwortet haben. Sollte das einmal nicht auf Anhieb klappen, können Sie die Tests beliebig oft wiederholen.

Wenn Sie die Wissenskontrolle für sämtliche Lektionen gemeistert haben, führen Sie bitte die abschließende Evaluierung des Kurses durch.

Die IU Internationale Hochschule ist bestrebt, in ihren Skripten eine gendersensible und inklusive Sprache zu verwenden. Wir möchten jedoch hervorheben, dass auch in den Skripten, in denen das generische Maskulinum verwendet wird, immer Frauen und Männer, Inter- und Trans-Personen gemeint sind sowie auch jene, die sich keinem Geschlecht zuordnen wollen oder können.

Übergeordnete Lernziele

Der Kurs **Einführung in Datenschutz und IT-Sicherheit** vermittelt Ihnen einen Überblick über die wichtigsten Grundlagen dieses Fachgebiets.

Nach erfolgreicher Teilnahme verstehen und beherrschen Sie die rechtlichen Rahmenbedingungen des Datenschutzes und der IT-Sicherheit sowie theoretische Modelle, operative Ziele und grundlegende Prinzipien des Datenschutzes und der IT-Sicherheit. Außerdem werden Sie wichtige Standards und Managementansätze der IT-Sicherheit kennenlernen. Zuletzt werden noch bewährte Schutz- und Sicherheitskonzepte für IT-Geräte und IT-Infrastrukturen vorgestellt.

Lektion 1

Begriffsbestimmungen und Hintergründe

LERNZIELE

Nach der Bearbeitung dieser Lektion werden Sie wissen, ...

- ... was Informationstechnik bedeutet und wie sie funktioniert.
- ... wie die Begriffe Sicherheit und Schutz zu verstehen sind.
- ... was Datenschutz bedeutet und worauf er begründet ist.
- ... was IT-Sicherheit bedeutet und wie sie zum Datenschutz steht.

1. Begriffsbestimmungen und Hintergründe

Einführung

Die Informationstechnik (IT) ist heute allgegenwärtig: im Haus, im Auto, am Arbeitsplatz etc. Auch Privatpersonen können sich heute ein Leben ohne E-Mail, Facebook und Google fast nicht mehr vorstellen. Für Verbände, Behörden und Unternehmen ist das Thema „Digitalisierung“ in einem globalen Umfeld ein Muss. Die Stichworte hier sind „Industrie 4.0“ und „Wirtschaft 4.0“.

Mit der überall zu beobachtenden Zunahme des Grades der Digitalisierung sind alle Nutzer immer mehr auf Informations- und Kommunikationssysteme angewiesen. Viele machen sich deshalb zu Recht Gedanken über die Sicherheit ihrer Daten und Geräte.

Und dann erfahren sie in den Medien, dass soziale Netzwerke Mitgliederdaten unerlaubt an Werbetreibende weitergeben, dass Hackern der Zugriff auf Millionen von Kundendaten gelingt und dass Krankenhäuser Patientendaten ungeschreddert im Altpapiercontainer entsorgen.

Spätestens seit den Enthüllungen von Edward Snowden, einem amerikanischen Whistleblower und ehemaligen CIA-Mitarbeiter, muss davon ausgegangen werden, dass Geheimdienste ungehindert Zugriff auf unsere Smartphones, Computer und E-Mails haben, dass sie zudem von den Herstellern eigene Hintertüren für verschlüsselte Geräte fordern und, dass sie sogar mit dem Verbot jeglicher verschlüsselter Kommunikation liebäugeln (Davies 2019).

Dies sind leider keine hypothetischen Szenarien – immer wieder gelangen Informationen über einen unerwünschten oder unerlaubten Zugriff auf persönliche oder geschäftliche Daten and die Öffentlichkeit. Und das, was bekannt wird, ist nach Einschätzung von Experten nur die Spitze des Eisbergs.

Dieser ungewollte Zugriff erfolgt aber nicht nur durch Kriminelle oder Geheimdienste. So steht beispielsweise seit den jüngsten Terroranschlägen für Bundesinnenminister Thomas de Maizière fest: „Datenschutz ist schön, aber in Krisenzeiten wie diesen hat Sicherheit Vorrang.“ Und in diesem Sinne verschärfte die Bundesregierung die anlasslose Speicherung von E-Mail und Telefon-Verbindungsdaten. Sie gab gar den sogenannten Bundestrojaner frei.

Was bedeutet aber nun eigentlich Datenschutz? Was meint der Begriff Sicherheit bei Informations- und Kommunikationssystemen? Welche Bedrohungen und Gefährdungen sind realistisch? Wie kann ich mich oder mein Unternehmen davor schützen?

Antworten zu diesen und vielen weiteren Fragen gibt das vorliegende Skript. Es führt in die wichtigsten Aspekte des Datenschutzes und der IT-Sicherheit ein, wobei praktische Mechanismen und konkrete Lösungen den Schwerpunkt bilden. Hinzu kommt eine einführende Behandlung rechtlicher Aspekte im nationalen und internationalen Kontext.

Abgerundet wird die Themenbehandlung durch die Erläuterung empfohlener Handlungsweisen zur Prävention, Erkennung und Korrektur von Datenschutz- und IT-Sicherheitspannen.

Mit den genannten Lernzielen vor Augen liegt der Fokus zunächst – soweit für das Verständnis des Folgenden erforderlich – auf dem Begriff „Informationstechnik“ und den wesentlichen technischen und organisatorischen Komponenten der Informationstechnik. Anschließend folgt eine kurze Diskussion der Begriffe Sicherheit und Schutz, die es dann gestattet, sowohl Datenschutz als auch IT-Sicherheit begrifflich und relativ zueinander einzuordnen.

1.1 Informationstechnik (IT) für die Unterstützung von privaten Aktivitäten und geschäftlichen Prozessen

Informationstechnik (IT) bezeichnet einen konkreten Einsatz von elektronischen Geräten für die Erhebung und Verwendung von Daten durch Menschen oder Maschinen. IT hat also stets einen bestimmten Anwendungsbereich in einer realen ökonomischen und/oder sozialen Umgebung. Dieser Anwendungsbereich kann eine Einzelperson, eine gesamte Firma oder auch nur ein einzelner Teil einer Firma (Beispiel: Abteilung) sein. Zudem benötigt IT stets (elektronische) Geräte und ist – in den meisten Fällen – in eine Arbeitsorganisation fest eingebunden. Diese Arbeitsorganisation orientiert sich dabei oft an Geschäftsprozessen. Im privaten Bereich dient die Informationstechnik persönlichen Aktivitäten wie E-Mail und Chat.

Daten sind in der Informationstechnik formalisierte Darstellungen von Sachverhalten, Konzepten, Vorstellungen und Anweisungen, die für die Übertragung, Speicherung und die Verarbeitung durch Menschen oder Maschinen geeignet sind. Eine Information ist dann die Bedeutung, die diesen aufgrund der den Daten zugrundeliegenden Vereinbarungen (Konventionen) beigelegt werden kann. Folglich ist die Bezeichnung Informationstechnik eigentlich etwas irreführend: Sie befasst sich gar nicht mit Informationen, sondern mit formalisierten Darstellungen von Informationen.

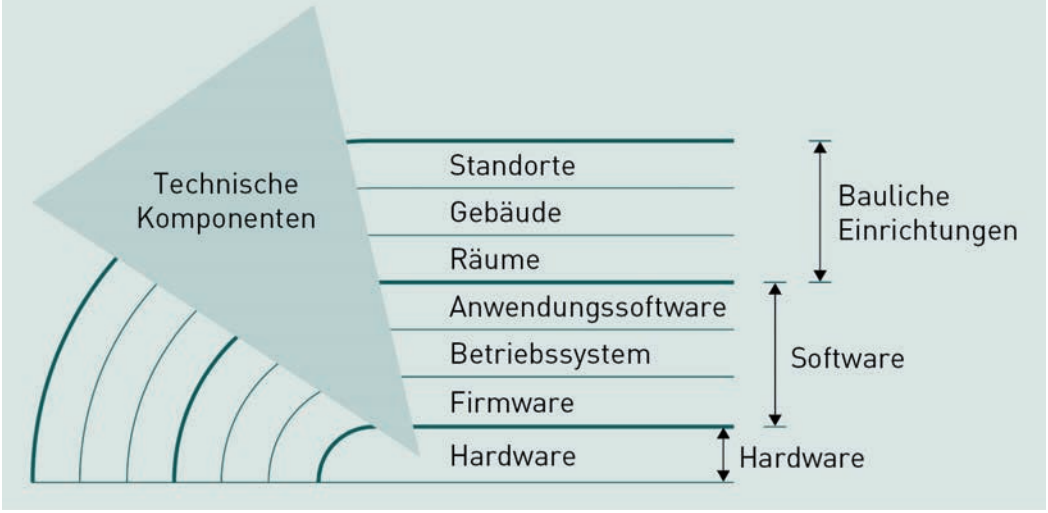
In diesem Zusammenhang ist auch noch der Begriff Signal wichtig. Signale sind Darstellungen von Daten durch charakteristische, räumliche und/oder zeitliche Veränderungen der Werte physikalischer Größen.

Die folgende Grafik zeigt das Zusammenspiel von Informationen, Daten und Signalen bei menschlichen Kommunikationsprozessen:

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) nennt eine konkrete Ausprägung der Informationstechnik einen „IT-Verbund". Dieser umfasst also alle technischen und alle organisatorischen Komponenten des konkreten Anwendungsbereiches, wobei für die technischen Komponenten auch der Begriff „IT-Infrastruktur" gebräuchlich ist.

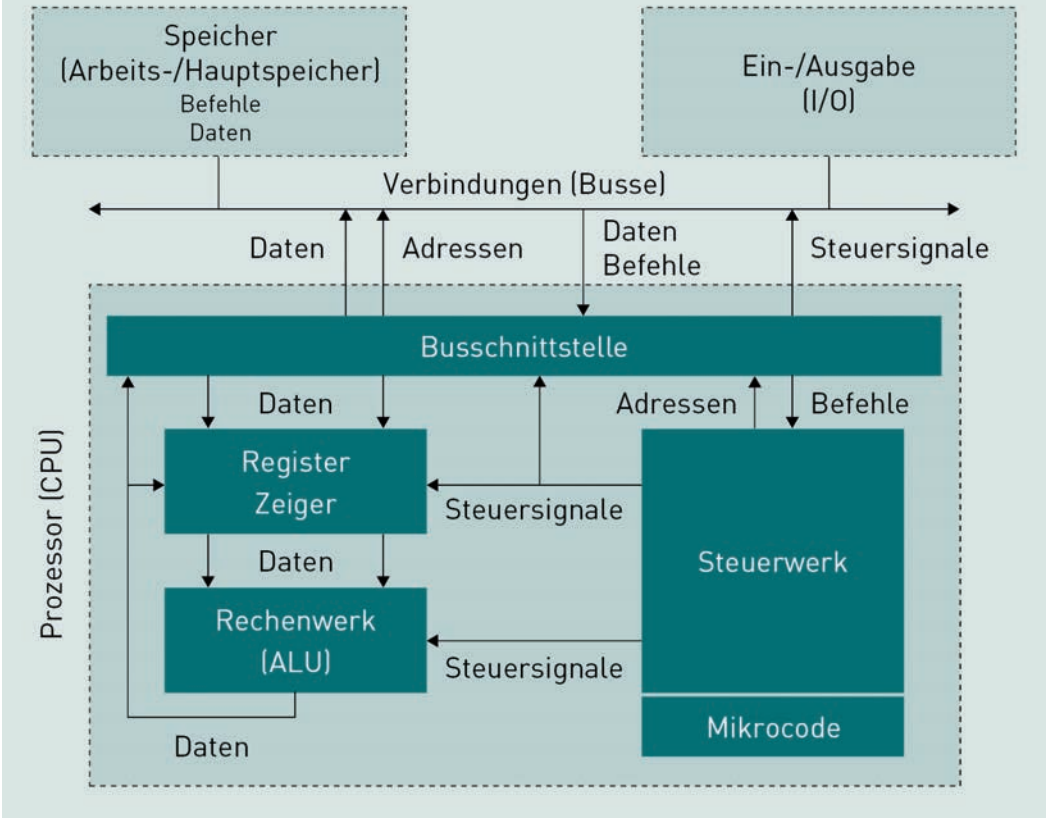
Wesentliche Bestandteile einer IT-Infrastruktur sind dabei Hardware, Software und bauliche Einrichtungen. Zur Hardware – den eigentlichen (elektronischen) Geräten – gehören die Rechengeräte (z. B. Computer, Tablets, Smartphones, Phablets [ein Kurzwort aus Phone und Tablet]), die Netzwerkgeräte (z. B. Switches, Router), Peripheriegeräte (z. B. Tastatur, Bildschirm, Drucker, Scanner, Kameras) sowie Geräte zum Betrieb der Hardware (z. B. unterbrechungsfreie Stromversorgungen). Zur Software gehört neben den anwendungsspezifischen Teilen (heute Applikationen oder kurz Apps genannt) vor allem die Systemsoftware (z. B. Firmware, Betriebssystem). Außerdem umfasst die technische IT-Infrastruktur die speziell für die Informationstechnik ausgestatteten Räumlichkeiten (z. B. Gebäude mit Zugangskontrolle, Räume mit spezieller Klimatechnik) und ihre Standorte.

Technische Komponenten eines IT-Verbundes



Hardware und Software der Rechengeräte entsprechen bis zum heutigen Tag dem bewährten Von-Neumann-Konzept für Rechnerarchitekturen:

Von-Neumann-Rechnerarchitektur



Dieses Konzept beschreibt die Architektur eines Universalrechners, der erst durch Software Funktionalität erlangt und in dem Programme und Daten binär, also allein mit den Zeichen 0 und 1, dargestellt und verwendet werden.

Hardware und Software kooperieren bei den heutigen Rechengeräten mit Windows-, Linux-, OS X-, iOS- und Android-Betriebssystemen prinzipiell wie folgt: Nach dem Einschalten ist für den sogenannten Boot-Vorgang die Firmware zuständig. Diese übernimmt die Grundfunktionen der Initialisierung bis zum Start des Betriebssystems. Die Firmware ist heutzutage eine UEFI-kompatible Firmware. Das **Unified-Extensible-Firmware-Interface (UEFI)** ermöglicht eine modulare Erweiterung der Firmware durch verschiedene Firmware-Module. Hierzu können zum Beispiel ein eingebettetes Netzwerkmodul für die Fernwartung, Module für Digital Rights Management (DRM), die BIOS-Emulation oder auch der Bootloader eines Betriebssystems gehören. UEFI beinhaltet zudem die Möglichkeit zur Nutzung eines Secure-Boot-Mechanismus, der den Start von Betriebssystemen auf ausdrücklich erlaubte Dateien beschränkt.

Unified-Extensible-Firmware-Interface
Das Unified-Extensible-Firmware-Interface (UEFI) bildet die Schnittstelle zwischen Firmware und Betriebssystem und ersetzt das Basic Input/Output System (BIOS).

Netzwerkgeräte unterstützen entweder lokale Netzwerke einer einheitlichen Technologie (Beispiele: LAN, WLAN, Bluetooth) oder Netzwerke von Netzwerken, die heute überwiegend auf der Protokollfamilie TCP/IP beruhen.

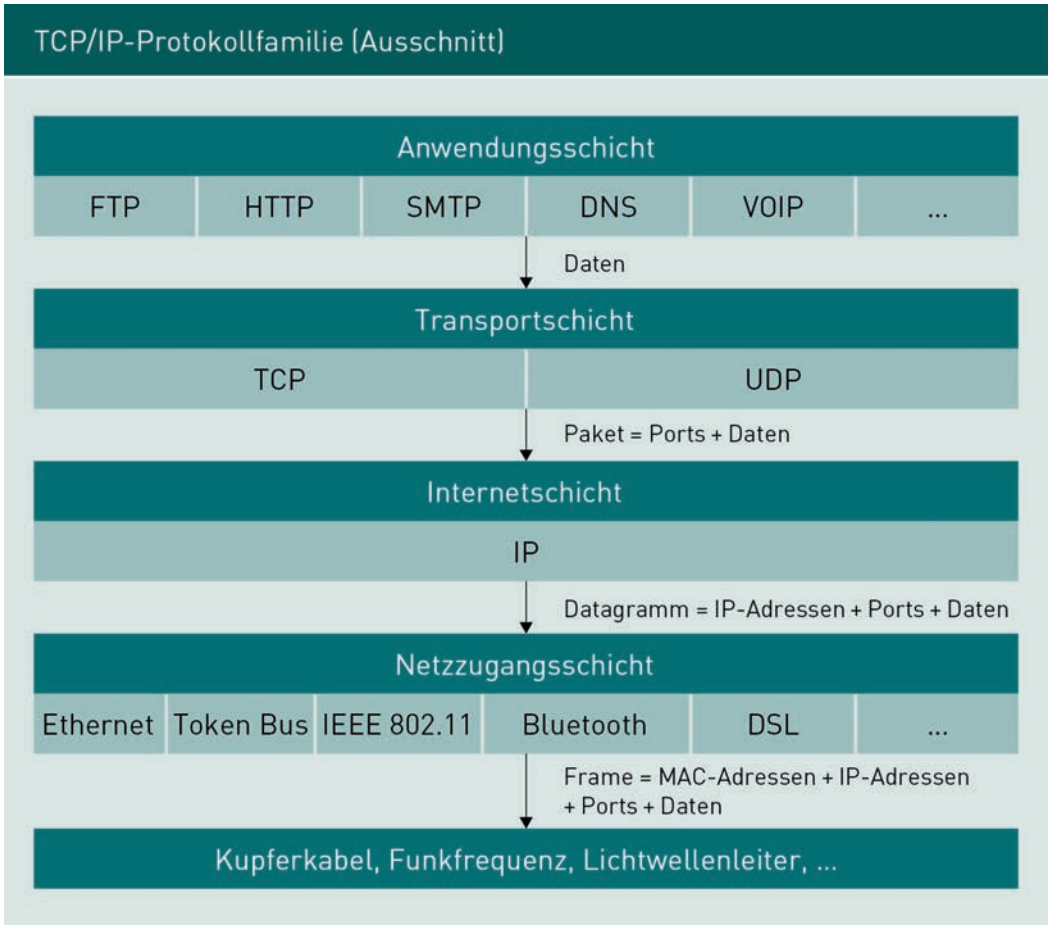
Ein LAN verwendet typisch die Ethernet-Technik nach IEEE 802.3, eine kabelgebundene Technik zur Übertragung von Daten. Sender und Empfänger werden hier durch eine sogenannte MAC-Adresse eindeutig identifiziert, die aus 48 Bit besteht und – typisch – hexadezimal angegeben wird: 00–80–41-ae-fd-7e. Die Adresse ff-ff-ff-ff-ff-ff ist hierbei für Übertragungen an alle Teilnehmer reserviert und wird Broadcast-Adresse genannt. Die zu übertragenden Daten werden in einen Rahmen (Frame) eingebettet, der auch die Sender- und die Empfänger-MAC-Adresse enthält, und an alle Teilnehmer übermittelt, wobei aber nur der explizit benannte Empfänger den Rahmen tatsächlich verwenden sollte. Die Übermittlung erfolgt nach dem First-Come-First-Served (FCFS)-Prinzip: Ein sendewilliger Teilnehmer prüft, ob das gemeinsame Übertragungsmedium frei ist, und sendet – gegebenenfalls nach einer zufälligen Verzögerung und erneuten Prüfung – seinen Rahmen. Während der Übermittlung achtet er darauf, ob andere Teilnehmer ebenfalls senden, und bricht gegebenenfalls seine Übertragung ab. Für die physikalische Übertragung der Rahmen an die Teilnehmer werden ein Hub oder ein Switch verwendet. Hubs stellen dabei mit einer sternförmigen Verkabelung mit Kabeln des CAT-Standards und RJ-45-Steckern bzw. -Buchsen lediglich die physikalisch einwandfreie Übertragung an alle angeschlossenen Geräte sicher. Switches leisten zusätzlich eine intelligente Auswertung der Sender- und Empfängeradressen, die dazu führt, dass nicht unbedingt alle Teilnehmer jeweils alle Rahmen empfangen.

Eine Randbemerkung: Die Abkürzung MAC wird im Bereich der IT-Sicherheit in mehreren verschiedenen Bedeutungen verwendet, die nicht verwechselt werden dürfen. Neben der hier beschriebenen MAC-Adresse, bei der MAC für „Media Access Control“ steht, gibt es auch noch die bei den Grundlagen der IT-Sicherheit beschriebene Zuweisung von Zugriffsrechten über „Mandatory Access Control“ sowie die sogenannten „Message Authentication Codes“, also schlüsselgesteuerte Hashfunktionen.

Ein WLAN entspricht funktional im einfachsten Fall einem LAN auf Ethernet-Basis, das aber kabellos mit Funkverbindungen operiert. Potenzielle Teilnehmer eines WLANs senden regelmäßig sogenannte Beacons, um ihre Präsenz anzuzeigen. Die Verbindung und der Datenaustausch erfolgen dann unmittelbar in einem Ad-Hoc-Netzwerk oder über einen Access Point (AP) in einem Infrastruktur-Netzwerk. IEEE 802.11 spezifiziert dazu nicht nur unterschiedliche Frequenzbereiche und Geschwindigkeiten, sondern auch Protokolle für die Auswahl des nächsten sendewilligen Teilnehmers und die Weitergabe von Teilnehmern an andere APs (Stichwort: Roaming).

Bluetooth war ursprünglich eine kabellose Übertragungstechnik für Sprache und Daten im Nahbereich (sogenannte Piconets). Mittlerweile bieten die aktuellen Versionen 4.x Leistungen und Reichweiten, die in Konkurrenz zu WLANs stehen.

TCP/IP ist eine Netzwerktechnik, die mithilfe einer übergeordneten Adressierungssystematik die Datenübertragung über die Grenzen von Netzwerken mit einheitlicher Übertragungstechnik, wie etwa Ethernet, gestattet. Die verschiedenen Protokolle dieser Technik, also die Vereinbarungen, die das Kommunikationsverhalten der Teilnehmer syntaktisch und semantisch festlegen, unterstützen dabei einander, um diese Leistung zu erbringen:



Jeder Teilnehmer erhält in TCP/IP-Netzwerken eine eindeutige und strukturierte Adresse, die IP-Adresse, die aus zwei Teilen besteht: einer Netzadresse und einer (lokalen) Teilnehmeradresse in diesem Netz. Eine IP-Adresse ist – jedenfalls in der hier nur betrachteten Version 4 – eine 32 Bit-Zahl, die meist – für eine bessere Lesbarkeit – durch vier durch Punkte getrennte Zahlen zwischen 0 und 255 geschrieben wird, z. B. 195.247.86.5. Die darin enthaltene Netzadresse wird oft durch eine angehängte „/n"-Notation ausgewiesen, wobei n die Anzahl der führenden Bits angibt, die diese Netzadresse enthalten. Bei der IP-Adresse 87.12.13.14/8 ist folglich die „87" die Netzadresse und „12.13.14" die (lokale) Teilnehmeradresse. Für 195.247.86.5/24 gilt entsprechend: Die Netzadresse ist „195.247.86" und die (lokale) Teilnehmeradresse „5". Da sich Menschen normalerweise Zahlen schlecht merken, können IP-Adressen durch einen Namen repräsentiert werden. So steht der Name www.iu.de beispielsweise für die IP-Adresse 78.137.97.49/8. Die erforderliche Umsetzung übernimmt der Domain Name Service (DNS). Die Zuordnungstabelle wird dabei in sogenannten DNS-Servern gespeichert und zum Abruf bereitgehalten. Bei jedem Verbindungswunsch mit einem nur namentlich bekannten Teilnehmer leistet zunächst der DNS die Umwandlung des Namens in die zugehörige IP-Adresse, mit der dann die Datenübermittlung über die Wegewahleinheiten (Router) erfolgt.

Diese Router sind die fundamentalen Bausteine der TCP/IP-Netzwerktechnik. Sie realisieren das Internet Protocol (IP), indem sie Dateneinheiten (Datagramme) auf Basis der Netzadressen von einem Sender zu einem Empfänger durch ein oder mehrere Zwischennetze hindurchbewegen. Dies geschieht verbindungslos: Router versuchen Datagramme in Richtung Empfänger zu bewegen, geben aber auf, wenn der Weg zum Empfänger sich als zu komplex erweist. In diesem Fall wird das Datagramm einfach vernichtet, ohne dass der Empfänger davon erfährt. Es wird lediglich ein – eher halbherziger – Versuch unternommen, den Sender hierüber zu informieren.

Router erwarten bei ihrer Arbeit von den beteiligten Netzen lediglich, dass sie ein Datenpaket innerhalb des jeweiligen Netzes übertragen können. Dies leisten beispielsweise alle Netze auf Ethernet Basis.

Transmission Control Protocol (TCP)
Das Transmission Control Protocol (TCP) ist ein zuverlässiges, verbindungsorientiertes Transportprotokoll für den Einsatz in paketvermittelten Netzwerken.

Das **Transmission Control Protocol (TCP)** dient innerhalb dieser Protokollfamilie der zuverlässigen und verbindungsorientierten Datenübertragung mit Routern. TCP verwendet dazu sender- und empfangsseitig sogenannte Ports, über die Sender und Empfänger für eine konkrete Datenübertragung fest gekoppelt werden. Vor der eigentlichen Datenübertragung wird bei TCP zwischen Sender und Empfänger vereinbart, über welche Ports die Übertragung stattfinden soll, und während der Datenübertragung wird dafür gesorgt, dass gegebenenfalls verloren gegangene Datagramme erneut auf den Weg gebracht werden.

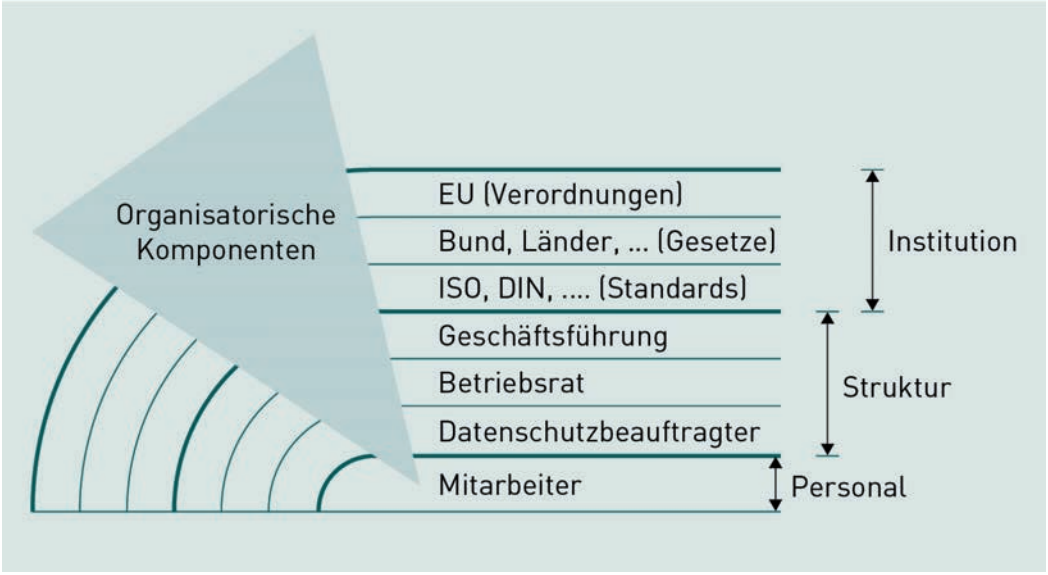
Da Router bei jedem Datagramm Zugriff auf die IP-Adressen und die gegebenenfalls verwendeten Ports haben, können sie zusätzliche Leistungen erbringen. Häufig fungieren sie beispielsweise auch als Firewall, d. h., sie unterbinden die Weiterleitung von Datagrammen auf Basis von Regeln, die Ports und/oder IP-Adressen als unzulässig spezifizieren. Der Begriff Firewall bezeichnet im Übrigen ursprünglich eine Trennwand, die ein Übergreifen von Feuer etwa im Auto verhindern soll.

Neben TCP gibt es auch noch das User Datagram Protocol (UDP) in der TCP/IP-Protokollfamilie, welches ähnlich wie TCP funktioniert, aber verbindungslos bleibt und somit ohne die Sicherstellung der Vollständigkeit einer Datenübertragung agiert. Es wird z. B. für Bild- und Tonübertragungen verwendet, da hier eine gewisse Anzahl von Fehlern wenig störend ist. Insbesondere die Internettelefonie, die oft Voice over IP (VoIP) genannt wird, nutzt dieses Protokoll. Dabei muss man aber zwischen den Datagrammen für den Verbindungsaufbau und -abbau und den Datagrammen mit den Sprachpaketen unterscheiden: Die Verbindungsdaten müssen natürlich fehlerfrei übertragen werden. Ohne eine definierte Verbindung ist ja schließlich keine Kommunikation möglich. Dagegen müssen die Sprachpakete möglichst schnell und verzögerungsfrei unterwegs sein. Daher nimmt man – bis zu einem gewissen Grade – eine unvollständige Übertragung in Kauf. Wenn mal ein Sprachpaket verloren geht, dann ist das nicht weiter schlimm.

Mittlerweile stützen sich derart viele Applikationen auf die TCP/IP-Protokollfamilie, dass es günstig ist, diese selbst innerhalb von Netzen mit einheitlicher Technologie zu verwenden, obgleich dies für den reinen Datenaustausch nicht notwendig wäre.

Die organisatorischen Komponenten eines IT-Verbundes erweitern die IT-Infrastruktur um institutionelle und personelle Aspekte. Institutionelle Aspekte sind sowohl Gesetze und Standards als auch organisatorische Strukturen, die Einfluss auf den konkreten IT-Verbund haben (Datenschutzbeauftragter, Betriebsrat, ...). Personelle Aspekte umfassen die Anzahl und die Qualifikationen der Mitarbeiter, die für die Planung, Wartung und den Betrieb des IT-Verbundes unerlässlich sind.

Organisatorische Komponenten eines IT-Verbundes

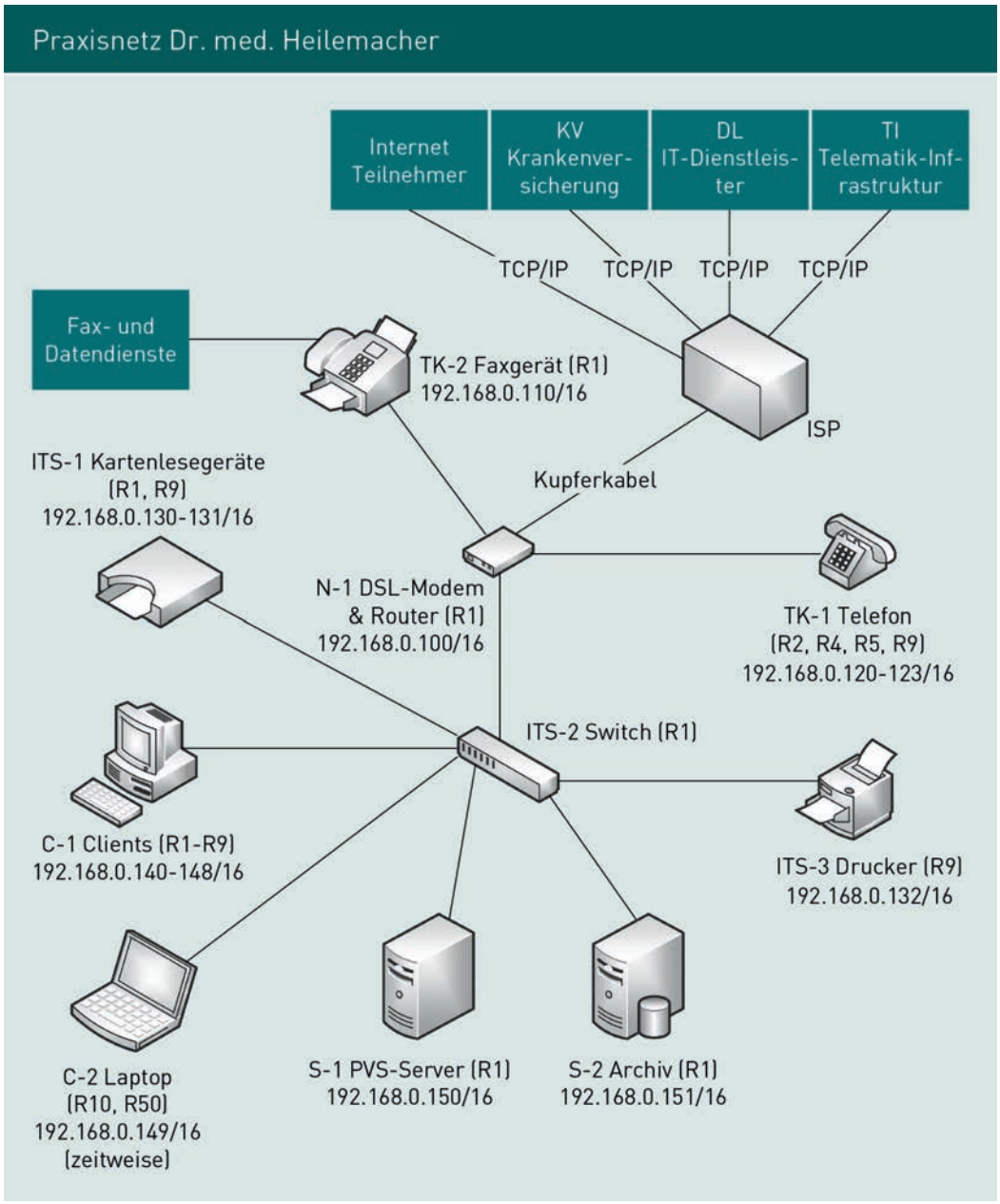


Zum besseren Verständnis dieser Terminologien soll zum Abschluss dieses Abschnitts der (ursprüngliche) IT-Verbund der Arztpraxis Dr. med. Heilemacher exemplarisch vorgestellt werden. Hier und auch später stützt sich die Darstellung auf fachliche Terminologien und Konzepte aus Kassenärztliche Bundesvereinigung (KBV 2016).

Kernstück der Informationstechnik dieser Arztpraxis ist das Praxisverwaltungssystem (PVS). Es bildet den gesamten Ablauf dieser Arztpraxis ab. Dies beginnt mit der Erhebung von Personalien und Versicherungsbedingungen und umfasst im Weiteren u. a.:

- Patientenakten, also Übersichten über Lebensdaten, Diagnosen und Behandlungen der Patienten, Dokumentationen von Messwerten und Therapieplänen sowie freie Notizen des Arztes;
- Zeit- und Aufgabenplanung des Arztes mit Agenda, Wartezimmer-Info, Aufgabenliste;
- Abholung von Laborresultaten über Internetverbindung und Meldung über eingetroffene neue Laborwerte;
- Erstellen und Übermitteln von Berichten, Bescheinigungen und Rezepten;
- Fakturierung und Abrechnungswesen nach deutscher Gesetzgebung;
- Statistiken über erbrachte Leistungen;
- Lagerverwaltung der Apotheke.

Der Arzt Dr. med. Heilemacher ist der Praxisinhaber (PI). Angestellt sind mehrere Sprechstundenhilfen und Assistenzärzte. Dieses Praxispersonal (PP) hat Zugriff auf das Praxisverwaltungssystem (PVS) und somit Zugriff auf Patientendaten. Es werden täglich automatisch Backups auf einem Archivrechner gespeichert. Manuell werden davon wöchentlich Kopien auf externen Datenträgern angelegt und außer Haus gebracht. Das Praxispersonal hat keinen Zugriff auf den Archivrechner oder die Sicherungskopien.



Die Abbildung veranschaulicht die (vereinfachte) IT-Infrastruktur der Praxis, mit zugehörigen IP-Adressen aus dem „privaten" Nummernbereich 192.168.0.0/16. Verschiedene Gerätetypen werden über den Switch (ITS-2) mithilfe der Ethernet-Technik (RJ-45, CAT-5E) verbunden. Die Kartenlesegeräte (ITS-1) werden als eigenständige Geräte direkt an das Netz angeschlossen, nicht an einen Computer. Der PVS-Server (S-1) baut über das DSL-Modem & Router (N-1) eine Verbindung zur TI auf (TI = Telematik-Infrastruktur für die elektronische Gesundheitskarte [eGK]). Der IT-Dienstleister (DL) schaltet sich für Fernwartungsaufgaben über das Internet auf S-1 auf.

Die nachfolgenden, tabellarischen Informationen detaillieren den IT-Verbund dieser Arztpraxis weiter:

Geräte der Arztpraxis					
Nr.	Beschreibung	Plattform	Anzahl	IP-Adresse	Räume
C-1	Arbeitsplatz-rechner	Windows 7	9	192.168.0.140–148/16	R1–R9
C-2	Laptop	Windows 7	1	192.168.0.149/16	R10, R50
ITS-1	Kartenterminal		2	192.168.0.130–131/16	R1, R9
ITS-2	Switch		1		R1
ITS-3	Drucker		1	192.168.0.132/16	R9
N-1	DSL-Modem & Router		1	192.168.0.100/16	R1
S-1	Server für Pra-xisverwal-tungssystem	Windows Server 2008	1	192.168.0.150/16	R1
S-2	Server für Archivierungs-system	Windows Server 2008	1	192.168.0.151/16	R1
TK-1	Telefone	Internet-Telefonie (VoIP)	4	192.168.0.120–123/16	R2, R4, R5, R9
TK-2	Faxgerät	Faxgerät	1	192.168.0.110/16	R1

Räume der Arztpraxis			
Nr.	Art	Gebäude	IT-Systeme/Datenträger
R1	Serverraum	Praxis	S-1, S-2, C-1, N-1, ITS-1, ITS-2,TK-2
R2	Büro Arzt	Praxis	C-1 , TK-1

Nr.	Art	Gebäude	IT-Systeme/Datenträger
R3–8	Behandlungsraum	Praxis	C-1, TK-1 (in R4 und R5)
R9	Rezeption	Praxis	C-1, ITS-1, ITS-3, TK-1
R10	Teeküche	Praxis	C-2
R50	Heimischer Büroraum	Praxisinhaber	C-2, externe Archiv-Datenträger
R99	Büroraum	IT-Dienstleister	Fernwartung von S-1

Institutionell sind für diese Arztpraxis vor allem zu nennen: die geltende Berufsordnung, die zuständige Ärztekammer, die Krankenversicherungen und die Kassenärztlichen Vereinigungen. Insbesondere muss das Praxispersonal über das, was ihm anvertraut oder bekannt geworden ist – auch über den Tod der Patientin bzw. des Patienten hinaus –, schweigen: Schriftliche Mitteilungen der Patientin bzw. des Patienten, ärztliche Aufzeichnungen, Röntgenaufnahmen und sonstige Untersuchungsbefunde dürfen Unbefugten niemals zugänglich sein.

1.2 Sicherheit und Schutz als Grundbedürfnisse

Der Mensch zeichnet sich gegenüber vielen anderen Lebewesen auch dadurch aus, dass er zunächst überhaupt ein bewusstes Konzept der Zukunft hat und dann noch versucht, zukünftige Umstände zu wissen und zu bestimmen. Nun sind aber viele zukünftige Umstände – jedenfalls nach dem heutigen Stand der Wissenschaft – nicht bestimmt und nicht gewiss. Jeder hat die Diskrepanz zwischen Erwartung und Realität bereits – manchmal schmerzlich – kennengelernt.

Man bezeichnet das Ausmaß der Bestimmtheit und Gewissheit von zukünftigen Umständen als Sicherheit. Sicherheit ist dementsprechend eine Erwartungssicherheit. Sie ist auf die Zukunft ausgerichtet und ist in ihrem Ausmaß an den jeweiligen Beobachter gebunden. Sie muss als relative Eindeutigkeit im Hinblick auf die Zukunft verstanden werden und misst die mehr oder weniger eindeutige Kenntnis zukünftiger Ereignisse.

Daher ist eine große Sicherheit schon seit Urzeiten ein grundlegendes Bedürfnis der Menschen. Sie waren und sind nämlich zahllosen Unsicherheiten ausgesetzt, mit denen sie sich auseinandersetzen müssen. Diese Auseinandersetzung ist für jeden Menschen

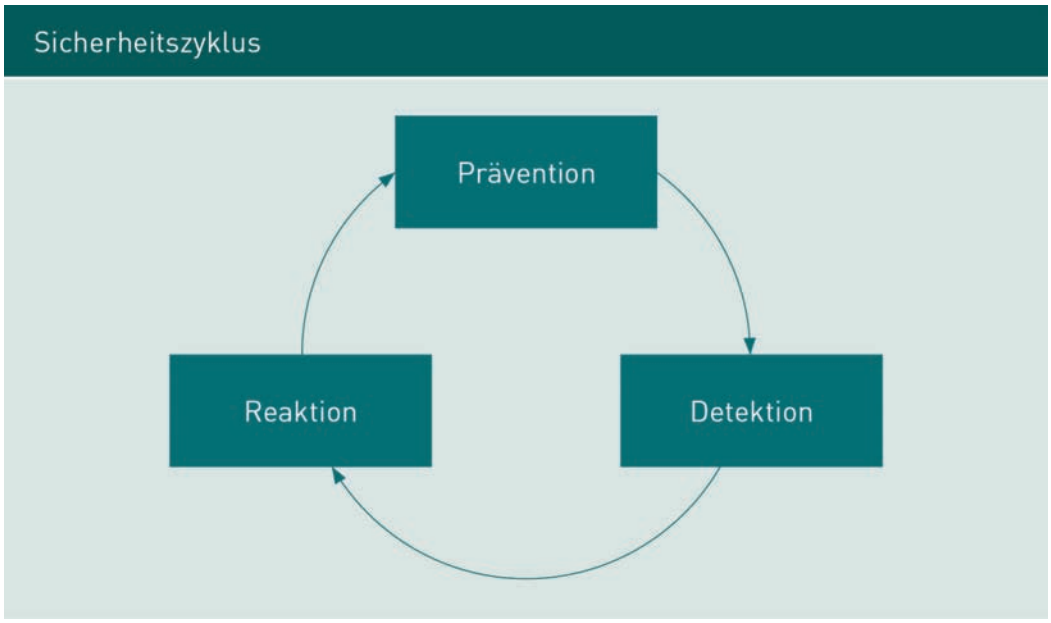
notgedrungen eine Kombination aus Intuition und Wahrscheinlichkeitsrechnung. Zu dieser Auseinandersetzung gehört also auch, dass man gelegentlich ein Risiko eingehen muss.

Sicherheit ist folglich ein (relativer) Zustand der zukünftigen Störungs- und Gefahrenfreiheit, der stets nur für einen bestimmten zeitlichen Horizont, eine bestimmte Umgebung und unter bestimmten Bedingungen gegeben ist. Im Extremfall können sämtliche Vorkehrungen zur Erhöhung der Sicherheit zu Fall gebracht werden durch Ereignisse, die sich nicht beeinflussen oder voraussehen lassen (beispielsweise ein Blitzeinschlag). Sicherheit bedeutet daher nicht, dass Störungen und Gefahren vollständig ausgeschlossen sind, sondern nur, dass sie hinreichend (beispielsweise im Vergleich zur Wahrscheinlichkeit eines Lottogewinns) unwahrscheinlich sind.

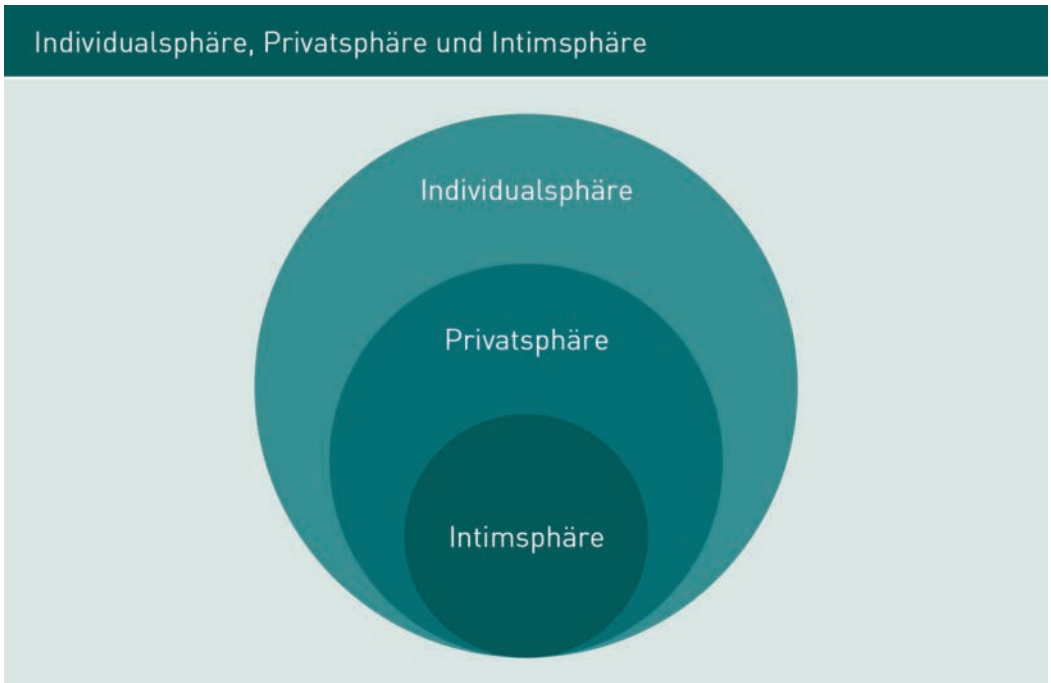
Bei Sicherheit kann es also nicht um die Herstellung von absoluter Sicherheit gehen, sondern immer nur um den Umgang mit den verbleibenden, zukünftigen Störungen und Gefahren.

Anders als im englischen Sprachraum wird im Deutschen normalerweise nicht zwischen den beiden Sicherheitsaspekten Security (Sicherheit gegen Einwirkungen [„Immunität“]) und Safety (Sicherheit der Auswirkungen [„Isolation“]) unterschieden, beide Begriffe werden stattdessen allgemein unter Sicherheit zusammengefasst. Paradoxerweise ist demnach im Deutschen Sicherheit nicht gleich Sicherheit (Security != Safety). Es ist aber unmittelbar einsichtig, dass in vielen praktisch relevanten Fällen Security Voraussetzung für Safety ist und damit einen gewissen Vorrang genießt. Daher geht es bei Sicherheitsüberlegungen – und auch hier – meist eher um Aspekte der Security.

Alles was ausdrücklich der Erhöhung der Sicherheit dient, wird als Schutz bezeichnet. Schutz fördert demnach gezielt die Bestimmtheit und Gewissheit zukünftiger Umstände. Ein Schutz bietet also Sicherheit und fördert das Sichersein. Die entsprechenden Maßnahmen sind definitionsgemäß präventiv, also in die Zukunft gerichtet: Störungen und Gefahren der Sicherheit sollen durch gewisse Vorkehrungen verhindert werden. Präventive Schutzmaßnahmen sind dabei psychologisch, technisch oder organisatorisch. Nicht selten versagt aber die Prävention. Dann ist es zwingend angezeigt, die Detektion mit einer anschließenden Reaktion zu forcieren. Die Aufgabe der Detektion ist es schnell zu erkennen, wenn Angriffe stattfinden, um darauf reagieren und die Angriffe abwehren zu können. Anschließend erfolgt die Reaktion, also neben der Korrektur auch die Sanktionierung von Fehlentwicklungen. Sanktionierungen sind oft im Straf- oder Zivilrecht begründet.



Zur Verbesserung des Schutzes haben sich Menschen schon seit Langem zu sozialen und politischen Gemeinschaften zusammengeschlossen. Sie erwarten für sich einen umfassenden, garantierten Schutz durch diese Gemeinschaften und dabei insbesondere den Schutz der Person. Hierbei wird bezüglich des Schutzanspruches oft hinsichtlich unterschiedlicher persönlicher Schutzbereiche differenziert:



Die **Intimsphäre** soll möglichst absolut durch die Gemeinschaft geschützt werden. Zu diesem intimen Lebensbereich einer Person gehört u. a. die Sexualität, Krankheiten, Gefühle und die Gedankenwelt.

Die **Privatsphäre** ist etwas weiter gefasst und betrifft im Wesentlichen den gesamten häuslichen Bereich sowie die Lebensbereiche, die nur nahestehenden Personen zugänglich sein sollen. Hierzu zählen aber auch die Interaktion mit Beziehungspartnern und Lebensgefährten in öffentlichen Bereichen. Große Sicherheit mit nur sehr restriktiven Ausnahmen soll hier die Gemeinschaft leisten.

Am weitesten gefasst ist die **Individualsphäre**. Dies ist der Bereich des persönlichen Lebens, der frei beobachtbar stattfindet und so ohnehin für jeden zugänglich ist. Aber auch dies soll kein sicherheitsfreier Raum sein. Zumindest soll hier Sicherheit der Beziehungen zur Umwelt, einschließlich des öffentlichen und beruflichen Wirkens einer Person, durch die Gemeinschaft hergestellt werden.

Das allgemeine Persönlichkeitsrecht, das im Grundgesetz verankert ist, ist der grundlegende Rechtsanspruch für die Sicherheit in diesen drei Sphären. Es ist das absolute und umfassende Recht auf Achtung und Entfaltung der Persönlichkeit.

1.3 Datenschutz als Persönlichkeitsrecht

Nach den bisherigen Ausführungen müsste der Begriff Datenschutz eigentlich all das bezeichnen, was dem Sichersein von formalisierten Informationsdarstellungen dient. Dies ist (leider) nicht so. Wir verstehen in Deutschland unter Datenschutz das, was treffender mit **„Verdatungsschutz“** bezeichnet werden kann. Wie ist es dazu gekommen?

Verdatungsschutz
Der Begriff „Datenschutz“ hat sich zwar durchgesetzt, ist aber unglücklich, da es nicht um den Schutz der Daten, sondern um den Schutz des Menschen geht, weshalb „Verdatungsschutz“ richtiger wäre.

Ab Beginn der 1960er-Jahre wuchs das Bewusstsein, dass die unbefugte Weitergabe von persönlichen Daten zu einer konkreten Beeinträchtigung der betroffenen Person führen kann. So heißt es im sogenannten Mikrozensus-Beschluss des Bundesverfassungsgerichts (BVerfG) vom 16.07.1969: „Der Staat darf durch keine Maßnahmen, auch nicht durch ein Gesetz, die Würde des Menschen verletzen oder sonst über die in Art. 2 Abs. 1 GG gezogenen Schranken hinaus die Freiheit der Person in ihrem Wesensgehalt antasten. Mit der Menschenwürde wäre nicht zu vereinbaren, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch nur in der Anonymität einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist.“

In den 1980er-Jahren wurde dann in der Bundesrepublik Deutschland eine Volkszählung geplant, die umfangreiche Daten über die Bevölkerung erfassen sollte. Dies löste bei manchen Unbehagen aus und führte in der Folge zu mehreren Verfassungsbeschwerden. Das BVerfG stellte zu diesen Verfassungsbeschwerden in seinem Urteil vom 15.12.1983 u. a. Folgendes fest:

- Jeder Bürger hat ein Recht, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“. Dieses Recht ergibt sich aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG und wird vom BVerfG als „Recht auf informationelle Selbstbestimmung“ bezeichnet.
- Es gibt „unter den Bedingungen der automatisierten Datenverarbeitung kein ‚belangloses‘ Datum“: Alle persönlichen Daten stehen unter dem Schutz des Grundgesetzes, losgelöst davon, ob sie eine sensible Information repräsentieren oder nicht.
- Die Bürger müssen wissen, „wer was wann und bei welcher Gelegenheit über sie weiß“. Es bestehen insofern weitgehende Aufklärungspflichten der Stelle, die persönliche Daten erhebt oder verwendet. Gleichzeitig gilt das Prinzip des Vorrangs der Selbstauskunft (Grundsatz der Direkterhebung): Wenn möglich, soll der Bürger selbst um Mitteilung seiner Daten gebeten werden, bevor von Dritten Auskünfte über eine Person eingeholt werden.
- Einschränkungen des Rechts auf informationelle Selbstbestimmung bedürfen einer ausdrücklichen gesetzlichen Grundlage. Diese Grundlage muss die wesentlichen Bedingungen für die Zulässigkeit der Datenerhebung und -verwendung so konkret wie möglich definieren. Ferner muss sie Aufklärungs-, Auskunfts- und Löschungspflichten vorsehen.
- Die Erhebung und Verwendung persönlicher Daten unterliegen einer strengen Zweckbindung: Sie dürfen nur für diesen konkreten, bestimmten Zweck erhoben und verwendet werden; jede Sammlung persönlicher Daten „auf Vorrat zu unbestimmten Zwecken“ ist unzulässig.

Diese Entscheidung wird allgemein als die eigentliche Geburtsstunde des Datenschutzes in Deutschland verstanden, obgleich beispielsweise das Bundesland Hessen und auch der Bund schon in den 1970er-Jahren in dieser Sache aktiv wurden. Allerdings mussten die früheren Ansätze für eine rechtliche Regelung des Datenschutzes nicht ein Grundrecht mit Verfassungsrang, nämlich das Recht auf informationelle Selbstbestimmung, berücksichtigen.

Datenschutz wurde in Deutschland seinerzeit formal definiert als der Schutz natürlicher Personen bei der Erhebung und Verwendung von Daten, die sie betreffen. Und diese Definition ist auch heute noch gültig.

In der Schweiz ist Datenschutz beispielsweise nicht auf natürliche Personen, also lebende Menschen als Rechtssubjekte, beschränkt, sondern bezieht auch juristische Personen in den Schutz mit ein. Das galt in der Vergangenheit auch in Österreich und Dänemark, gilt aber seit der Einführung der europäischen Datenschutz-Grundverordnung (DSGVO) nur noch mit Einschränkungen.

Daten, die eine natürliche Person betreffen, werden als personenbezogene Daten bezeichnet. Dies sind alle Daten, die eindeutig einer bestimmten natürlichen Person zugeordnet sind oder für die diese Zuordnung zumindest mittelbar erfolgen kann. Beispiele sind Namen, Kennnummern, Standortdaten, Online-Kennungen und Merkmale, die die physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Aspekte einer natürlichen Person betreffen.

Die durch personenbezogene Daten bestimmte oder bestimmbare Person wird als Betroffener bezeichnet. Die Institution, die personenbezogene Daten erhebt oder verwendet, heißt Verantwortlicher.

In seinem Urteil vom 27.02.2008 hat das BVerfG übrigens eine weitere, wichtige Entscheidung zum Persönlichkeitsrecht mit Auswirkungen auf die Informationstechnik veröffentlicht, die sich unmittelbar auf den Schutz von Daten im eigentlichen Sinne und nur mittelbar auf den Datenschutz auswirkt: „Das allgemeine Persönlichkeitsrecht umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme."

Dies bedeutet u. a., dass jeder heimliche Zugriff auf ein informationstechnisches System, das „einen Einblick in wesentliche Teile der Lebensgestaltung einer Person" gestattet, nur in ganz wenigen Ausnahmefällen statthaft ist. Zu diesen informationstechnischen Systemen zählen – laut BVerfG – ausdrücklich nicht nur Smartphones, sondern auch PCs, Rechnernetze und – nicht überraschend – das gesamte Internet. Daten sind nach dieser Entscheidung immer dann ausdrücklich durch die Verfassung geschützt, wenn sie nicht nur einen punktuellen Bezug zu einem bestimmten Lebensbereich eines Betroffenen haben.

Damit ist man aber bereits beim Begriff der IT-Sicherheit angelangt.

1.4 IT-Sicherheit als Qualitätsmerkmal von IT-Verbünden

Bei einem IT-Verbund bezeichnet Sicherheit – entsprechend den früheren Ausführungen – das (zukünftige) Ausmaß des voraussichtlich störungsfreien und gefahrenfreien Betriebs.

Dieser störungsfreie Betrieb wird zunächst bestimmt durch die Qualität der eingesetzten Hardware: Bauteile bzw. Bestandteile dürfen nicht durch Überbelastung oder Materialversagen ihre Funktionsfähigkeit verlieren. Bei IT-Geräten erlangt aber auch die Software zunehmende Bedeutung für den störungsfreien Betrieb. Um Software für sicherheitskritische IT-Verbünde zu entwickeln, muss oft ein hoher Aufwand für die Sicherstellung der (relativen) Fehlerfreiheit betrieben werden. Im Allgemeinen müssen dazu strenge Maßstäbe an den Softwareentwicklungsprozess gelegt werden. Für verschiedene Industrien, wie z. B. die Luftfahrtindustrie, sind daher die Anforderungen an sicherheitsorientierte Softwareentwicklungsprozesse in Normen festgelegt. Diese Normen betreffen vor allem den Safety-Aspekt der Sicherheit.

Das Ausmaß des störungsfreien Betriebs eines IT-Verbundes wird Verfügbarkeit genannt. Tritt bei einer möglichen Störung keine Gefährdung auf, so spricht man auch einfach nur von Zuverlässigkeit.

Sicherheit eines IT-Verbundes ist aber auch das Ausmaß des gefahrenfreien Betriebs. Eine Gefahr ist in der Informationstechnik jeder Sachverhalt, der negative materielle oder immaterielle Auswirkungen hat.

Es hat sich herausgestellt, dass wesentliche Anteile des Ausmaßes des gefahrenfreien Betriebs in der Informationstechnik gut durch die Begriffe Vertraulichkeit und Integrität (Unverfälschtheit) erfasst werden. In der Literatur werden in diesem Zusammenhang auch Begriffe wie die Authentizität von Daten und die Nicht-Abstreitbarkeit von Inhalten herangezogen. Da diese aber als Spezialfälle der Integrität angesehen werden können, sind sie hier nicht gesondert aufgeführt.

Mit diesen Vorbereitungen kann man IT-Sicherheit nun pragmatisch wie folgt definieren: IT-Sicherheit eines konkreten IT-Verbundes ist das Vorhandensein von Vertraulichkeit, Integrität und Verfügbarkeit in einem geplanten Ausmaß.

Dabei bedeuten diese sogenannten **Schutzziele** konkret:

Schutzziele
Das sind Aussagen über Sicherheitsniveaus, welche erreicht werden sollen.

- **Vertraulichkeit:** „Daten werden nur Befugten bekannt; Funktionen werden nur von Befugten genutzt."
- **Integrität:** „Daten sind richtig, vollständig und aktuell oder aber dies ist erkennbar nicht der Fall; Funktionen sind verlässlich und vertrauenswürdig oder aber es ist erkennbar, wenn dies nicht der Fall ist."
- **Verfügbarkeit:** „Daten und Funktionen sind dort und dann zugänglich, wo und wann sie von Befugten gebraucht werden."

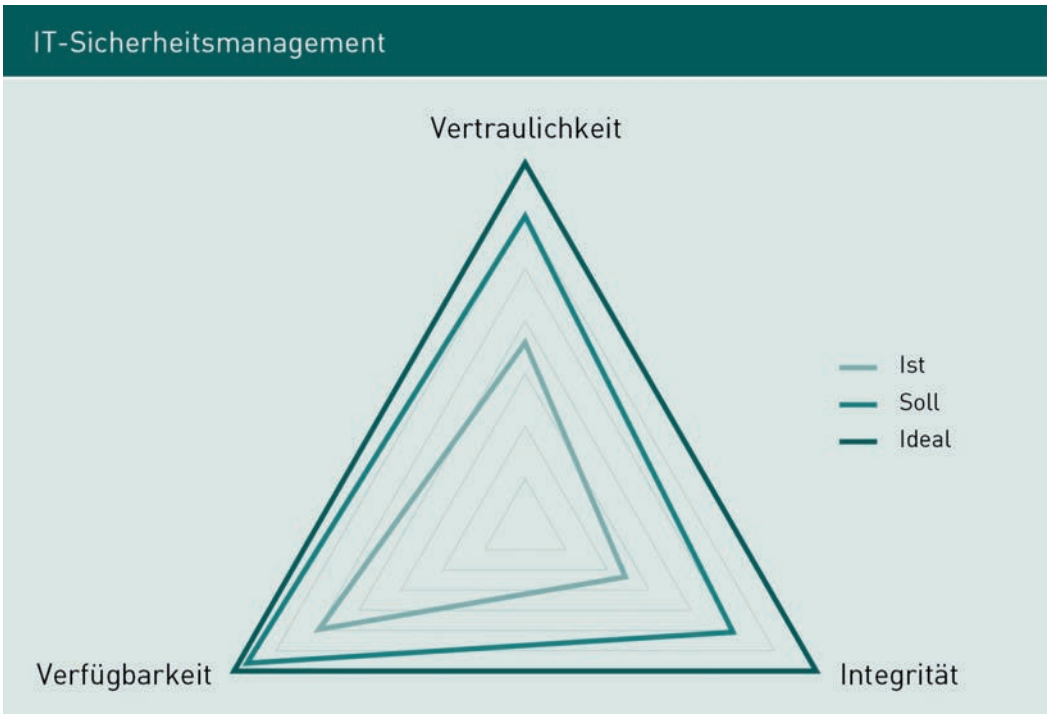
Das erforderliche Ausmaß der Vertraulichkeit wird in der IT-Sicherheit ermittelt durch Fragen wie „Kann durch das Bekanntwerden von Daten dem Unternehmen oder Dritten ein Schaden entstehen?".

Für die Bestimmung des erforderlichen Ausmaßes der Integrität müssen Fragen wie „Kann in einem Geschäftsprozess durch manipulierte Daten ein Schaden entstehen? Können durch verfälschte Daten Vertrauensverluste in das Unternehmen entstehen? Können verfälschte Daten Fehlentscheidungen hervorrufen?" beantwortet werden.

Verfügbarkeitsbetrachtungen erfordern die Beantwortung von Fragen wie „Kann ein Geschäftsprozess nicht durchgeführt werden, da notwendige Daten nicht vorhanden sind? Schreiben Gesetze die Verfügbarkeit von Daten vor? Können Personen beeinträchtigt werden, wenn Daten nicht zur Verfügung stehen?".

Es ist zu beachten, dass die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit nicht unabhängig voneinander sind. So kann beispielsweise eine Verbesserung der Vertraulichkeit durch technische Maßnahmen sehr wohl die Verfügbarkeit beeinträchtigen.

Unter IT-Sicherheitsmanagement wird der Prozess zur Gewährleistung der IT-Sicherheit eines IT-Verbundes innerhalb einer Unternehmung oder Organisation verstanden. Typisch werden in diesem Prozess laufend die Ist-Werte den Soll-Werten gegenübergestellt und es werden – darauf basierend – Maßnahmen identifiziert und implementiert, die eine Annäherung an den Soll-Zustand wahrscheinlich machen. Die nachfolgende Grafik illustriert dies:



1.5 Abgrenzung Datenschutz und IT-Sicherheit

Es ist nun auch klar, wie die Begriffe Datenschutz und IT-Sicherheit gegeneinander abzugrenzen sind: Beim Datenschutz geht es vorrangig um den Schutz der (natürlichen) Personen. Datenschutz soll ja das Grundrecht auf informationelle Selbstbestimmung garantieren und so jede (natürliche) Person vor dem Missbrauch der sie betreffenden Daten schützen. Dies beginnt schon mit der Frage, ob die entsprechenden Daten überhaupt erhoben oder verwendet werden dürfen. Dabei ist ein möglicher Einsatz von IT nur nachrangig von Bedeutung.

IT-Sicherheit befasst sich dagegen mit dem Schutz aller Daten eines konkreten IT-Verbundes, unabhängig davon, ob diese Daten eine (natürliche) Person betreffen oder nicht. IT-Sicherheit soll alle Daten eines IT-Verbundes vor unberechtigter Änderung und unbefugter Kenntnisnahme schützen. Bei IT-Sicherheit geht es also nicht um die Frage, ob irgendwelche Daten überhaupt erhoben oder verwendet werden dürfen, sondern es geht um die Frage, was getan werden muss, um die Erhebung und Verwendung aller Daten eines konkreten IT-Verbundes möglichst sicher zu gestalten. Dies bedeutet notwendigerweise, dass ein Hauptaugenmerk auf die Zuverlässigkeit des konkreten IT-Verbundes zu legen ist.

In der Praxis gibt es jedoch oft Überschneidungen von Datenschutz und IT-Sicherheit. Der Schutz der Patientendaten in der Arztpraxis zum Beispiel ist Anliegen des Datenschutzes und der IT-Sicherheit. Die persönlichen Daten von Patienten unterliegen den gesetzlichen Regelungen des Datenschutzes. Natürlich hat der Praxisinhaber aber auch

schon aufgrund seiner Berufsordnung ein starkes Eigeninteresse daran, dass die Patientendaten nicht öffentlich werden. Und so können oft mit denselben Maßnahmen sowohl Anforderungen des Datenschutzes als auch der IT-Sicherheit erfüllt werden.

Neben den Überschneidungen der beiden Bereiche gibt es aber auch Situationen, in denen IT-Sicherheit und Datenschutz gegensätzliche Ziele verfolgen. Das Speichern von Nutzungsdaten, z. B. welcher Praxismitarbeiter sich wann an welchem Rechnersystem angemeldet hat, ist solch eine Situation. Aus Sicht der IT-Sicherheit sollte man diese Daten immer erheben und für die Analyse zukünftiger Sicherheitsvorfälle beinahe unbegrenzt aufbewahren. Zweifelsohne handelt es sich dabei aber auch um Daten, die die Praxismitarbeiter ganz persönlich betreffen. Schon ihre Erhebung ist daher grundsätzlich erst einmal nicht statthaft.

Zusammenfassung

Informationstechnik (IT) bezeichnet jeden konkreten Einsatz von elektronischen Geräten in einer realen ökonomischen und/oder sozialen Umgebung.

Ein IT-Verbund ist die konkrete Ausprägung der Informationstechnik und umfasst – vor allem – die technischen und die organisatorischen Komponenten dieses konkreten Anwendungsbereiches. Für die technischen Komponenten verwendet man auch den Begriff IT-Infrastruktur.

Sicherheit bezeichnet das Ausmaß der Bestimmtheit und Gewissheit von zukünftigen Umständen. Schutz ist jede Maßnahme zur Erhöhung der Sicherheit.

Das Allgemeine Persönlichkeitsrecht ist im Artikel 2 des Grundgesetzes geregelt. Es räumt jedem Einzelnen das Recht auf eine unbeeinträchtigte Individualsphäre (Selbstbestimmungsrecht, z. B. das Recht auf informationelle Selbstbestimmung), Privatsphäre (Leben im häuslichen Bereich, Privatleben) und Intimsphäre ein.

Die informationelle Selbstbestimmung ist das Recht des Einzelnen, grundsätzlich selbst über jede Erhebung und jegliche Verwendung seiner ihn betreffenden Daten zu bestimmen.

Datenschutz bezeichnet den Schutz natürlicher Personen bei der Erhebung und Verwendung von Daten, die sie persönlich betreffen.

IT-Sicherheit ist formal der störungsfreie und gefahrenfreie Betrieb eines IT-Verbundes und pragmatisch das geplante Ausmaß der Vertraulichkeit, der Integrität und der Verfügbarkeit eines IT-Verbundes.

Wissenskontrolle

Haben Sie diese Lektion verstanden?

Dann haben Sie jetzt die Möglichkeit, das Gelernte auf unserer Lernplattform zu überprüfen.

Viel Erfolg!

Lektion 2

Grundlagen des Datenschutzes

LERNZIELE

Nach der Bearbeitung dieser Lektion werden Sie wissen, ...

... welche Prinzipien im Datenschutz Anwendung finden.

... welche rechtlichen Vorgaben zum Datenschutz in Deutschland zu beachten sind.

... was die wichtigsten gesetzlichen Grundlagen des Datenschutzes sind.

... wie man die eigenen Daten im Alltag besser schützen kann.

2. Grundlagen des Datenschutzes

Einführung

Eine Frau wehrt sich gegen die Absage einer Sicherheitsfirma wegen fehlender charakterlicher Eignung, die mit Verweis auf anonym zugespielte Bilder und Texte aus einem Internetforum begründet wurde.

In dem Internetforum beschrieb die Frau, dass sie sich regelmäßig an Glücksspielen beteiligt, teilweise auch um große Summen. Die Frau erwähnte in diesem Internetforum unzutreffender Weise auch, dass sie bereits Mitarbeiterin der Sicherheitsfirma sei.

Wurde der Frau zu Unrecht abgesagt?

Ein Unternehmen speichert den gesamten E-Mail-Verkehr mit seinen Kunden im Rahmen der Bearbeitung der Bestellungen. Er wird später von einem Kunden wegen fehlerhafter Lieferung verklagt. Das Unternehmen legt den E-Mail-Verkehr mit diesem Kunden im Prozess zu seiner Verteidigung vor.

Darf es das?

2.1 Prinzipien

Datenschutz ist in Deutschland und der EU ein Grundrecht, nämlich das Recht auf informationelle Selbstbestimmung. Dies ist das Recht des Einzelnen, selbst über die Erhebung und die Verwendung der ihn persönlich betreffenden Daten zu bestimmen. So bleibt es beispielsweise jedem selbst überlassen, ob er Informationen über sich im Internet veröffentlicht oder nicht. Werden gegen seinen Willen solche Veröffentlichungen gemacht, kann er dagegen vorgehen, da sein Recht auf informationelle Selbstbestimmung verletzt wurde.

Hauptziel des Datenschutzes ist demnach, das Recht des Einzelnen auf informationelle Selbstbestimmung zu garantieren.

Auch wenn das Recht auf informationelle Selbstbestimmung des Einzelnen beachtet werden muss, kann das naturgemäß nicht dazu führen, dass etwa jegliche Weitergabe von Daten über Personen verboten wird. Dann wäre jede Kommunikation unterbunden. Es muss vielmehr definiert werden, ab welcher Schwelle der Kommunikation der Datenschutz einsetzen soll.

Die Gesetzgeber sehen die Gefährdung des Rechts auf informationelle Selbstbestimmung nicht in der Bedeutung der einzelnen Daten. (Zur Erinnerung: Laut BVerfG gibt es keine belanglosen Daten.) Die Gefährdung, die mit dem Datenschutzrecht geregelt werden soll, ist vielmehr diejenige, bei der Muster gebildet werden können. Die Bildung von Mustern ermöglicht nämlich oft das Gewinnen zusätzlicher Informationen über eine Person, die man aus den einzelnen Daten nicht hätte ziehen können. Geregelt wird

folglich nur die Erhebung und Verwendung von Sammlungen personenbezogener Daten, die strukturiert aufgebaut sind und nach bestimmten Merkmalen gezielt ausgewertet werden können. Datenschutz hat also konkret das Ziel, strukturierte, merkmalsbezogene Erhebungen von personenbezogenen Daten und die Verwendung solcher Datensammlungen zu regulieren.

Diese Regulierungen orientieren sich an den folgenden allgemeinen Prinzipien:

- **Datengeheimnis:** Es ist untersagt, personenbezogene Daten unbefugt zu erheben oder zu verwenden.
- **Datenvermeidung:** Die Gestaltung und Auswahl von Verfahren zur Erhebung und Verwendung personenbezogener Daten hat sich an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben oder zu verwenden.
- **Erforderlichkeit:** Das Erheben und Verwenden personenbezogener Daten hat sich auch am Grundsatz der Erforderlichkeit zu orientieren. Der Begriff der Erforderlichkeit ist dabei eng auszulegen. Erforderlich sind personenbezogene Daten nur dann, wenn die Aufgabe sonst nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllt werden kann.
- **Interessenabwägung:** Die berechtigten Interessen der erhebenden bzw. verwendenden Stelle sind immer gegenüber den schutzwürdigen Interessen Betroffener abzuwägen.
- **Schutzbedarf:** Werden personenbezogene Daten erhoben oder verwendet, sind technische und organisatorische Maßnahmen zu treffen, um die Sicherheit der eingesetzten IT im Interesse des Schutzes des Persönlichkeitsrechtes zu gewährleisten.
- **Selbstauskunft:** Die Erhebung personenbezogener Daten muss – soweit möglich – beim Betroffenen erfolgen.
- **Transparenz:** Es ist Pflicht, den Betroffenen (dessen Daten gespeichert werden) über die Daten, die Zweckbestimmung der Erhebung und Verwendung und die Identität der verantwortlichen Stelle zu informieren.
- **Verhältnismäßigkeit:** Es dürfen nicht mehr personenbezogene Daten erhoben oder verwendet werden als notwendig („Übermaßverbot“).
- **Zweckbindung:** Bei jeder Erhebung oder Verwendung personenbezogener Daten ist zwingend ein hinreichend präziser Verwendungszweck festzulegen, von dem nur in wohl definierten Ausnahmefällen abgewichen werden kann.

2.2 Rechtliche Vorgaben

Überblick

Die Mitgliedsstaaten der Europäischen Union haben alle Gesetze und Regelungen zum Schutz personenbezogener Daten (im Folgenden – wegen der Häufigkeit des Vorkommens – oft mit PBD abgekürzt).

Damit das Datenschutzniveau in allen Staaten der EU zukünftig einen einheitlichen Mindeststandard erfüllt, wurde im Mai 2016 die sogenannte „Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“ beschlossen. Sie wird kurz mit **DSGVO** (EU-Datenschutz-Grundverordnung) bezeichnet und gilt ab 25.05.2018 EU-weit. ln dieser Verordnung wurde ein allgemein verbindlicher Datenschutzstandard für alle EU-Staaten festgelegt.

Die Gesetzgeber der Länder, des Bundes und der EU haben aber schon früher in verschiedenen Gesetzen Bestimmungen aufgenommen, die den Datenschutz in Deutschland regeln. In Deutschland galt daher das Bundesdatenschutzgesetz in der sogenannten alten Fassung (BDSG a.F.), das mit der Einführung der DSGVO in der neuen Fassung (BDSG n.F.) abgelöst wurde. Das BDSG n.F. ist inhaltlich kein eigenständiges Gesetz mehr, sondern enthält „nur“ noch Konkretisierungen und Ergänzungen zur DSGVO. Darüber hinaus gibt es weitere Gesetze, die Vorgaben machen, wie mit PBD umgegangen werden darf. Beispielsweise wird auch durch Regelungen im **Telekommunikationsgesetz (TKG)**, **Telemediengesetz (TMG)** oder in den **Sozialgesetzbüchern (SGB)** der Datenschutz gewährleistet.

Die DSGVO mit ihren 99 Artikeln und 173 Erwägungsgründen ist deutlich umfangreicher als das BDSG. Zudem richtet die DSGVO an den nationalen Gesetzgeber die Aufgabe, auf nationaler Ebene zusätzlich bestimmte Bereiche noch auszugestalten, bzw. gibt ihm die Möglichkeit zur Gestaltung bestimmter Bereiche an die Hand. In Deutschland ist dies eben durch das BDSG n.F. geschehen, andere EU-Staaten haben vergleichbare Regelungen.

Aufgrund der föderalen Struktur der Bundesrepublik gibt es außerdem **Landesdatenschutzgesetze (LDSG)** in den einzelnen Bundesländern, die aber im Wesentlichen nur Landes- und kommunale Behörden betreffen, für Unternehmen (in der Terminologie der Datenschutzgesetzgebung: nicht-öffentliche Stellen) haben diese LDSG nur geringe Bedeutung. Auch die Kirchen haben sich eigene Regelungen zum Umgang mit PBD gegeben. Zudem kann beispielsweise in Dienst- und Betriebsvereinbarungen geregelt sein, was im Unternehmen hinsichtlich des Umgangs mit PBD der Beschäftigten zu beachten ist.

Geltungsbereiche

Das Erheben und Verwenden von PBD für persönliche oder familiäre Zwecke fällt grundsätzlich nicht unter die Vorgaben des Datenschutzrechts (Art. 2 Abs. 2 DSGVO). Datenschutzrecht wirkt also vor allem in der beruflichen oder geschäftlichen Sphäre.

Ob und inwieweit ein Unternehmen welche Datenschutzgesetze beachten muss, hängt davon ab, wie das Unternehmen organisiert ist. Für ein privatrechtliches Unternehmen gilt grundsätzlich das BDSG. Für den Kindergarten einer Kirchengemeinde gilt hingegen das kirchliche Datenschutzrecht. Dagegen unterliegt beispielsweise die Datenverarbeitung einer Stadtverwaltung den datenschutzrechtlichen Regelungen des Bundeslandes, in dem sie ihren Sitz hat.

Allen Regelungen ist gemeinsam, dass sie lediglich Daten betreffen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Abs. 1 DSGVO). Derartige Daten heißen personenbezogene Daten (PBD). Typische PBD sind Name, Adresse, Telefonnummer, Bankverbindung. Von einem Personenbezug kann man immer dann ausgehen, wenn ohne besondere Schwierigkeiten von einem Datum auf die dazugehörige natürliche Person geschlossen werden kann. Können Daten nicht auf eine natürliche Person bezogen werden, weil sie beispielsweise anonymisiert wurden, dann fallen die Erhebung und Verwendung solcher Daten nicht unter das Datenschutzrecht. Das ist allerdings nicht zu verwechseln mit der Pseudonymisierung von Daten, bei der der Personenbezug nur mit Hilfe gesondert gespeicherter Daten wie einer Zuordnungstabelle möglich ist. Eine solche Pseudonymisierung kann helfen, personenbezogene Daten vor Missbrauch zu schützen, aber sie ändert nichts daran, dass es sich um personenbezogene Daten handelt, die dem Datenschutz unterliegen.

Daten über juristische Personen, also z. B. Daten über eine AG, eine GmbH oder eine GmbH & Co. KG, werden vom Datenschutzrecht nach DSGVO nicht erfasst. (In einigen Länder, insbesondere Österreich und die Schweiz, gelten eine Reihe von Datenschutzregeln aber auch für juristische Personen.) Eine Ausnahme liegt aber beispielsweise vor, wenn es sich bei einem Unternehmen um eine Personengesellschaft handelt, da dahinter unmittelbar natürliche Personen stehen. Auch die PBD von Kunden, Lieferanten und Sachbearbeitern unterliegen in allen Unternehmen den Bestimmungen des Datenschutzes.

Die Verfasser des Datenschutzrechts wollen PBD gerade dann schützen, wenn Informationstechnik eingesetzt wird. Die dabei zum Einsatz kommenden IT-Anwendungen erzeugen vielfache Risiken für die PBD. So können elektronisch geführte Daten oft in einer Weise verknüpft oder ausgewertet werden, die erst einmal nicht gestattet ist. Weil dies ohne Informationstechnik nicht so einfach geht, werden Verarbeitungen von PBD ohne den Einsatz von Informationstechnik grundsätzlich nicht vom Datenschutzrecht erfasst. Allerdings gibt es zwei wichtige Ausnahmen von dieser Regel:

1. Eine sogenannte nicht automatisierte Datei ist eine (zielstrebig zusammengetragene) Sammlung von Daten, die durch ihren gleichartigen Aufbau nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann (Beispiel: Patientenkarteikarten in einer Arztpraxis). Auch solche Datensammlungen unterliegen den Bestimmungen des Datenschutzrechts.
2. PBD von Beschäftigten dürfen nur dann erhoben und verwendet werden, wenn sie für die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich sind. Dies gilt unabhängig vom Einsatz der Informationstechnik, sodass gegebenenfalls auch Papierakten zu Beschäftigten datenschutzkonform geführt werden müssen.

Beispiel: Dr. Heilemacher kommt morgens in die Praxis und fragt seine Sprechstundenhilfe: „Na, wie geht es denn heute?“. Wenn sie darauf antwortet, ist es bereits das Erheben personenbezogener Daten. Dies ist nur deshalb erlaubt, weil der Doktor die Information nicht in einen Computer oder in eine strukturierte Sammlung eingibt, die ausgewertet werden kann.

Wie bereits erwähnt, sind PBD niemals belanglos. Es gibt aber einige PBD, für die das Datenschutzrecht einen besonderen Schutz verlangt. Diese dürfen nur unter ganz bestimmten Voraussetzungen erhoben oder verwendet werden, insbesondere ist gegebenenfalls eine besondere Einwilligung nach Art. 9 DSGVO erforderlich. Welche Daten zu diesen besonders schutzbedürftigen PBD zählen, legt ebenfalls Art. 9 DSGVO fest: Danach gehören zu den sogenannten besonderen Kategorien personenbezogener Daten solche, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Begriffe

Im Datenschutz werden drei Gruppen von Beteiligten unterschieden:

- **Betroffene:**
  - Dies sind die natürlichen Personen, deren Daten verarbeitet werden.
- **Verantwortlicher:**
  - Dies ist die Person oder sonstige Einheit, die über die Verarbeitung entscheidet und daher die Verantwortung dafür trägt. Der Verantwortliche kann die Verarbeitung selbst durchführen oder durch andere, beispielsweise einen Auftragsverarbeiter, durchführen lassen.
- **Auftragsverarbeiter:**
  - Dies ist die Person oder sonstige Einheit, die die Verarbeitung im Auftrag des Verantwortlichen durchführt. Er muss diese Verarbeitung gemäß den Vorgaben des Verantwortlichen und auf Basis eines schriftlichen Vertrages durchführen, trägt dafür aber normalerweise nicht die Verantwortung für die Rechtmäßigkeit der Verarbeitung.

Im BDSG a.F. gab es eine relativ detaillierte Untergliederung in Erhebung, Verwendung, Verarbeitung etc. von personenbezogenen Daten. Mit der DSGVO wurden diese verschiedenen Tätigkeiten unter dem Begriff der „Verarbeitung“ zusammengefasst, wobei die Verarbeitung von PBD wie folgt definiert ist:

Verarbeitung ist jeder „mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“ (Art. 4 Abs. 2 DSGVO).

Verbot mit Erlaubnisvorbehalt

Das Datenschutzrecht basiert auf dem sogenannten „Verbotsprinzip mit Erlaubnisvorbehalt". Dieses Prinzip besagt, dass das Erheben oder Verwenden von PBD prinzipiell verboten ist. Ausnahmen von diesem prinzipiellen Verbot erfordern eine einschlägige Rechtsgrundlage. Diese kann sich aus dem Datenschutzrecht (in erster Linie DSGVO), aus einer vorrangigen Rechtsvorschrift oder aus der (wirksamen) Einwilligung des Betroffenen ergeben.

Das BDSG a.F. galt als Auffanggesetz, d.h. andere, spezifischere gesetzliche Regelungen zum Datenschutz hatten im Zweifel Vorrang. Das gilt mit der DSGVO nur noch sehr eingeschränkt, denn hier hat im Zweifel die DSGVO als EU-Verordnung Vorrang vor nationalen Gesetzen.

Das hat beispielsweise zur Folge, dass für eine bisher vorrangige Rechtsvorschrift wie das Gesetz über das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG), die rechtliche Gültigkeit umstritten ist, auch wenn man meist weiterhin von dieser Gültigkeit ausgeht. Dort ist in § 22 das sogenannte Recht am eigenen Bild geregelt. Danach kann der Abgebildete selbst darüber bestimmen, ob und wie ein Bildnis (= Foto, Video, Zeichnung, ...) an Dritte weitergegeben wird, also z. B. ob es in einer Broschüre oder im Internet veröffentlicht wird. Das Gesetz sieht ausdrücklich vor, dass der Abgebildete in jede Verbreitung seines Bildnisses wirksam einwilligen muss. Allerdings sieht das KunstUrhG im § 23 (1) auch Ausnahmen von dieser Einwilligungspflicht vor:

1. **Bildnisse mit zeitgeschichtlichem Bezug:** Eine Einwilligung ist beispielsweise bei Politikern, Schauspielern und Musikern nicht erforderlich, weil es sich bei diesen um sogenannte Personen der Zeitgeschichte handelt. Trotzdem ist auch bei diesen Personen die Intimsphäre immer tabu!
2. **Personen als Beiwerk:** Steht im Mittelpunkt eines Bildes eine Landschaft oder eine Örtlichkeit und ist eine abgebildete Person quasi eine „Randerscheinung", dann ist auch hier keine Einwilligung der abgebildeten Person erforderlich. Juristisch gesehen ist sie nämlich nur „Beiwerk".
3. **Bilder von Versammlungen:** Werden Bilder von öffentlichen Versammlungen oder ähnlichen Veranstaltungen (z. B. Demo, Betriebsfest, Weihnachtsfeier) gemacht, dann ist eine Einwilligung der abgebildeten Personen nicht erforderlich, wenn erkennbar die Ansammlung von Menschen im Vordergrund steht und nicht bestimmte Personen.

Nach allgemeiner Rechtsprechung implizieren die Vorschriften des KunstUrhG auch, dass schon das Erstellen eines Bildnisses nur dann gestattet ist, wenn es an Dritte weitergegeben werden darf. Falls keine der genannten Ausnahmen greift, darf also der Abgebildete sogar darüber bestimmen, ob überhaupt ein Bildnis seiner Person erstellt werden darf.

Explizite Einwilligungen

Mit einer expliziten Einwilligung möchte ein Betroffener die Erhebung oder Verwendung einiger seiner PBD für einen bestimmten Zweck ermöglichen. Betroffene können jedoch nur in solche Erhebungen oder Verwendungen von PBD sinnvoll einwilligen, deren Konsequenzen sie hinreichend klar einschätzen können.

Für eine Einwilligung fordert die DSGVO in Art. 4, Abs. 11, explizit, dass diese „freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich" erfolgen muss: Es ist bei der Einwilligung auf die Bedeutung der Einwilligung, den Zweck der Erhebung oder Verwendung sowie auf das Recht und die Folgen der Verweigerung und des Widerrufs der Einwilligung hinzuweisen. Das äußere Erscheinungsbild der Einwilligung ist hervorzuheben.

Beispiel für eine Einwilligungserklärung:

„Ich bin mit der Zusendung von Informationen über Ihre neuen Produkte und Dienstleistungen einverstanden. Diese Einwilligung kann ich jederzeit schriftlich per Brief oder per E-Mail an <E-Mail-Adresse-die-die-Widersprüche-bearbeitet> mit Wirkung für die Zukunft widerrufen. Für die Zusendung der Informationen nutzen Sie bitte folgende Kontaktdaten: E-Mail-Adresse oder Postadresse."

Die DSGVO sieht ein Mindestalter von 16 Jahren für die wirksame Erteilung einer Einwilligung in die Erhebung oder Verwendung von PBD vor.

Anders als in der Vergangenheit muss eine Einwilligung gemäß DSGVO nicht schriftlich erfolgen, auch wenn dies aus Nachweisgründen oft empfehlenswert ist.

Möglich ist beispielsweise auch eine elektronische Einwilligung per Web-Formular, E-Mail oder Telefax. Hierbei muss aber sichergestellt sein, dass die elektronische Einwilligung eindeutig und bewusst abgegeben wird. Typisch muss bei Web-Formularen ein Kästchen mit einem Häkchen vorgesehen sein, welches der Kunde anklicken muss, und erst dann ist seine Einwilligung erteilt **(„Opt-In-Verfahren")**. Zudem müssen elektronische Einwilligungserklärungen systemseitig protokolliert werden. D. h., es muss jederzeit die Möglichkeit bestehen, den Einwilligungstext einzusehen und die Einwilligungserklärung zu widerrufen.

Opt-In-Verfahren
Das ist ein Bestätigungskonzept für Transaktionen, das eine ausdrückliche Zustimmung des Betroffenen erfordert.

Rechtsgrundlagen

Für relativ häufig vorkommende Situationen hat die DSGVO zudem eine Rechtsgrundlage geschaffen, nach der Organisationen PBD auch ohne explizite Einwilligung erheben oder verwenden dürfen.

Nach Art. 6 Abs. 1 DSGVO ist demnach die Verwendung von PBD zulässig, wenn eine der folgenden Bedingungen erfüllt ist:

a. „Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
b. die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
c. die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
d. die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
e. die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
f. die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt."

Die in der Praxis wichtigsten Rechtsgrundlagen sind die Einwilligung (Bedingung a), die Vertragserfüllung (Bedingung b) sowie das berechtigte Interesse (Bedingung f).

Ein typisches Beispiel zu Bedingung b) sind Lieferadressen, denn ohne diese könnte die Lieferung und damit die Erfüllung eines Kaufvertrags nicht erfolgen. Dies gilt aber ausdrücklich nur für die Verarbeitung, die für die Vertragsabwicklung erforderlich ist. Wenn später die gleichen Daten für die Versendung von Werbung verwendet werden sollen, dann ist Bedingung b) als Rechtsgrundlage nicht mehr ausreichend, sondern hierfür wird eine separate Einwilligung notwendig.

Hier ist zu beachten, dass bei Bedingung f) eine Interessenabwägung zwischen den berechtigten Interessen des Verantwortlichen und den Interessen etc. der betroffenen Person gefordert ist.

Folglich wurde im Übrigen in dem zu Anfang dieser Lektion geschilderten Fall der Frau entsprechend Bedingung f) zu Recht abgesagt. Zum einen hat nämlich die Sicherheitsfirma ein überwiegendes Interesse daran, die charakterliche Eignung von Bewerbern genau zu kennen. Zum anderen hat die Frau die verwendeten Informationen selbst preisgegeben. Dass sie dabei auch noch unwahre Angaben gemacht hat, unterstreicht nur ihre mangelnde charakterliche Eignung.

Auch das Unternehmen darf – um die ebenfalls zu Anfang dieser Lektion gestellte Frage zu beantworten – gemäß Bedingung f) den E-Mail-Verkehr zu seiner Entlastung im Prozess vorlegen, da es sich nur so gegen den Vorwurf der falschen Lieferung wehren kann.

Keine explizite Einwilligung erfordert die Verarbeitung von besonderen PBD durch Ärzte (und durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen), soweit sie zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist (§22 (1) b) BDSG n.F.).

Instanzen

Die Kontrolle des Datenschutzes hat der Gesetzgeber sogenannten Aufsichtsbehörden übertragen. Meist sind dies im privatwirtschaftlichen Bereich die **Landesbeauftragten für den Datenschutz.** Ihnen werden in §40 BDSG n.F. umfangreiche Rechte eingeräumt.

Landesbeauftragten für den Datenschutz
Sie sind die Beauftragten eines deutschen Bundeslandes, die die öffentlichen Stellen des jeweiligen Landes in Fragen des Datenschutzes überwachen und beraten.

So können sie jederzeit Informationen über die Erhebung oder Verwendung von PBD von den privatwirtschaftlichen Unternehmen anfordern, für die sie zuständig sind. Sogar Kontrollen vor Ort können durchgeführt werden. Und dafür ist noch nicht einmal eine Anmeldung erforderlich. Aufsichtsbehörden kümmern sich regelmäßig auch um Beschwerden von Betroffenen, die in ihrem Zuständigkeitsbereich residieren.

Werden von einer Aufsichtsbehörde Verstöße gegen den Datenschutz festgestellt, kann sie die Beseitigung der Mängel verlangen und gegebenenfalls auch ein Bußgeld verhängen.

Den mit der Erhebung oder Verwendung von PBD befassten Mitarbeitern einer verantwortlichen Stelle ist es untersagt, dies unbefugt zu tun (Datengeheimnis). Anders als in BDSG a.F. ist eine Verpflichtung auf das Datengeheimnis nicht mehr explizit gefordert, ergibt sich aber implizit aus der Forderung von Art. 24 nach Umsetzung geeigneter technischer und organisatorischer Maßnahmen zum Datenschutz. Zwar ist die Schriftform für diese Verpflichtung nicht vorgeschrieben, aus Beweisgründen sollte sie aber schriftlich erfolgen. Das Datengeheimnis gilt übrigens auch nach dem Ende der Tätigkeit für die verantwortliche Stelle weiter.

Fast immer ist die Geschäftsleitung des Verantwortlichen dazu verpflichtet, die Einhaltung aller datenschutzrechtlichen Vorschriften zu kontrollieren und sicherzustellen. Eine zusätzliche Kontrollfunktion kann bzw. muss oft ein Datenschutzbeauftragter wahrnehmen (Art. 37-39 DSGVO; § 38 BDSG n.F.). Er wirkt darauf hin, dass die datenschutzrechtlichen Vorschriften in der verantwortlichen Stelle eingehalten und umgesetzt werden. Insofern unterstützt er die Geschäftsleitung, welche aber alle diesbezüglich erforderlichen Entscheidungen eigenverantwortlich treffen muss.

Rechte der Betroffenen

Die DSGVO legt auch fest, welche Rechte ein Betroffener im Umfeld der Erhebung oder Verwendung seiner PBD hat. Dabei kann niemand – etwa durch Vertragsklauseln – daran gehindert werden, diese Rechte auszuüben.

Zu den Rechten eines Betroffenen zählen das Recht auf Auskunft und das Recht auf Berichtigung, Löschung oder Sperrung von PBD.

Jedermann kann grundsätzlich von allen Institutionen ohne Angabe von Gründen **Auskunft** darüber verlangen, ob und gegebenenfalls welche PBD zu seiner Person gespeichert sind (Art. 15 DSGVO). Die Institution muss bei positivem Bescheid in seiner Auskunft auch mitteilen, zu welchem Zweck die Speicherung der PBD erfolgt ist und an welche Empfänger diese gegebenenfalls weitergegeben wurden.

Nichtzutreffende PBD müssen korrigiert werden (Art. 16 DSGVO). **Berichtigungen** müssen durch die verantwortliche Stelle auch an die Stellen weitergegeben werden, an die diese nichtzutreffenden Daten bereits übermittelt wurden.

PBD unterliegen auch einer **Löschpflicht** (Art. 17 DSGVO). Diese ist insbesondere immer dann gegeben, wenn die Speicherung dieser PBD

- gar nicht zulässig war (Beispiel: unwirksame Einwilligung) oder
- nicht mehr erforderlich ist (Beispiel: Daten aus einem Gewinnspiel, wenn das Gewinnspiel abgeschlossen ist).

Hierbei spricht man auch vom **Recht, vergessen zu werden** (vgl. Art. 17 DSGVO). Eingeschlossen ist dabei, dass Verknüpfungen zu oder Kopien von veröffentlichten und allgemein zugänglichen Daten entfernt werden müssen. Dies dürfte für manch ein soziales Netzwerk eine fast unlösbare Aufgabe sein.

Auch wenn PBD gelöscht werden könnten, müssen diese unter Umständen weiterhin gespeichert bleiben. Dies gilt insbesondere dann, wenn sogenannte **Aufbewahrungspflichten** bestehen. So müssen beispielsweise steuerrechtlich relevante Belege zehn Jahre lang im Unternehmen aufbewahrt werden.

Stehen einer Löschung von PBD etwa derartige Aufbewahrungspflichten entgegen, dann sieht die DSGVO zwingend vor, dass diese von einer weiteren Verwendung wirksam auszuschließen sind (Einschränkung der Verarbeitung gemäß Art. 18 DSGVO; auch als "Sperrung" bekannt). Eine Sperrung von PBD ist auch immer dann vorzunehmen, wenn die Löschung unverhältnismäßig aufwendig ist oder wenn die Richtigkeit der PBD vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

Verarbeitung im Auftrag

Das Datenschutzrecht gestattet es ausdrücklich, dass eine verantwortliche Stelle einen Dienstleister mit der Verarbeitung ihrer PBD beauftragen kann. Geregelt ist diese sogenannte Auftragsverarbeitung im Art. 28, 29 DSGVO.

Unabdingbare Voraussetzung für diese Auftragsdatenverarbeitung ist ein schriftlicher Vertrag, der den strengen (!) Vorgaben des Art. 28 Abs. 3 DSGVO entspricht und dabei genau festlegt, auf welche Art und Weise der Dienstleister handeln muss. Für den

Schutz, der dann im Auftrag verarbeiteten PBD bleibt aber stets der Auftraggeber voll verantwortlich. Dies impliziert, dass er die entsprechenden Tätigkeiten des Dienstleisters engmaschig kontrollieren muss.

Auch bei Wartungsdienstleistungen gelten unter Umständen diese Vorgaben, beispielsweise, wenn dabei der Zugriff auf PBD nicht ausgeschlossen werden kann. Beispiel: Die Dienstleistung für die Fernwartung des PVS in der Arztpraxis Dr. med. Heilemacher muss vertraglich gemäß Art. 28 DSGVO geregelt werden.

Übermittlung ins Ausland

Für die Übermittlung von PBD ins Ausland müssen grundsätzlich zwei Voraussetzungen erfüllt sein: Zuerst einmal handelt es sich um eine Form der Verarbeitung der PBD, für die es eine Rechtsgrundlage geben muss, so wie auch im Inland. Zusätzlich muss sichergestellt sein, dass die Daten auch nach der Übermittlung ins Ausland angemessen geschützt sind. Diese Voraussetzung wird im Folgenden näher betrachtet.

Unproblematisch ist die Übermittlung von PBD an Institutionen in anderen Mitgliedstaaten der Europäischen Union, an Institutionen in Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum (Norwegen, Liechtenstein, Island) und an Organe und Einrichtungen der Europäischen Gemeinschaft.

In anderen Fällen dürfen aber PBD an ausländische Institutionen ohne Weiteres nicht übermittelt werden. Grund hierfür ist die (oft berechtigte) Annahme, dass erst einmal kein angemessenes Datenschutzniveau bei einer empfangenden Stelle im Ausland vorausgesetzt werden kann. Die DSGVO kennt in diesem Zusammenhang auch nicht das sogenannte Konzernprivileg. Daher dürfen auch verschiedene, rechtlich selbstständige Unternehmen einer internationalen Unternehmensgruppe nicht ohne Weiteres PBD einander zur Verfügung stellen.

Für die somit problematische Übermittlung von PBD an ausländische Institutionen – ein Thema, das insbesondere bei sozialen Netzwerken und bei Cloud-Dienstanbietern auftritt – sind die Datenschutzregelungen (Art. 44-50 DSGVO) recht engmaschig und kompliziert.

Auch hier gilt das Prinzip des Verbots mit Erlaubnisvorbehalt, d.h. eine Datenübertragung ins Nicht-EU-Ausland ist grundsätzlich verboten, wenn nicht einer der definierten Erlaubnistatbestände greift. Diese Erlaubnistatbestände beschreiben verschiedene Optionen, wie die Einhaltung eines angemessenen Datenschutzniveaus sichergestellt werden kann.

Ein angemessenes Datenschutzniveau gilt beispielsweise als gewährleistet, wenn die Europäische Kommission dies durch einen sogenannten Angemessenheitsbeschluss ausdrücklich festgestellt hat. Dies ist bisher u. a. der Fall für alle Institutionen in den Ländern Argentinien, Guernsey, Kanada (mit einigen Ausnahmen) und Schweiz. Bis Juli 2020 gab es einen solchen Angemessenheitsbeschluss auch für Unternehmen in den USA, die sich dem sogenannten EU-US-Privacy Shield angeschlossen hatten und sich

damit selbst zum Schutz PBD nach den dort definierten Regeln verpflichtet hatten. Durch eine Entscheidung des Europäischen Gerichtshofes (EuGH), das sogenannte „Schrems II"-Urteil, wurde dieser Angemessenheitsbeschluss aber ebenso wie die Vorgängerregelung „Safe Harbor" für ungültig erklärt und ist daher nicht mehr anwendbar. Hintergrund ist die umfassende Möglichkeit US-amerikanischer Geheimdienste, auf bei amerikanischen Unternehmen gespeicherte Daten von EU-Bürgern zuzugreifen, wogegen es für nicht-Amerikaner auch keine Rechtsmittel gibt.

Eine weitere verbreitete Grundlage, um ein angemessenes Datenschutzniveau beim Empfänger der Daten sicherzustellen, sind die von der Europäischen Kommission definierten Standardvertragsklauseln für Verträge zwischen Sender und Empfänger PBD. Hier wurde aber spätestens durch das genannte „Schrems II"-Urteil deutlich, dass diese Standardvertragsklauseln nicht immer ausreichen, sondern dass diese ggf. durch zusätzliche Regelungen ergänzt werden müssen, um ein angemessenes Datenschutzniveau zu erreichen.

Daneben definiert die DSGVO noch einige weitere „Garantien", mit denen ein angemessenes Datenschutzniveau sichergestellt werden kann, beispielsweise verbindliche interne Datenschutzrichtlinien (Binding Corporate Rules BCR), oder für Einzelfälle die Möglichkeit, einen Datentransfer über eine Einwilligung des Betroffenen zu erlauben.

Darüber hinaus kann die zuständige Aufsichtsbehörde einzelne Übermittlungen von PBD an gewisse Stellen im Ausland genehmigen, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte nachweist.

Sanktionen

Ein Datenschutzverstoß, also das unzulässige Erheben oder Verwenden von PBD, kann erhebliche Folgen für die Täter und /oder für die verantwortliche Stelle selbst haben. Mit der DSGVO wurden die möglichen Bußgelder massiv erhöht, in besonderen Fällen können Bußgelder in Höhe von bis zu vier Prozent des Jahresumsatzes des Unternehmens verhängt werden.

Darüber hinaus kann ein Datenschutzverstoß einen nachhaltigen Imageschaden bewirken. Es kann mitunter Jahre dauern, bis dieser getilgt ist. Artikel 33 und 34 DSGVO schreiben übrigens vor, dass eine verantwortliche Stelle bei schwerwiegenden Datenschutzverstößen (wie Diebstahl von Kreditkarteninformationen) die zuständige Aufsichtsbehörde und die betroffenen Personen informieren muss. Daher können zumindest schwerwiegende Datenschutzverstöße auch nicht so leicht verheimlicht werden.

Ist einem Arbeitnehmer ein grob fahrlässiger oder gar vorsätzlicher Datenschutzverstoß anzulasten, dann kann dies zu arbeitsrechtlichen Konsequenzen führen. Solch ein Datenschutzverstoß zieht oft eine arbeitsrechtliche Abmahnung nach sich. Ist dem Arbeitgeber die weitere Beschäftigung des Arbeitnehmers nicht mehr zuzumuten, dann kann er allein aufgrund des Datenschutzverstoßes schon eine Kündigung aussprechen.

In besonders schweren Fällen kann dies sogar fristlos erfolgen. Entsteht dem Arbeitgeber durch einen grob fahrlässigen oder gar vorsätzlichen Datenschutzverstoß ein Schaden, dann kann er diesen vom Verursacher ersetzt verlangen.

Artikel 82 DSGVO regelt auch **Schadensersatzansprüche für einen Betroffenen,** wenn diesem ein Schaden durch einen Verstoß gegen die Regelungen des Datenschutzes entstanden ist.

Sondervorschriften

Das BDSG enthält auch Vorschriften zum Einsatz von Videoüberwachung in Institutionen (§4 BDSG n.F.). Die DSGVO befasst sich hingegen nicht explizit mit der Zulässigkeit derartiger Videoüberwachungen. Erwähnung finden diese lediglich in Artikel 35 DSGVO: Dieser regelt die Notwendigkeit einer sogenannten Datenschutz-Folgenabschätzung.

Auf jeden Fall sind bei der Videoüberwachung in Institutionen alle Bereiche ausgeschlossen, die der Privat- oder der Intimsphäre von Personen zuzuordnen sind. Das Grundrecht des Einzelnen auf Privatsphäre hat hier immer Vorrang. Beispiel: Behandlungszimmer des Arztes.

Hinsichtlich der Zulässigkeit der Videoüberwachung ist bei öffentlich zugänglichen Räumen einer Institution §4 BDSG n.F. zu beachten, der u. a. eine Videoüberwachung zur Kontrolle des Zutritts gestattet.

Ein öffentlich zugänglicher Raum einer Institution ist jeder Bereich, der von jedermann betreten werden kann. Beispiel: Rezeption in der Arztpraxis. Nicht öffentlich zugänglich ist hingegen ein Raum, der nur von ausgewählten Personen betreten werden soll. Beispiel: Teeküche in der Arztpraxis.

Der heimliche Einsatz von Videoüberwachung ist fast immer verboten. In wenigen Ausnahmefällen kann allerdings auch der heimliche Einsatz von Videoüberwachung bei Vorliegen konkreter Verdachtsmomente gestattet sein. Beispiel: Aufklärung von wiederholtem Medikamentendiebstahl in der Arztpraxis.

Auf den Umstand, dass ein Bereich videoüberwacht wird, muss die verantwortliche Stelle daher fast immer durch entsprechende, gut sichtbare Schilder hinweisen (§ 4 (2) BDSG n.F.). Sind auch Beschäftigte einer Institution von einer Videoüberwachung betroffen, muss datenschutzrechtlich zusätzlich auch § 26 BDSG n.F. beachtet werden. Dieser regelt nämlich das Erheben und Verwenden von PBD im Verhältnis zwischen Arbeitgeber und Arbeitnehmer.

Danach ist das Erheben und Verwenden personenbezogener Daten von (potenziellen) Beschäftigten nur zulässig, wenn dies für die Entscheidung über die Begründung, die Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich ist. Dabei kommt es vor allem auch darauf an, ob das Erheben oder Verwenden PBD zur Erreichung eines bestimmten Zwecks tatsächlich erforderlich ist. Ähnlich wie bei der

Videoüberwachung enthält die DSGVO keinerlei spezifische Regelungen zum Beschäftigtendatenschutz. Stattdessen steht es den einzelnen EU-Mitgliedsländern frei, diesen Themenkomplex zukünftig eigenständig zu regulieren (sogenannte „Öffnungsklausel“).

Zu den bekanntesten, unzulässigen Erhebungen personenbezogener Daten bei Bewerbern gehört die Frage nach einer Schwangerschaft. Bewerberinnen müssen darauf nie antworten. Sie dürfen diese Frage aber auch mit einer Lüge beantworten. Erst recht muss die Bewerberin niemals von sich aus offenbaren, dass sie schwanger ist.

Gibt es im Unternehmen übrigens einen Betriebsrat, darf dieser nach § 87 (1) Nr. 6 Betriebsverfassungsgesetz (BetrVG) oft auch beim Erheben und Verwenden personenbezogener Beschäftigtendaten mitbestimmen. Dies gilt jedenfalls immer dann, wenn die fragliche Erhebung oder Verwendung der Daten eine Überwachung des Verhaltens oder der Leistung von Arbeitnehmern nicht von vornherein ausschließt.

2.3 Informationelle Selbstbestimmung im Alltag

Betroffene können durch ihr Verhalten erheblich dazu beitragen, dass eigene und auch fremde personenbezogene Daten geschützt sind und nicht ungewollt in die Hände von Dritten gelangen:

1. Es sollten nur die absolut erforderlichen persönlichen Daten preisgegeben werden, insbesondere online.
2. Dokumente und Papiere mit persönlichen Daten sollten geschreddert werden, bevor sie entsorgt werden.
3. Kennnummern, die von Behörden o. ä. stammen, wie Steuernummer, Nummer des Personalausweises, Kontonummer etc. sollten niemals preisgegeben werden, es sei denn, es ist absolut notwendig und rechtlich erforderlich. Derartige Kennnummern sollten niemals als Passwort genutzt werden.
4. Persönliche Dokumente (Pass, Geburtsurkunde) sollten an einem sicheren Ort aufbewahrt werden, am besten in einem Safe.
5. In sozialen Medien sollten nur wenige persönliche Informationen preisgegeben werden. Die Einstellungsmöglichkeiten und Sicherheitsmechanismen können hier auch hilfreich sein.
6. Zugangsdaten zu Online-Konten und Online-Diensten dürfen niemals per E-Mail oder Telefon preisgegeben werden. Wer eine Aufforderung erhalten hat, sollte den Dienstleister selbst über vertrauenswürdige Kanäle kontaktieren und in Erfahrung bringen, ob die Aufforderung zur Preisgabe legitim ist.
7. Es sollten komplexe Passwörter genutzt werden. Diese sollten niemals aufgeschrieben und weitergegeben werden. Wem dies schwerfällt, sollte einen sogenannten „Passwortmanager“ nutzen.
8. Es ist darauf zu achten, dass Geräte softwaremäßig stets auf dem neuesten Stand sind.
9. Vertrauliche Daten sollten verschlüsselt werden.
10. Öffentliche WLAN-Spots ohne gesicherte Verbindungen sollten nicht genutzt werden.

11. Beim Herunterladen oder Nutzen von Apps ist darauf zu achten, dass diese keinen Zugriff auf persönliche Daten haben, es sei denn, dieser ist zwingend erforderlich.
12. Auf die Zahlungsinformationen von Bezahlkarten ist genau zu achten. Am besten werden diese täglich geprüft.
13. Bei Verlust einer Bezahlkarte, sollte die ausgebende Stelle umgehend informiert werden.
14. Ein jährliches Abfragen der „Schufa-Auskunft“ ist sinnvoll. Diese ist kostenlos.
15. Privat, beruflich und geschäftlich sollte das „Recht am eigenen Bild“ beachtet werden.

Zusammenfassung

Zweck des Datenschutzrechts ist, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Die wichtigsten gesetzlichen Regelungen zum Datenschutz sind enthalten in der DSGVO, darüber hinaus auch im Bundesdatenschutzgesetz (BDSG), dem Telekommunikationsgesetz (TKG), dem Telemediengesetz (TMG), den Sozialgesetzbüchern (SGB), den Landesdatenschutzgesetzen (LDSG) und den entsprechenden Regelungen der Kirchen.

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Das Erheben, Verarbeiten oder Nutzen von personenbezogenen Daten ist im beruflichen oder geschäftlichen Umfeld grundsätzlich verboten. Es ist nur dann erlaubt, wenn sich dies aus der DSGVO, einer vorrangigen Rechtsvorschrift oder der Einwilligung des Betroffenen ergibt.

Selbst bei Vorliegen eines Erlaubnistatbestandes ist (zumindest oft) noch eine Interessenabwägung durchzuführen, d. h., es ist zu prüfen, ob nicht das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung oder Verwendung überwiegt.

Den bei der Verarbeitung von personenbezogenen Daten beschäftigten Personen ist es untersagt, diese unbefugt zu erheben oder zu verwenden (Datengeheimnis).

Jede natürliche Person hat das Recht auf Auskunft über sie betreffende, personenbezogene Daten und das Recht auf Berichtigung, Löschung und Sperrung seiner personenbezogenen Daten. Diese Rechte sind unabdingbar.

Die Aufgabe eines (gesetzlichen) Datenschutzbeauftragten ist insbesondere die Hinwirkung auf die Einhaltung der verschiedenen Vorschriften über den Datenschutz.

Auftragsverarbeitung im Sinne des Datenschutzes ist die Erhebung oder Verwendung von personenbezogenen Daten durch einen Dienstleister im Auftrag einer verantwortlichen Stelle. Das Datenschutzrecht legt im Detail fest, welche Rechte, Pflichten und Maßnahmen im Einzelnen durch Vertrag zwischen Auftraggeber und Auftragnehmer zu treffen sind. Besondere Regelungen gelten für personenbezogene Daten bei einer Übertragung ins Ausland, insbesondere ins außereuropäische.

Bei Videoüberwachung in öffentlich zugänglichen Bereichen muss § 4 BDSG n.F. beachtet werden. Auf den Einsatz von Videoüberwachung muss hingewiesen werden. Heimliches Überwachen ist grundsätzlich unzulässig.

Personenbezogene Daten von Beschäftigten dürfen nur erhoben, verarbeitet oder genutzt werden, wenn dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist.

Gegen die DSGVO wird verstoßen, wenn unrechtmäßigerweise personenbezogene Daten erhoben oder verwendet werden. Die Folgen von Datenschutzverstößen sind Geldbußen von bis zu 4% des weltweiten Jahresumsatzes oder Freiheitsstrafen von bis zu zwei Jahren. Bei schwerwiegenden Verstößen müssen die Datenschutzaufsichtsbehörde und die betroffenen Personen informiert werden. „Datenschutzpannen“ können zudem nachhaltig das Ansehen einer Institution negativ beeinträchtigen.

Wird ein Datenschutzverstoß von einem Arbeitnehmer vorsätzlich oder grob fahrlässig verursacht, kann das Unternehmen den entstandenen Schaden von ihm ersetzt verlangen. Eine Verletzung datenschutzrechtlicher Bestimmungen kann auch zu einer Abmahnung führen. Ist dem Unternehmen die weitere Beschäftigung des Arbeitnehmers nicht mehr zuzumuten, dann kann dieses eine Kündigung aussprechen. Bei besonders schwerwiegenden Verstößen kann dies sogar fristlos erfolgen.

Wissenskontrolle

Haben Sie diese Lektion verstanden?

Dann haben Sie jetzt die Möglichkeit, das Gelernte auf unserer Lernplattform zu überprüfen.

Viel Erfolg!

Lektion 3

Grundlagen der IT-Sicherheit

LERNZIELE

Nach der Bearbeitung dieser Lektion werden Sie wissen, ...

... welche Paradigmen der IT-Sicherheit zugrunde liegen.

... welche grundlegenden Modelle der IT-Sicherheit es gibt.

... welche rechtlichen Vorgaben es für die IT-Sicherheit gibt.

3. Grundlagen der IT-Sicherheit

Einführung

Wer ein gewisses Ausmaß von Vertraulichkeit, Integrität und Verfügbarkeit für einen IT-Verbund planen, einführen und kontrollieren will, der ist mit einem sehr komplexen Anliegen konfrontiert.

Zum Glück gibt es aber heute in der Wissenschaft einen allgemeinen Konsens über gewisse Annahmen und Vorstellungen, die für dieses Anliegen Lösungen anbieten. Diese Annahmen und Vorstellungen spiegeln sich in sogenannten Paradigmen wider. Dabei handelt es sich um „Muster“ oder „Vorbilder“, die eine ganzheitliche Sicht auf die IT-Sicherheit eines IT-Verbundes erleichtern.

Ein Modell der IT-Sicherheit eines IT-Verbundes geht noch einen Schritt weiter: Es beschreibt Zustände und ihre Übergänge, unterscheidet sichere von unsicheren Zuständen und erklärt, unter welchen Umständen sichere Zustände erreicht werden. Aufgabe eines Modells der IT-Sicherheit ist es dabei oft, einen Kunden davon zu überzeugen, dass ein IT-Verbund sicher ist. Darüber hinaus dienen aber derartige Modelle auch als Baupläne für sichere Systeme oder Systemkomponenten.

Ebenfalls zu den Grundlagen gehören die rechtlichen Vorgaben der IT-Sicherheit. Während die bis dahin bereits behandelten grundlegenden Aspekte eher der Prävention dienen, geht es hier vor allem um die Reaktion auf erwiesenes Fehlverhalten (vgl. Eckert 2014).

3.1 Paradigmen der IT-Sicherheit

Ein Regelwerk, welches das geplante Ausmaß von Vertraulichkeit, Integrität und Verfügbarkeit eines IT-Verbundes mehr oder weniger verbindlich festlegt, kann stets mithilfe informeller Texte dargestellt werden. Allerdings öffnet dies unterschiedlichen Interpretationen Tür und Tor, wenn die Texte nicht präzise genug abgefasst werden.

ACL

Dies wurde schon erkannt, als noch Großrechner in der IT vorherrschten, die die Daten vieler Nutzer verwalteten und verarbeiteten. Daher verwendete man schon früh in diesen Regelwerken der IT-Sicherheit eine sogenannte Zugriffsliste (Access Control List [ACL]), die für jeden Nutzer (Mensch, Maschine, …) und für jedes Objekt (Datei, Gerät, …) des IT-Verbundes einzeln vermerkt, welche Nutzungsrechte (Lesen, Schreiben, Einschalten, Konfigurieren, …) am spezifischen Objekt dem jeweiligen Nutzer eingeräumt werden.

Diese präzise Festlegung und Kontrolle von Nutzungsrechten entsprang der Erkenntnis, dass es eine notwendige Voraussetzung für IT-Sicherheit ist, stets zu wissen, wer mit wem wie interagiert bzw. interagieren darf.

Bei Dateien und Geräten gibt es beispielsweise die Nutzungsoptionen READ, WRITE und EXECUTE und die Freigabe einer dieser Nutzungsoptionen wird dann je Nutzer in einer ACL wie folgt explizit festgelegt:

ACL				
	...	Objekt-1	Objekt-2	...
...	...	...	...	...
Nutzer-1	...	READ, WRITE	EXECUTE	...
...	...	...	...	...

In den Zeilen werden dabei die Nutzer und in den Spalten die Objekte aufgelistet. An den Schnittpunkten werden dann die Nutzungsrechte vermerkt.

Je nachdem, wie verbindlich die Pflege und Durchsetzung einer ACL im laufenden Betrieb eines IT-Verbundes ist, spricht man von Discretionary Access Control (DAC) oder Mandatory Access Control (MAC).

Discretionary Access Control (DAC)

Bei DAC überlässt man es typisch dem Besitzer bzw. Erzeuger eines Objektes, die Nutzungsrechte festzulegen. Dies trifft etwa auf UNIX-artige Betriebssysteme zu, wo der „Owner“ für sich, für die Mitglieder seiner Gruppe und für alle anderen Nutzer jeweils unterschiedliche Nutzungsrechte festlegen kann. Auch bei sozialen Netzwerken ist DAC meist das geeignete Mittel zum Zweck.

Allerdings wird in der Praxis bei DAC der Nutzer oft allein durch seinen Benutzernamen bestimmt und nicht durch weitere Attribute. Zudem wird meist bei fehlendem Eintrag angenommen, dass der nicht genannte Nutzer alle Nutzungsrechte hat.

Mandatory Access Control (MAC)

Bei MAC hingegen ist eine rigorose Strategie fest verankert. Typisch wird die ACL zentral gepflegt und automatisch erzwungen. Dabei ist fast immer ein fehlender Eintrag gleichbedeutend mit: Der Nutzer hat keinerlei Nutzungsrechte am Objekt.

Egal ob DAC oder MAC, die Pflege einer ACL wird schnell allein schon wegen der Größe und der Dynamik des IT-Verbundes problematisch. Daher ist man auch schon seit geraumer Zeit dazu übergegangen, Nutzer und Objekte bestimmten Gruppen zuzuordnen und dann nur noch für diese Gruppen Nutzungsrechte festzulegen. Beispiel: Nur die Mitglieder der Gruppe „Praxispersonal" dürfen Dateien der Gruppe „Patientendaten" einsehen (READ) und verändern (WRITE).

Gruppen können dabei auch Teile von anderen Gruppen sein. Und – zur Vereinfachung der Pflege der ACL – geht man dann generell von einer Rechtevererbung aus: Eine Gruppe erbt in jedem Fall alle Nutzungsrechte, die einer umfassenderen Gruppe eingeräumt wurden. Hierin verbirgt sich jedoch auch ein häufiger Fehlerfall, wenn etwa widersprüchliche Nutzungsrechte auftreten. In der Praxis wird daher von „unten nach oben" so lange die Vererbungskette durchforscht, bis eine explizite Einräumung (Allow) oder Verweigerung (Deny) eines Nutzungsrechts gefunden wurde.

Role Based Access Control (RBAC)

Noch einen Schritt weiter geht die sogenannte Role Based Access Control (RBAC): Dieses Konzept vergibt Nutzungsrechte auf Grundlage des aktuellen Arbeitsprozesses.

Bei RBAC werden den Nutzern Rollen zugeordnet (etwa: Administrator, Gast, ...). Nutzer können dabei formal zwar mehrere Rollen besitzen, aber stets nur in einer Rolle handeln. Rollen können auch hierarchisch gegliedert sein (im Sinne von: „... ist ein ..."). An eine Rolle sind oft auch eine oder mehrere Gruppenzugehörigkeiten (mit den eingeräumten Nutzungsrechten) gebunden. Je nach der aktuellen Rolle des Nutzers (und gegebenenfalls den damit verbundenen Gruppenzugehörigkeiten) erteilt oder sperrt das System dann das Nutzungsrecht für ein Objekt (oder eine Gruppe von Objekten) auf Basis einer entsprechenden ACL. Beispielsweise nutzt das Microsoft Active Directory (AD) diesen Ansatz.

Es ist wichtig darauf hinzuweisen, dass es bei RBAC zwar auch eine Rechtevererbung (auf Basis von Gruppenzugehörigkeiten oder Rollenhierarchien), aber keine Rollenvererbung gibt. Der Grund dafür ist, dass bei RBAC sich die Unterteilung der Nutzer danach richtet, in welcher Rolle, also in Ausübung welcher Aufgaben, sie ein spezifisches Nutzungsrecht benötigen, und dass für die Ausübung einer Aufgabe nur die minimal notwendigen Nutzungsrechte gelten sollen.

Ein Beispiel soll dies verdeutlichen: In der Arztpraxis Dr. med. Heilemacher könnte man die Rollen Praxisinhaber (PI), Praxispersonal (PP) und Dienstleister (DL) definieren, wobei sinnvollerweise die Rolle PI die Rolle PP umfasst. Für Notfälle mag dem Praxisinhaber neben der Rolle PI auch die Rolle eines DL fest zugeordnet sein, damit er gegebenenfalls auch Wartungsaufgaben durchführen kann. Dies bedeutet aber nicht, dass er in seiner Rolle als PI Wartungsaufgaben durchführen kann. Er muss dazu explizit die Rolle PI ablegen und die Rolle DL annehmen, was – typisch – ein Abmelden als PI und dann ein Anmelden als DL erfordert. In der Rolle PI sind Wartungsaufgaben NICHT durchführbar, sehr wohl aber alle Aufgaben, die der Rolle PP zugeordnet sind.

3.2 Modelle der IT-Sicherheit

Für eine feingranulare Steuerung von Nutzungsrechten sind die bisher vorgestellten Ansätze manchmal nicht ausreichend. So ist beispielsweise die Anforderung „Labordaten der letzten drei Kalenderjahre dürfen nur vom Praxisinhaber gelöscht werden“ nicht unmittelbar abbildbar. In solchen Fällen können aber Modelle der IT-Sicherheit helfen.

In den folgenden Abschnitten werden zwei derartige Modelle der IT-Sicherheit skizziert, und zwar

- das Bell-LaPadula-Modell mit dem Sicherheitsziel der Vertraulichkeit von gemeinsam genutzten Objekten und
- das Biba-Modell mit dem Sicherheitsziel der Integrität von Objekten.

Bei beiden Modellen, also Bell-LaPadula und Biba, ist es wichtig zu berücksichtigen, dass es sich um Modelle handelt, die nicht automatisch „richtig“ sind, sondern die Grundkonzepte beschreiben, die in bestimmten Situationen angewendet werden können, in anderen nicht. In ihrer Reinform passen sie nur sehr selten, denn auch in einer militärischen Organisation müssen beispielsweise Informationen auch „nach unten“ fließen können. Man muss die Modelle daher als Ausgangspunkt nehmen und dann punktuell öffnen, mit dem Risiko, dass dann die nachweisbaren Sicherheitseigenschaften nicht mehr vollumfänglich gelten.

Es gibt zahlreiche weitere Modelle der IT-Sicherheit (Chinese Wall, BMA, Clark-Wilson, ...) für die verschiedensten Sicherheitsziele und IT-Verbünde, diese zwei sind daher nur als einfache Beispiele zu verstehen. Sie helfen aber trotz ihrer Einfachheit beispielsweise schon erheblich, um gewisse Regeln einer IT-Sicherheitsstrategie mit geringem Aufwand zu forcieren.

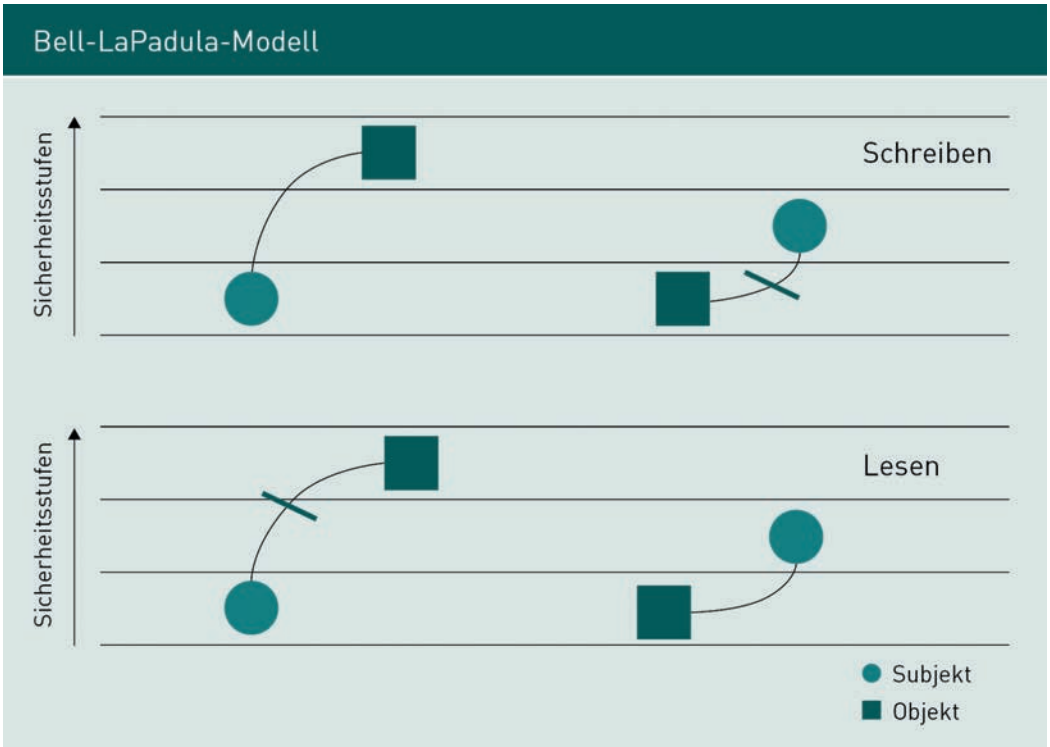
Bell-LaPadula

Die Idee von Bell und LaPadula besteht darin, Festlegungen der Nutzungsrechte in einer ACL um eine generelle Zugriffsregel zu erweitern, die bei jedem Zugriff eines Nutzers auf ein Objekt ebenfalls durchgesetzt wird. Dazu werden Nutzer und Objekte in Sicherheitsstufen eingeteilt, die in einer Ordnung zueinanderstehen, das heißt, dass sie gleich sind oder die eine „höher“ als die andere ist. Sie spiegeln bei Bell-LaPadula für Objekte eine Einstufung hinsichtlich der Vertraulichkeitsanforderungen wider. Beispiele von derartigen Sicherheitsstufen für Patientendaten sind etwa „öffentlich<individuell<privat<intim“, je nachdem welcher Sphäre diese Daten entstammen. Beim Militär o. ä. findet man z. B. Sicherheitsstufen wie „öffentlich<vertraulich<geheim<streng geheim“.

Jeder Nutzer und jedes Objekt erhält dann eine Sicherheitseinstufung anhand der Sicherheitsstufen; dem Nutzer wird also eine Clearance und dem Objekt eine Classification zugeordnet.

Der angestellte Arzt in der Praxis Dr. med. Heilemacher darf zum Beispiel bis zur Sicherheitsstufe „privat“ Dokumente lesen, aber keine Dokumente der Sicherheitsstufe „intim“. Damit hat er die Sicherheitsstufe „privat“. Er hätte dann eine höhere Sicherheitsstufe als ein Drucker der Arztpraxis, der nur „öffentliche“ und „individuelle“ Dokumente drucken darf, aber keine „privaten“ oder „intimen“, da er die Sicherheitsstufe „individuell“ hat.

Mit Bezug auf derartige Sicherheitseinstufungen wird bei Bell-LaPadula die Regel festgelegt, dass ein Subjekt nur Objekte niedrigerer oder gleicher Sicherheitseinstufung lesen (no-read-up) und nur Objekte höherer oder gleicher Einstufung schreiben darf (no-write-down).



Der oben genannte, angestellte Arzt dürfte zum Beispiel bei Anwendung von Bell-LaPadula alle Ausgaben des erwähnten Druckers lesen, aber nichts auf diesem Drucker drucken. Damit wird verhindert, dass irgendwelche Objekte Nutzern niedrigerer Sicherheitseinstufungen zur Kenntnis kommen können. Hierdurch wird die Vertraulichkeit in (vor allem) hierarchisch organisierten Arbeitsumgebungen, wie zum Beispiel beim Militär, geschützt.

Das Bell-LaPadula-Modell wird meist mithilfe von MAC durchgesetzt. In seiner Wirkung verhindert es dann aufgrund der MAC ausdrücklich und wirkungsvoll den Informationsfluss „von oben nach unten“.

Ein praktisches Problem von IT-Verbünden, die Bell-LaPadula einsetzen, besteht darin, dass gelegentlich Objekte von einem höher eingestuften Nutzer gelesen, verändert und zurückgeschrieben werden. Dieses zurückgeschriebene Objekt muss dann automatisch

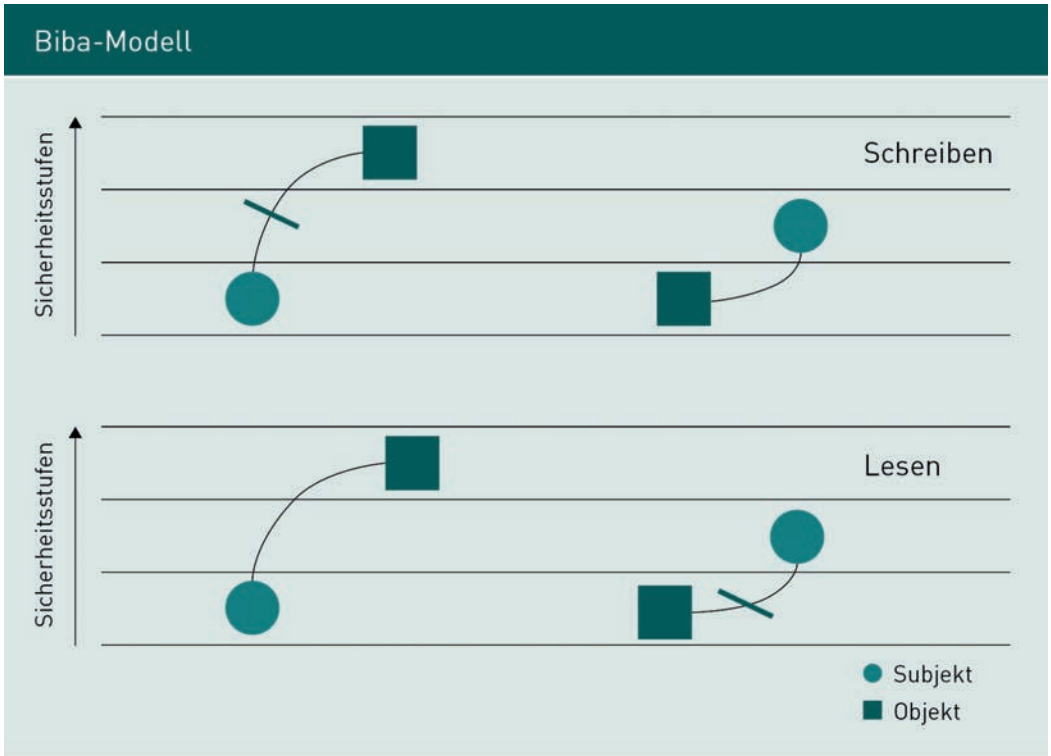
auf die Schutzstufe dieses Nutzers hochgestuft werden. Objekte können also durch den laufenden Betrieb automatisch hoch-, aber nicht heruntergestuft werden. Daher wandern mit der Zeit mehr und mehr Objekte nach oben und werden dem Zugriff der darunter angeordneten Nutzer entzogen, bis schließlich der IT-Verbund oft nicht mehr funktionsfähig ist. Dann müssen von Hand alle die Objekte wieder herabgestuft werden, die „unten“ gebraucht werden.

Im Beispiel der Arztpraxis kann der Praxisinhaber beim Einsatz von Bell-LaPadula einem niedriger eingestuften Subjekt kein Objekt zum Lesen zukommen lassen. Damit sind etwa schriftliche Weisungen des Praxisinhabers an Mitarbeiter nur möglich, wenn eine manuelle Anpassung der Sicherheitsstufe erfolgt.

Biba

Auch das Biba-Modell verwendet Sicherheitseinstufungen wie bei dem Bell-LaPadula-Modell, der Fokus liegt hier aber auf der Integrität der Objekte. Das Biba-Modell stellt sozusagen eine Umkehrung des Bell-LaPadula-Modells dar: Hier werden Objekte nicht vor der Kenntnisnahme, sondern vor der Manipulation durch Unbefugte geschützt.

Wird nämlich unterstellt, dass eine höhere Sicherheitseinstufung auch eine höhere Integrität bedeutet, so wird beim Biba-Modell die Regel festgelegt, dass ein Subjekt nur Objekte niedrigerer oder gleicher Sicherheitseinstufung schreiben (no-write-up) und nur Objekte höherer oder gleicher Einstufung lesen darf (no-read-down).



Hat eine Praxisangestellte etwa die Einstufung „individuell“, dann kann sie bei Anwendung von Biba ein „privates“ Gutachten des angestellten Arztes lesen, jede von ihr veränderte oder auch nur unter einem anderen Namen gespeicherte Version ist aber maximal nur noch „individuell“, hat also eine niedrigere Einschätzung bezüglich der Integrität.

Das Biba-Modell wird beispielsweise seit Windows Vista bei allen Microsoft-Windows-Desktopbetriebssystemen unter dem Namen MIC (Mandatory Integrity Control) mit den Sicherheitsstufen: Low, Medium, High und System verwendet, da es ja bei Systemdateien vor allem auf Integrität und weniger auf Vertraulichkeit ankommt.

3.3 Rechtliche Vorgaben der IT-Sicherheit

Ziel dieses Lernzyklus ist es, meist tabellarisch einen knappen Überblick über einige derzeit bestehende Schutzpflichten zu geben, die gesetzlich für Betreiber von IT-Verbünden gelten. Soweit diese zivilrechtlich begründet sind, führen sie bei schuldhafter Verletzung zur Haftung des Verantwortlichen. Anforderungen aus dem Strafrecht können bei schuldhafter Verletzung Geldbußen oder Freiheitsstrafen nach sich ziehen.

Das Strafgesetzbuch (StGB) enthält u. a. die folgenden Vorschriften, die das genannte Fehlverhalten teils erheblich sanktionieren:

Schutzziele der IT-Sicherheit und zugehörige Vorschriften des StGB	
Vertraulichkeit	§ 202a StGB Ausspähen von Daten § 202c StGB Vorbereiten des Ausspähens und Abfangens von Daten § 203 StGB Verletzung von Privatgeheimnissen
Integrität	§ 263a StGB Computerbetrug § 265a StGB Erschleichen von Leistungen § 268 StGB Fälschung technischer Aufzeichnungen § 269 StGB Fälschung beweiserheblicher Daten § 270 StGB Täuschung im Rechtsverkehr bei Datenverarbeitung § 303a StGB Datenveränderung
Verfügbarkeit	§ 303b StGB Computersabotage

Besondere Bedeutung hat § 202a StGB. Darin ist das „Ausspähen von Daten“ unter Strafe gestellt: „Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft“.

Um eine Zugangssicherung handelt es sich schon, wenn diese den Zugang zu den Daten nicht nur unerheblich erschwert. Das Gesetz verlangt bewusst nicht, dass Zugangssicherungen erst mit einem bestimmten Aufwand oder bestimmten IT-Kenntnissen überwunden werden können. Schon das Verschließen eines Raumes reicht aus. Nur wenn jedermann ohne Weiteres eine Zugangssicherung überwinden kann, genügt sie nicht mehr.

Daneben regelt § 202c StGB beispielsweise den Umgang mit Hackertools und Schadsoftware. Auch wenn diese nur zu Test- oder Prüfzwecken beschafft oder erstellt werden, ist besondere Sorgfalt geboten. Solche Software sollte an niemanden weitergegeben werden, wenn nicht sicher ist, dass er oder sie die Software nur zu genehmigten Testzwecken einsetzen will. Eine Weitergabe sollte nur an bekannte und zuverlässige Dritte erfolgen. Keinesfalls sollte solche Software einem unbestimmten Empfängerkreis etwa im Internet zugänglich gemacht werden.

Auch zum Schutz personenbezogener Daten sind im Bereich IT-Sicherheit technische und organisatorische Maßnahmen zwingend erforderlich. Folgerichtig wurden im BDSG a.F. für IT-Verbünde, die personenbezogene Daten erheben oder verwenden, nachfolgende Verpflichtungen festgelegt, die auch als die „8 Gebote“ des Datenschutzes bekannt sind. Implizit sind diese acht Gebote auch in Art. 24 der DSGVO enthalten. Es gilt danach [Hervorhebungen durch den Autor],

1. „Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren **(Zutrittskontrolle)**,
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können **(Zugangskontrolle)**,
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können **(Zugriffskontrolle)**,
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist **(Weitergabekontrolle)**,
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind **(Eingabekontrolle)**,
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können **(Auftragskontrolle)**,
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind **(Verfügbarkeitskontrolle)**,
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können“ **(Trennungsgebot/Zweckbindungsgebot)**.

Eine zu erwägende Maßnahme bei Nummer 2, 3 und 4 ist dabei ausdrücklich die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

So muss gemäß Nummer 1 die Arztpraxis Dr. med Heilemacher mithilfe geeigneter baulicher, technischer, organisatorischer und personeller Maßnahmen verhindern, dass Unbefugte Zutritt zum Serverraum (R1) haben, da dort personenbezogene Daten verarbeitet werden. Die Sicherung dieses Serverraums könnte etwa durch Sicherheitsschlösser, Chipkartenleser, Codeschlösser, Sicherheitsverglasung und Alarmanlagen erfolgen.

Das IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) ist ein im Juli 2015 in Kraft getretenes Gesetz. Mit dem Gesetz werden insbesondere die Betreiber besonders gefährdeter Infrastrukturen (sogenannte **Kritische Infrastrukturen**) wie Energie, Wasser, Gesundheit oder Telekommunikation verpflichtet, ihre IT-Verbünde besser zu schützen. Neben der obligatorischen Meldung von IT-Sicherheitsvorfällen werden Mindeststandards für die IT-Sicherheit bei den Betreibern solcher IT-Verbünde festgelegt. Dazu sollen die jeweiligen Branchen selbst solche Standards entwickeln, die dann vom BSI genehmigt werden müssen. Danach sollen die Unternehmen alle zwei Jahre nachweisen, dass sie die Anforderungen noch erfüllen.

Kritische Infrastrukturen (KRITIS)
Diese sind laut Bundesinnenministerium „Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden".

Das IT-Sicherheitsgesetz beantwortet jedoch noch nicht die Frage, welche Unternehmen konkret als Kritische Infrastrukturen im Sinne des Gesetzes gelten. Das Gesetz definiert diese lediglich abstrakt. Für die Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation, Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr wurden mit der **KRITIS**-Verordnung Anlagenkategorien und Schwellenwerte definiert, welche Anlagen als kritische Infrastrukturen gelten. Dabei werden Schwellenwerte vielfach so definiert, dass sie etwa 500.000 Nutzern oder Kunden entsprechen.

Das IT-Sicherheitsgesetz hat aber auch noch andere Konsequenzen, die sich in Änderungen bzw. Ergänzungen bestehender Gesetze widerspiegeln. So gelten beispielsweise jetzt für Betreiber von gewerblichen Webangeboten (etwa Online-Shops) erhöhte Anforderungen an die technischen und organisatorischen Maßnahmen zum Schutz ihrer Kundendaten und der von den Kunden genutzten IT-Systeme (§ 13 (7) TMG). Eine hierzu explizit geforderte Maßnahme ist die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens, soweit dies technisch möglich und wirtschaftlich zumutbar ist. Auch DSL-Anbieter sind beispielsweise jetzt verpflichtet, ihre Kunden zu warnen, wenn sie bemerken, dass der Anschluss des Kunden für IT-Angriffe missbraucht wird. Gleichzeitig müssen sie ihre Kunden auf mögliche Wege zur Beseitigung dieser Störung hinweisen.

Zusammenfassung

Ein bewährtes Vorgehen zur Durchsetzung von Sicherheitsanforderungen in der IT ist die Verwendung von Zugriffskontrolllisten (ACL). Hiermit sind Nutzungsrechte für Objekte effizient bestimmbar und Rechterücknahmen meist einfach realisierbar. Zudem sind sie einfach zu implementieren. Ein Nachteil ist die schlechte Skalierbarkeit.

ACLs können entsprechend der DAC- oder MAC-Philosophien verwendet werden. In der ACL können Nutzer- oder Gruppenrechte für Objekte oder Objektgruppen aufgeführt sein. Eine weitere Variante ist die Nutzung von Rollen (RBAC). Bei Gruppen besteht eine Rechtevererbung, bei Rollen wird ausdrücklich eine Rollenvererbung ausgeschlossen.

Durch Einführung von Sicherheitsstufen kann eine ACL durch Regeln ergänzt werden. Die Regeln des Bell-LaPadula-Modells, also no-read-up und no-write-down, unterstützen dann effektiv das Schutzziel Vertraulichkeit. Das Biba-Modell mit den Regeln no-write-up und no-read-down unterstützt das Schutzziel Integrität.

Rechtliche Regelungen mit Einfluss auf die IT-Sicherheit finden sich u. a. im StGB, dem BDSG, dem TMG und dem IT-Sicherheitsgesetz. Sie sanktionieren Fehlverhalten, verpflichten zu technischen und organisatorischen Maßnahmen bei der Verarbeitung von personenbezogenen Daten und sorgen für Transparenz und verpflichtenden Sicherheitsmaßnahmen bei kritischen Infrastrukturen.

Wissenskontrolle

Haben Sie diese Lektion verstanden?

Dann haben Sie jetzt die Möglichkeit, das Gelernte auf unserer Lernplattform zu überprüfen.

Viel Erfolg!

Kritische Infrastrukturen (KRITIS)
Diese sind laut Bundesinnenministerium „Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“.

Lektion 4

Standards und Normen der IT-Sicherheit

LERNZIELE

Nach der Bearbeitung dieser Lektion werden Sie wissen, ...

... welche wichtigen Standards und Normen mit Bedeutung für die IT-Sicherheit es gibt.

... welche Inhalte dieser Standards und Normen im betrieblichen Alltag wichtig sind.

4. Standards und Normen der IT-Sicherheit

Einführung

Herausgegeben und aktualisiert werden die Standards und Normen für die IT-Sicherheit häufig von der International Organization for Standardization (kurz ISO) und der International Electrotechnical Commission (kurz IEC).

Dabei ist zu beachten, dass die hier gezeigten Inhalte lediglich eine Momentaufnahme sind. Der Fortschritt – vor allem im technischen Bereich – verlangt, dass auch Normen und Standards regelmäßig weiterentwickelt werden müssen. Eine Anwendung der Standards und Normen bedarf daher stets einer genauen Untersuchung, inwieweit eine inhaltliche Vorgabe zu einem bestimmten Zeitpunkt noch geeignet, erforderlich oder angemessen ist.

4.1 Grundlegende Standards und Normen

Im Gegensatz zu spezifischen Vorgaben, bei denen vor allem technische Verfahren für den Schutz der IT sorgen, beschreiben grundlegende Standards und Normen Prozesse, Arbeitsanweisungen, Maßnahmen und /oder Richtlinien, mit denen Institutionen aus eigenem Antrieb heraus versuchen können, die IT-Sicherheit zu erhöhen. Die Umsetzung und Einhaltung obliegt dabei in der Regel den beteiligten Personen und wird meist durch spezifische Standards und Normen unterstützt. Regelmäßige Kontrollen und Schulungen sorgen dann für eine „korrekte“ Implementierung der geplanten Maßnahmen.

ISO/IEC 27000-Reihe (ISO27K)

Bei der ISO/IEC 27000-Reihe (oft auch nur kurz ISO27K genannt) handelt es sich um die wichtigste Familie von grundlegenden Standards der IT-Sicherheit. Einen Überblick über die wichtigsten Normen dieser Reihe im März 2021 gibt die nachfolgende Liste:

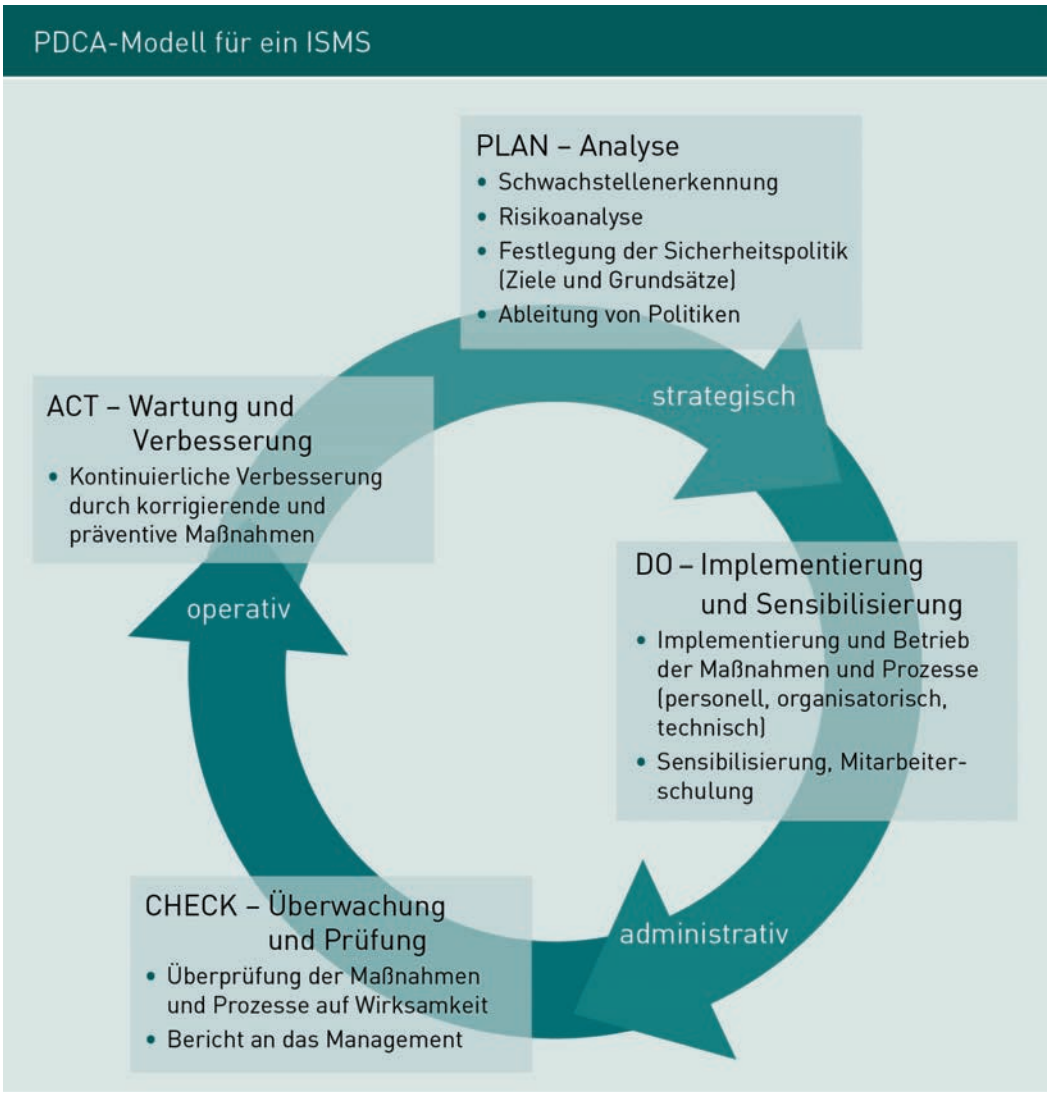
- ISO/IEC 27000:2018 – Information security management systems – Overview and vocabulary
- ISO/IEC 27001:2013 – Information security management systems – Requirements
- ISO/IEC 27002:2013 – Code of practice for information security controls
- ISO/IEC 27003:2017 – Information security management system - Guidance
- ISO/IEC 27004:2016 – Information security management – Monitoring, measurement, analysis and evaluation
- ISO/IEC 27005:2018 – Information security risk management
- ISO/IEC 27006:2015 – Requirements for bodies providing audit and certification of information security management systems

- ISO/IEC 27007:2020 – Guidelines for information security management systems auditing
- ISO/IEC 27018:2019 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Die ISO/IEC 27001 ist dabei die wichtigste Norm in der ISO/IEC 27000-Reihe. Sie definiert u. a. die wesentlichen Anforderungen an ein IT-Sicherheit-Managementsystem (ISMS) und kann daher als einziger aus der Normenreihe die Grundlage einer entsprechenden Zertifizierung bilden. Sie ist prozessorientiert und dient der Einrichtung, Umsetzung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung eines ISMS. Dieser prozessorientierte Ansatz umfasst folgende Punkte:

- Verständnis der Anforderungen an eine Organisation der IT-Sicherheit und die Notwendigkeit, eine Leitlinie und Ziele für die IT-Sicherheit festzulegen.
- Umsetzung und Einsatz von Maßnahmen, um die Risiken der IT-Sicherheit einer Institution integrativ mit den allgemeinen Geschäftsrisiken einer Institution zu verwalten.
- Überwachung und Überprüfung der Leistung und Wirksamkeit des ISMS.
- Ständige Verbesserung des ISMS auf Basis von objektiven Messungen.

Er wird häufig – aber nicht zwingend – mittels eines PDCA-Modells (Demingkreis) abgebildet:



Dieses klassische Vorgehensmodell („Demingkreis“) dient bekanntlich allgemein einer Strukturierung des Verstehens und des Verbesserns in einen iterativen, mehrphasigen Prozess. Hierfür übernimmt es im konkreten Fall die Anforderungen von vorgelagerten Phasen und liefert dann IT-Sicherheit als Ergebnis der Aktionen und Prozesse, die durchgeführt wurden.

Die ISO/IEC 27002 ist ein ergänzender Leitfaden für das Management von IT-Sicherheit, aber keine Spezifikation. Sie dient allein dem besseren Verständnis der in der ISO/IEC 27001 definierten Anforderungen und als Basis zur Entwicklung von institutionseigenen Verfahren und Regelungen. Dazu bietet er eine Auswahl von Maßnahmen, gegliedert in zurzeit 14 Sicherheitskategorien, 35 Maßnahmenziele und 114 Maßnahmen.

IT-Grundschutz (IT-GS)

IT-Grundschutz (IT-GS) ist ein allgemeiner Standard mit Bezug zu Datenschutz und IT-Sicherheit, der vom BSI Mitte der 1990er-Jahre entwickelt und in 2017 grundlegend modernisiert wurde. Diese Modernisierung bedeutet eine Konzentration auf mittlere Institutionen und umfasst vornehmlich alternative Vorgehensweisen sowie eine Verschlankung der Bausteine.

Ein vollständiger Einsatz von IT-GS liefert …

- … Methoden und Verfahren zur schrittweisen Einführung eines ISMS.
- … Hilfestellungen zu allen Phasen des IT-Sicherheit-Prozesses.
- … bewährte Lösungen aus der Praxis („Best Practice").
- … abgestufte Möglichkeiten der Zertifizierung nach ISO/IEC 27001.

IT-GS stellt hierzu Methoden und Hilfestellungen zur Verfügung, mit denen Institutionen einen IT-Verbund zunächst dokumentieren und dann angemessene Sicherheitsmaßnahmen auswählen können.

Dabei wird im Regelfall nur auf die bewährten und erprobten Standard-Sicherheitsmaßnahmen für Komponenten zurückgegriffen, die einen normalen Schutzbedarf haben. Typischerweise sind dies Maßnahmen, die für den konkreten IT-Verbund stets erforderlich sind, also z. B. Schutzmaßnahmen gegen Feuer, Diebstahl, Schadsoftware oder Hardware-Defekte. Lediglich in den Fällen, wo diese nicht ausreichen, werden gegebenenfalls weitere Maßnahmen auf Basis einer ergänzenden Sicherheitsanalyse identifiziert. Letzteres ist erfahrungsgemäß für nur 20 % oder weniger der Komponenten erforderlich.

Der IT-GS gestattet sogar anfänglich den vollständigen Verzicht auf eine Feststellung des Schutzbedarfs. Beispielsweise kann dann eine Institution zunächst (möglichst) flächendeckend alle Standard-Sicherheitsmaßnahmen umsetzen, um so die größten Risiken zu senken, bevor tatsächliche Sicherheitsanforderungen im Detail analysiert werden.

Das IT-GS-Prozessmodell beruht ebenfalls auf dem Demingkreis und unterstützt somit das kontinuierliche Verstehen und Verbessern des Vorgehens.

Prinzipiell kann IT-GS in Institutionen jeder Art und Größe eingesetzt werden. Vor allem für kleine und mittlere Unternehmen gibt es jedoch auch angepasste Ansätze (vgl. etwa ISIS12, das vom Netzwerk Informationssicherheit im Mittelstand [NIM] des Bayerischen IT-Sicherheitscluster e. V. für mittelständische Unternehmen und Organisationen entwickelt wurde).

Unternehmen, die IT-GS konsequent einsetzen, können ihren IT-Verbund nach ISO/IEC 27001 zertifizieren lassen.

Formal umfasst IT-GS die BSI-Standards, das IT-Grundschutz-Kompendium (als Ablösung der IT-Grundschutz-Kataloge) sowie den neuen Leitfaden Basisabsicherung.

Die BSI-Standards enthalten Beschreibungen der empfohlenen Methoden, Prozesse, Verfahren und Vorgehensweisen. Das IT-Grundschutz-Kompendium enthält Beschreibungen der Komponenten mit ihren Gefährdungen und Sicherheitsanforderungen.

BSI-Standards
Die ursprüngliche Reihe der BSI-Standards 100-x wurde im Rahmen der Modernisierung abgelöst durch die neuen BSI-Standards 200-x.

- **BSI-Standard 200–1: Managementsysteme für Informationssicherheit** (vgl. Bundesamt für Sicherheit in der Informationstechnik 2017a):
  - Dieser Standard definiert die generellen Anforderungen an ein ISMS für die IT-GS- Vorgehensweise. Er bewegt sich im Rahmen der ISO/IEC 27001 und berücksichtigt zahlreiche Empfehlungen der ISO/IEC 27002. Er bietet eine leicht verständliche und systematische Anleitung, unabhängig davon, mit welchen Methoden die Anforderungen umgesetzt werden.
- **BSI-Standard 200–2: IT-Grundschutz-Methodik** (vgl. Bundesamt für Sicherheit in der Informationstechnik 2017b):
  - Dieser Standard enthält eine praxiserprobte Anleitung, wie ein ISMS gemäß BSI-Standard 200–1 in der Praxis umgesetzt werden kann. Dabei wird neben der eigentlichen Vorgehensweise auch der Aufbau einer Organisationsstruktur für die IT-Sicherheit behandelt.
- **BSI-Standard 200–3: Risikoanalyse auf der Basis von IT-Grundschutz** (vgl. Bundesamt für Sicherheit in der Informationstechnik 2017c):
  - Wird im Rahmen von BSI-Standard 200–2 die Entscheidung für eine ergänzende Sicherheitsanalyse getroffen, bietet dieser Standard hierfür eine effektive und effiziente Methode.
- **BSI-Standard 100–4: Notfall-Management** (vgl. Bundesamt für Sicherheit in der Informationstechnik 2008):
  - Dieser Standard beschreibt eine Methodik zur Etablierung eines Notfallmanagements. Er basiert auf dem bisherigen BSI-Standard 100–2 und ergänzt diesen wo notwendig.

IT-Grundschutz-Kompendium
Das Kompendium gliedert sich, nach einführenden Beschreibungen, in die folgenden Elemente (vgl. Bundesamt für Sicherheit in der Informationstechnik 2018):

- Rollendefinition,
- Glossar,
- Elementare Gefährdungen,
- Bausteine
  - Prozess-Bausteine,
  - System-Bausteine.

In der ersten Edition des Kompendiums sind rund 80 Bausteine enthalten, die jeweils aus einer kurzen Beschreibung, Verweisen auf die relevanten Gefährdungen und den zugehörigen Sicherheitsanforderungen auf den drei Ebenen Basis-, Kern- und Standardabsicherung sowie Anforderungen für einen hohen Schutzbedarf bestehen. Die Basisanforderungen sind als Minimalanforderungen definiert. Die Kernanforderungen dienen der selektiven Absicherung von besonders wichtigen Prozessen und Systemen, im IT-Grundschutz auch als „Kronjuwelen" bezeichnet. Diese Anforderungen werden durch die Standardanforderungen erweitert, um ein im Normalfall angemessenes Sicherheitsniveau zu erreichen, wie es beispielsweise für eine Zertifizierung nach ISO/IEC 27001 erforderlich ist. Schließlich enthalten die modernisierten Bausteine auch ausgewählte Sicherheitsanforderungen bei hohem Schutzbedarf.

Anders als in den IT-Grundschutz-Katalogen enthalten die Bausteine im Kompendium keine Beschreibungen der Sicherheitsmaßnahmen mehr, sondern konzentrieren sich auf die zu erfüllenden Anforderungen.

ISO/IEC 20000–1

Diese Norm ist eng verwandt mit ITIL, einem verbreiteten Referenzmodell für das IT-Servicemanagement, und spezifiziert Anforderungen an (interne oder externe) IT-Organisationen hinsichtlich der Erbringung von prozessorientierten Dienstleistungen (IT-Servicemanagement). Mehrere der darin geforderten Prozesse (vor allem Information Security Management, Incident Management, Event Management und Service Continuity Management) haben Überschneidungen mit der ISO/IEC 27001. Typisch wird die ISO/IEC 20000–1 lediglich auf IT-Bereiche angewandt, während der Anwendungsbereich der ISO/IEC 27001 alle Arten von Institutionen umfasst.

ISO 22301

Die Norm ISO 22301 beschäftigt sich mit der Sicherstellung der geschäftlichen Kontinuität (Business Continuity Management [BCM]) und spezifiziert Anforderungen an BCM-Systeme in Institutionen. BCM-Systeme nach ISO 22301 haben auch (aber nicht nur) einen IT-Bezug. Mit dem Thema BCM beschäftigt sich auch ein Themenbereich der ISO/IEC 27001, allerdings nur aus der Perspektive der IT-Sicherheit (d. h., inwiefern die Geschäftstätigkeit durch IT-Sicherheitsvorfälle gefährdet werden kann).

ISO 9001

Diese Norm spezifiziert allgemeine Anforderungen an Qualitätsmanagementsysteme, hat aber auch viele Bezüge zur IT-Sicherheit, beispielsweise bezüglich der Pflichten

- zum Schutz der immateriellen Güter (Betriebsgeheimnisse, ...),
- zur Sicherstellung der Verfügbarkeit von IT-Anwendungen,

- hinsichtlich Kennzeichnung, Aufbewahrung, Schutz und Wiederauffindbarkeit von (elektronischen) Dokumenten sowie
- zur Ermittlung, Bereitstellung und Aufrechterhaltung der infrastrukturellen Komponenten.

COBIT

Das Rahmenwerk COBIT – ein Kunstwort, das ursprünglich einmal von „Control Objectives for Information and Related Technology" abgeleitet wurde – beschreibt eine von Anspruchsgruppen („Stakeholder") getriebene Methodik für Governance und Management von IT. Es beschreibt primär allerdings nicht, wie etwas umzusetzen ist, sondern vielmehr was umzusetzen ist. Zu diesem Zweck stellt die Version COBIT 2019 ein sogenanntes Kernmodell bereit, strukturiert in Domänen, die jeweils eine Reihe von „Governance- und Management-Designzielen" enthalten. COBIT beschränkt sich dabei nicht auf Datenschutz und IT-Sicherheit, sondern propagiert ein einheitliches, integriertes Rahmenwerk für alle IT-Prozesse durch Berücksichtigung der fünf Domänen:

- **EDM** (Evaluate, Direct, Monitor) – „Evaluieren, Vorgeben und Überwachen"
- **APO** (Align, Plan, Organise) – „Anpassen, Planen und Organisieren"
- **BAI** (Build, Acquire, Implement) – „Aufbauen, Beschaffen und Implementieren"
- **DSS** (Deliver, Service, Support) – „Bereitstellen, Betreiben und Unterstützen"
- **MEA** (Monitor, Evaluate, Assess) – „Überwachen, Evaluieren und Beurteilen"

Mit den Designzielen APO13 („Managed Security") und DSS05 („Managed Security Services") enthält COBIT konkrete Anforderungen zu Datenschutz und IT-Sicherheit.

APO13 „Managed Security" gehört zur Domäne „Anpassen, Planen und Organisieren", befasst sich also damit, Sicherheit von Anfang an im Aufbau einer IT-Infrastruktur zu berücksichtigen. Die Kernanforderungen sind Aufbau und Pflege eines Informationssicherheits-Managementsystems (ISMS), die Erstellung und Pflege eines Plans für den Umgang mit Risiken in Bezug auf IT-Sicherheit und Datenschutz, und schließlich die regelmäßige Überwachung und Prüfung des ISMS. Diese als Praktiken bezeichneten Kernanforderungen werden im Modell detailliert beschrieben, mit Teilschritten, Verantwortlichkeiten, Ein- und Ausgabedaten etc.

Das Designziel DSS05 setzt sehr viel später im Lebenszyklus an, denn es gehört zur Domäne „Bereitstellen, Betreiben und Unterstützen". Hier geht es also darum, Sicherheit im Betrieb einer IT-Infrastruktur sicherzustellen. Diese Aufgabe wird in die folgenden Praktiken heruntergebrochen, die dann ebenfalls detailliert beschrieben werden:

- Schutz gegen Schad-Software
- Managen der Netzwerk- und Verbindungs-Sicherheit
- Managen der Sicherheit von Endgeräten
- Identitätsmanagement und Management von Zugriffsrechten
- Management des physischen Zugangs zu IT-Komponenten

- Management vertraulicher Dokumente und Ausgabegeräte
- Management von Schwachstellen und Überwachung der Infrastruktur aus sicherheitsbezogenen Ereignissen

Im Gegensatz zu vorherigen Versionen stellt COBIT seit Version 5 auch einen Umsetzungsleitfaden (Implementation Guide) zur Verfügung. Er kann als Grundlage für individuelle Einführungsplanungen dienen und umfasst zahlreiche „Best Practice"-Ansätze u.a. zum Thema der IT-Sicherheit.

Der allgemeine Planungsansatz in COBIT ist Top-down: Zunächst werden die Zielvorgaben für die IT aus den Unternehmenszielen und aus der Unternehmensstrategie für die IT abgeleitet. Dabei geht es insbesondere um eine ausreichende Erfüllung der Anforderungen der Anspruchsgruppen, also z. B. auch um die Datenschutzbelange von Kunden und Lieferanten.

Auf Basis dieser Zielvorgaben für die IT wird anschließend die Architektur der IT bestimmt. Sie umfasst dann (idealerweise) angemessene IT-Prozesse, für die jeweils Metriken, die die Beurteilung der Zielerreichung gestatten, definiert sind.

4.2 Spezifische Standards und Normen

Spezifische Standards und Normen beschreiben vor allem technische Verfahren, die die Sicherheit ausgewählter Teilbereiche von IT-Verbünden stärken können.

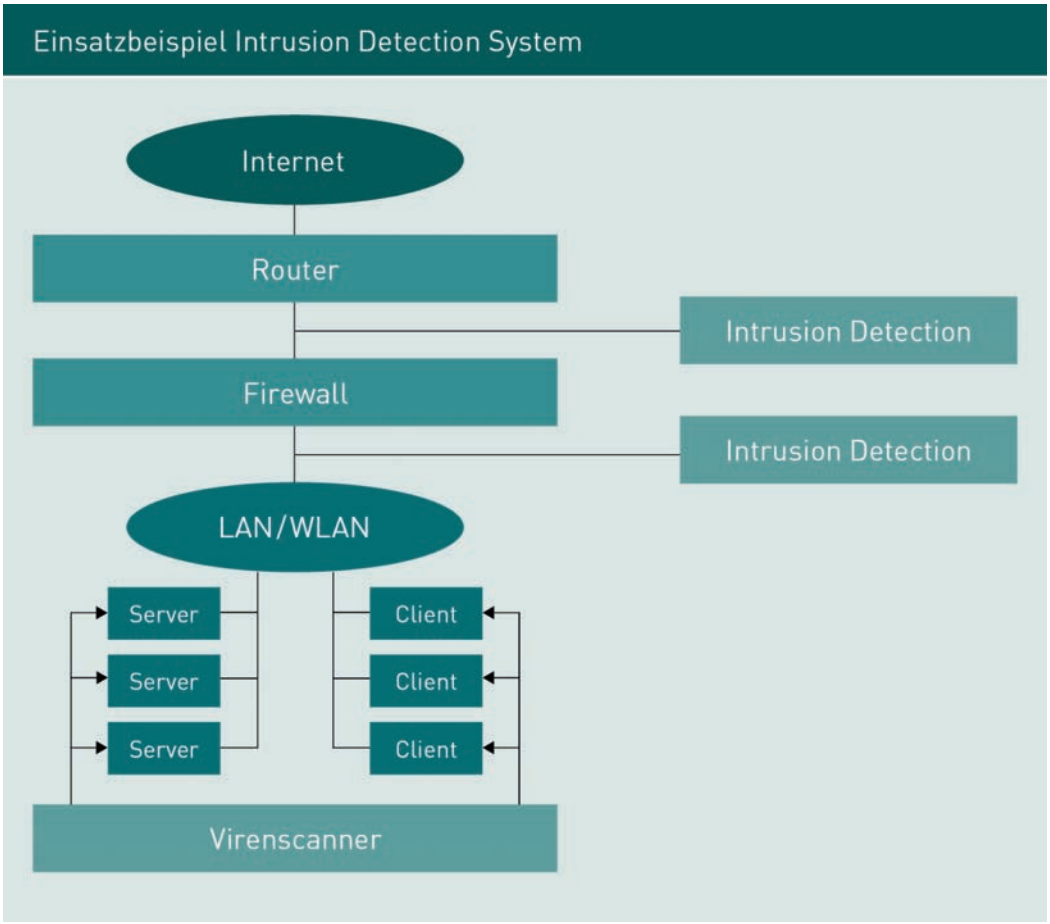
ISO/IEC 27033

Ziel dieses Standards ist es, Netzwerksicherheit für unterschiedliche Zielgruppen einer Institution nachhaltig herzustellen. In den enthaltenen Richtlinien werden Sicherheitsaspekte sowohl bei der Beschaffung von Netzwerken als auch bei der Wartung und beim Betrieb von Netzwerken betrachtet. Verantwortliche für die IT-Sicherheit einer Institution können zahlreiche Inhalte dieses Standards in eigene, spezifische Netzwerkanforderungen leicht integrieren.

ISO/IEC 27039

Diese Norm beschäftigt sich mit der erfolgversprechenden Auswahl und dem zielgerichteten Betrieb eines Systems zur Erkennung eines Eindringens in Netzwerke (Intrusion Detection System [IDS]) und der Reaktion auf ein solches Eindringen (Intrusion Prevention System [IPS]). Die übliche Bezeichnung „Intrusion Prevention System" kann dabei irreführen: Gemeint ist nicht die vorbeugende Prävention eines Eindringens, sondern die schnelle Reaktion auf einen Angriff und damit das Verhindern (Prävention) eines solchen Eindringens in ein System.

Ein IDS sucht – unabhängig von einer Firewall – nach verdächtigen Aktivitäten in Netzwerken:



Gemäß ISO/IEC 27039 sollte man bei einer Neuplanung eines IDS-Einsatzes wie folgt vorgehen:

- **Auswahl:** Die Auswahl sollte vor allem auf einer Analyse basieren, die die Problemzonen eines Netzwerks ermittelt, für die ein IDS erforderlich sein könnte. Daneben müssen natürlich Aufwände – wie beispielsweise Kosten für Anschaffung und Betrieb – bei der Auswahl berücksichtigt werden. Schließlich müssen für die Produkte, die in die engere Wahl kommen, auch Merkmale wie Alarmierungsstrategien (per E-Mail, SMS, ...) und enthaltene Zusatzwerkzeuge bewertet werden, die für den effizienten und effektiven Einsatz eines IDS oft unabdingbar sind.
- **Einsatz:** Für den Einsatz müssen zunächst die Aktivitäten definiert werden, die der Inbetriebnahme des IDS dienen. Dabei müssen auch die verschiedenen Platzierungsmöglichkeiten für ein IDS und die Schutzerfordernisse des IDS geklärt werden.
- **Betrieb:** Der Betrieb eines IDS erfordert die Etablierung der erforderlichen Betriebsprozesse, das Tuning des IDS sowie die Behandlung von Schwachstellen und Alarmierungen.

Für jeden Aspekt dieser drei Vorgehensphasen enthält die Norm ISO/IEC 27039 zahlreiche Erläuterungen und praxiserprobte Lösungsvorschläge.

GoBD

Die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) regeln die Aufbewahrung von handelsrechtlich und steuerrechtlich relevanten Dokumenten in digitaler Form. Die GoBD wurden durch Schreiben des Bundesfinanzministeriums am 14.12.2014 in elektronischer Form publiziert. Sie sind seit dem 01.01.2015 gültig und lösen die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) sowie die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) ab.

Wesentliche Anforderungen der GoBD mit Bezug zur IT-Sicherheit sind die zukünftige Verfügbarkeit und Integrität von digitalen Unterlagen. Bestimmte Formate (etwa WORD-Formate) oder Aufbewahrungsformen (etwa NTFS-Dateisysteme) digitaler Unterlagen erfüllen ohne weitere Maßnahmen nicht die Anforderungen der GoBD.

Hinsichtlich einer Digitalisierung von Papierdokumenten per Scanner verlangen daher die GoBD:

- Der Prozess muss so gestaltet sein, dass alle Seiten vollständig gescannt werden und optisch mit dem Original übereinstimmen.
- Werden gescannte Papierdokumente per Texterkennung (Optical Character Recognition [OCR]) durch Informationen ergänzt (z. B. zu durchsuchbaren PDF-Dateien erweitert), so sind diese Informationen ebenfalls aufzubewahren.
- Ein farbiges Scannen ist nur dann erforderlich, wenn die Farbgestaltung des Papierdokumentes von wesentlicher Bedeutung ist.
- Wird ein Papierdokument nach dem Scannen verändert, so ist dieses erneut zu scannen und ein fester Bezug zum Original zu erzeugen (z. B. durch ein Zusammenführen der Scanergebnisse). Das nachträgliche Anbringen von Vermerken, Barcodes, farblichen Hervorhebungen usw. darf jedoch niemals einen Einfluss auf die Lesbarkeit des Papierdokuments haben.
- Nach dem Einscannen dürfen Papierdokumente prinzipiell entsorgt werden, soweit verbindliche Aufbewahrungsfristen dem nicht entgegenstehen.
- Für die Nutzung von Scannern ist zwingend eine sogenannte Verfahrensdokumentation zu erstellen, die allen beteiligten Mitarbeitern als Arbeitsanweisung und Dritten als Nachweis für die Erfüllung der gesetzlichen Anforderungen dienen kann. Diese Verfahrensdokumentation muss (lt. GoBD Rzn. 136) verbindlich regeln:
  - „wer scannen darf,
  - zu welchem Zeitpunkt gescannt wird (z. B. beim Posteingang, während oder nach Abschluss der Vorgangsbearbeitung),
  - welches Schriftgut gescannt wird,
  - ob eine bildliche oder inhaltliche Übereinstimmung mit dem Original erforderlich ist,

- wie die Qualitätskontrolle auf Lesbarkeit und Vollständigkeit und
- wie die Protokollierung von Fehlern zu erfolgen hat."

Für bereits digital empfangene Dokumente (insbesondere per E-Mail) verlangen die GoBD:

- Digital empfangene Dokumente, die steuer- oder handelsrechtlich von Bedeutung sind, müssen grundsätzlich in dem Format aufbewahrt werden, in dem sie empfangen wurden (also z. B. eine E-Mail – mit oder ohne Anhängen – als EML- oder MSG-Datei). Eine Umwandlung in ein anderes Format (z. B. MSG in PDF) ist nur in Ausnahmefällen zulässig.

Gerade bei empfangenen E-Mails ist aber zu beachten, dass ihre Aufbewahrung stets weiteren gesetzlichen Regelungen unterliegen kann, wie insbesondere Vorschriften aus dem Datenschutzrecht. Häufig kommen dazu noch innerbetriebliche Regelungen in Form von Dienst- oder Betriebsvereinbarungen.

Bei digitalen Ausgangsdokumenten mit steuer- oder handelsrechtlicher Bedeutung gilt laut GoBD:

- Die relevanten Inhalte, nicht ihre optische Gestaltung, müssen langfristig wiederherstellbar sein. Formatierungsinformationen (wie Layout, Zeichensätze, Schriftfarbe, ...) sind nicht reproduktionspflichtig.
- Bildliche Abweichungen zwischen dem ursprünglichen Dokument und der Reproduktion dürfen allerdings eine Einschätzung und Bewertung des Sachverhalts nicht unangemessen erschweren.

Zusammenfassung

Zur Realisierung von IT-Sicherheit wurden vielfältige Standards entwickelt (z. B. ISO/IEC 27K, IT-GS), die kontinuierlich aktualisiert und modernisiert werden. Durch eine Anwendung dieser Standards wird sichergestellt, dass allgemein anerkannte Methoden und Verfahren in die Realisierung von IT-Sicherheit eingehen.

Eine konforme Umsetzung von Standards der IT-Sicherheit ist in der Regel überprüfbar und gelegentlich auch zertifizierbar. Eine Zertifizierung kann dann als Nachweis der Standardkonformität gegenüber Dritten dienen.

Für eine umfassende Zertifizierung der IT-Sicherheit muss die internationale Norm ISO/IEC 27001 verbindlich angewandt werden. Weitere hiermit verwandte Normen bieten wertvolle Hilfen hinsichtlich der Interpretation, des Verständnisses und der Anwendung der Norm ISO/IEC 27001. Beabsichtigt eine Institution eine Konformitätsbewertung gemäß ISO/IEC 27001, so kann sie sich auch für das BSI als Zertifizierungsstelle entscheiden.

Es existieren darüber hinaus Standards, in denen IT-Sicherheit als Teilaspekt oder aus einer bestimmten sachlichen Perspektive betrachtet wird. Dabei bestehen oft inhaltliche Überschneidungen mit den Standards, die IT-Sicherheit im Hauptfokus haben. Für Institutionen sind mit Blick auf die Verfügbarkeit und Integrität von digitalen Unterlagen hier insbesondere die GoBD zu nennen, die dafür sorgen, dass sich ein sachverständiger Dritter jederzeit einen zuverlässigen Überblick über alle vorhandenen, digitalen Informationen verschaffen kann.

Wissenskontrolle

Haben Sie diese Lektion verstanden?

Dann haben Sie jetzt die Möglichkeit, das Gelernte auf unserer Lernplattform zu überprüfen.

Viel Erfolg!

Lektion 5

Erstellung eines IT-Sicherheitskonzeptes auf Basis von IT-Grundschutz

LERNZIELE

Nach der Bearbeitung dieser Lektion werden Sie wissen, ...

- ... wie ein IT-Sicherheitskonzept auf Basis von IT-Grundschutz (IT-GS)
- ... für einen konkreten IT-Verbund erstellt werden kann.
- ... wie der Schutzbedarf ermittelt wird.
- ... was der Basis-Sicherheitscheck umfasst.

5. Erstellung eines IT-Sicherheitskonzeptes auf Basis von IT-Grundschutz

Einführung

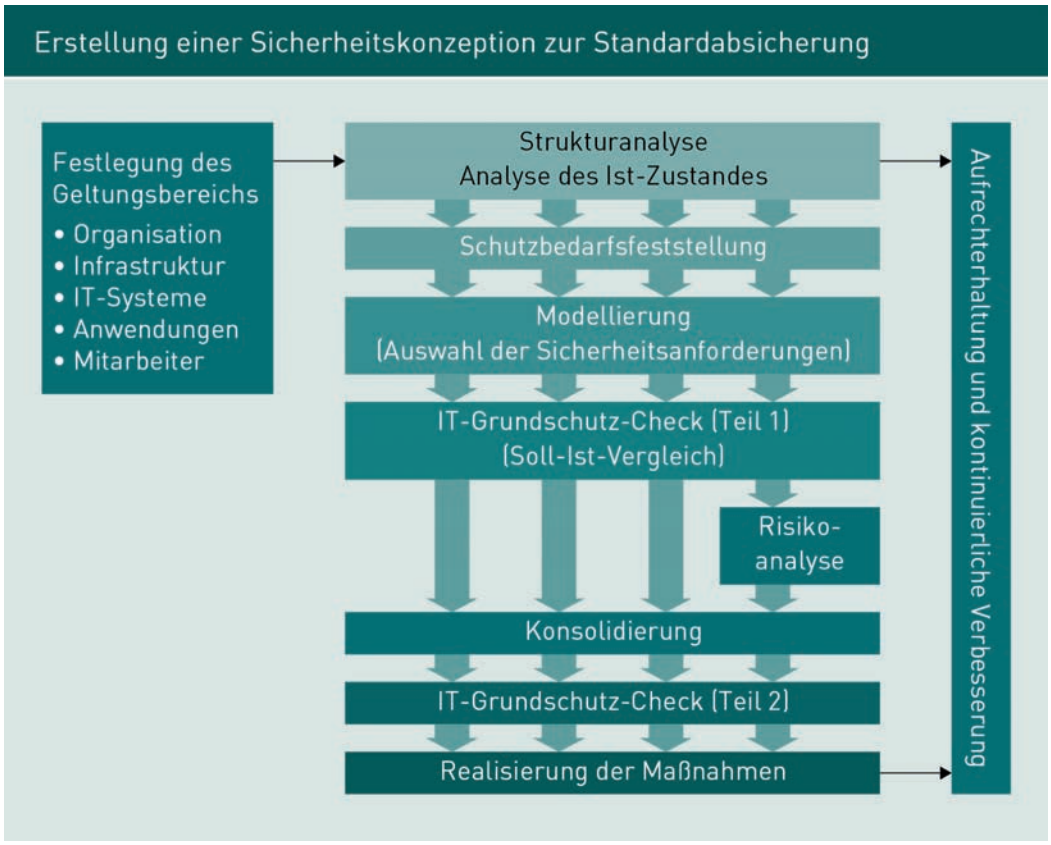
IT-Sicherheit kann offensichtlich nur durch geplantes und organisiertes Vorgehen aller Beteiligten entstehen. Voraussetzung für die sinnvolle Umsetzung und Erfolgskontrolle von entsprechenden Schutzmaßnahmen ist daher ein geplanter und gesteuerter IT-Sicherheitsprozess.

Dieser beginnt gemäß IT-GS mit der Initiierung des IT-Sicherheitsprozesses, der Erstellung einer Leitlinie zur IT-Sicherheit sowie der Festlegung der grundlegenden Organisation für das Management der IT-Sicherheit. Diese beinhaltet sowohl den formalen Aufbau der Organisation als auch die Ressourcenzuteilung inklusive Mitarbeiter.

Nach dieser Initiierung des Sicherheitsprozesses erfolgt die Erstellung des IT-Sicherheitskonzeptes. Die konkreten Schritte dieser Erstellung auf Basis von IT-Grundschutz (IT-GS) für die Standardabsicherung sind Gegenstand dieser Lektion.

Die wesentlichen Schritte lauten im Überblick:

- **Strukturanalyse:** Zunächst werden die wesentlichen Bestandteile (Anwendungen, IT-Systeme, Räume, Gebäude, ...) des IT-Verbundes erfasst. Vorteilhafterweise wird hier mit den Anwendungen begonnen und – darauf aufbauend – werden die weiteren relevanten Objekte identifiziert.
- **Schutzbedarfsfeststellung:** Dann wird für jedes Objekt des IT-Verbundes der Schutzbedarf bezüglich Vertraulichkeit, Verfügbarkeit und Integrität festgelegt. Dieser wird anhand der möglichen Schäden, die durch die Beeinträchtigung der betroffenen Anwendungen möglich sind, bestimmt. IT-GS setzt dabei drei qualitative Schutzbedarfsklassen ein: normal, hoch und sehr hoch. Diese müssen situationsspezifisch von jeder Institution inhaltlich gegeneinander abgegrenzt werden.
- **Modellierung (Auswahl der Sicherheitsanforderungen):** Ausgehend von den Ergebnissen der Strukturanalyse und der Schutzbedarfsfeststellung werden die relevanten Bausteine sowie die relevanten Sicherheitsanforderungen ausgewählt.
- **IT-Grundschutz-Check:** Anschließend erfolgt eine Überprüfung, welche der durch die Modellierung identifizierten Anforderungen bereits erfüllt sind. Daraus ergibt sich, wo noch Handlungsbedarf besteht.
- **Risikoanalyse:** Bei hohem oder sehr hohem Schutzbedarf von Objekten des IT-Verbundes wird eine ergänzende Risikoanalyse durchgeführt, die möglicherweise zusätzlich erforderliche Maßnahmen zum Ergebnis hat. Die Ergebnisse werden gegebenenfalls mit den Ergebnissen der Modellierung konsolidiert und der IT-Grundschutz-Check entsprechend überarbeitet.
- **Realisierung der Maßnahmen:** Ausgehend von den Ergebnissen des IT-Grundschutz-Checks werden die notwendigen Maßnahmen zur Erfüllung der Anforderungen umgesetzt.



Bei der hieran anschließenden Umsetzung des IT-Sicherheitskonzeptes findet zunächst eine Verdichtung der Maßnahmen statt. Dazu werden die aus den Bausteinen abgeleiteten Maßnahmen und die sich aus den gegebenenfalls durchgeführten ergänzenden Sicherheitsanalysen ergebenden Maßnahmen zunächst zusammengeführt. Anschließend wird geprüft, ob und gegebenenfalls wie die verbleibenden umzusetzenden Maßnahmen an den konkreten IT-Verbund angepasst werden müssen. Die abschließenden Aufgaben betreffen vor allem die Zeit- und Kostenplanung der Umsetzungsmaßnahmen.

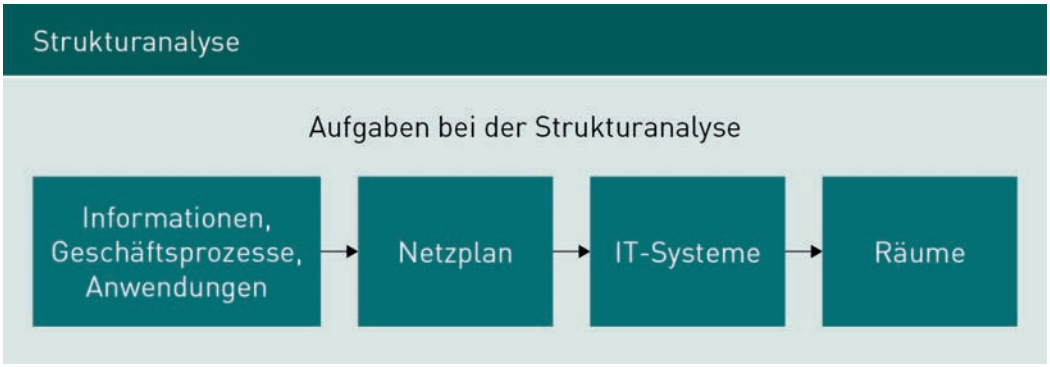
In der geplanten Überarbeitung des IT-GS können die genannten Schritte über sogenannte IT-Grundschutz-Profile für spezifische Anwendungsfelder pauschalisiert angegangen werden, sodass Institutionen (zunächst) schneller in Sachen IT-Sicherheit voranschreiten können.

Die nachfolgenden Erläuterungen orientieren sich eng an Fraunhofer-Institut für Sichere Informationstechnologie (SIT 2010) und Bundesamt für Sicherheit in der Informationstechnik (2017b).

5.1 Strukturanalyse

Die Strukturanalyse eines IT-Verbundes ist laut IT-GS in vier Schritte gegliedert:

1. **Erfassung der Anwendungen:** Um die relevanten Anwendungen zu identifizieren, werden die Geschäftsprozesse, die verarbeiteten Daten und die (befugten) Nutzer ermittelt.
2. **Netzplanerhebung:** Der technische IT-Verbund wird erfasst und in vereinfachter Form dargestellt.
3. **Erhebung der IT-Systeme:** Alle relevanten IT-Systeme des IT-Verbundes werden erfasst und aufgelistet.
4. **Erfassung der Räume:** Bei der Erfassung der Räume werden gegebenenfalls auch externe Räume erfasst, sofern sie für die Analyse relevant sind.



Datenträger, beispielsweise für die Archivierung oder für den Datenaustausch mit Externen, sollten in diesem Kontext als Anwendungen betrachtet werden. Dies gilt mindestens dann, wenn sie schutzbedürftige Informationen enthalten.

Bei allen Teilen der Strukturanalyse kann durch angemessene Gruppenbildung der Zeitaufwand vermindert und es können die Ergebnisse übersichtlicher gestaltet werden. Diese Gruppenbildung von Objekten ist immer dann angezeigt, wenn die Objekte aus Sicht der IT-Sicherheit vergleichbar sind, also insbesondere ähnlichen Gefährdungen ausgesetzt sind.

Für das Beispiel der Arztpraxis bedeutet eine Strukturanalyse demnach konkret, dass die bereits in den Abbildungen zum „Praxisnetz Dr. med. Heilemacher“ sowie den Geräten und Räumen der Arztpraxis detailliert aufgeführten Angaben lediglich ergänzt werden müssen durch eine Liste der Anwendungen nebst den dazu gehörigen Nutzern und durch eine Liste der Abhängigkeiten dieser Anwendungen von den Objekten des IT-Verbundes:

Anwendungen der Arztpraxis

Nr.	Anwendung	Art der Daten	Nutzer
A-1	Praxisverwaltungssystem (PVS)	P	PP, PI
A-2	Archivierungssystem	P	PI

Nr.	Anwendung	Art der Daten	Nutzer
A-3	Externe Archiv-Datenträger	P	PI
A-4	Fernwartungssoftware	S, ggf. P	DL, PI
A-5	Datenaustausch mit Labor	P	PP
A-6	Datenaustausch mit KV	V, (P)	PP
A-7	Datenaustausch mit Privatärztlicher Verrechnungsstelle	P	PP, PI
A-8	Datenaustausch mit Krankenhäusern und anderen Praxen	P	PP, PI
A-9	Kommunikation mit Patienten	P	PP, PI

Legende:
P Patientendaten
(P) Anonymisierte oder pseudonymisierte Patientendaten
S Systemspezifische oder technische Informationen
V Verwaltungsspezifische Daten
PI Verantwortlicher Arzt, Praxisinhaber
PP Praxispersonal
DL Dienstleister für IT

Abhängigkeiten der Anwendungen von Objekten des IT-Verbundes

Nr.	Anwendung	S-1	S-2	C-1	C-2	ITS-1	ITS-2	ITS-3	TK-1	TK-2	N-1
A-1	Praxisverwaltungssystem	x		x	x	x	x	x			
A-2	Archivierungssystem	x	x		x		x				

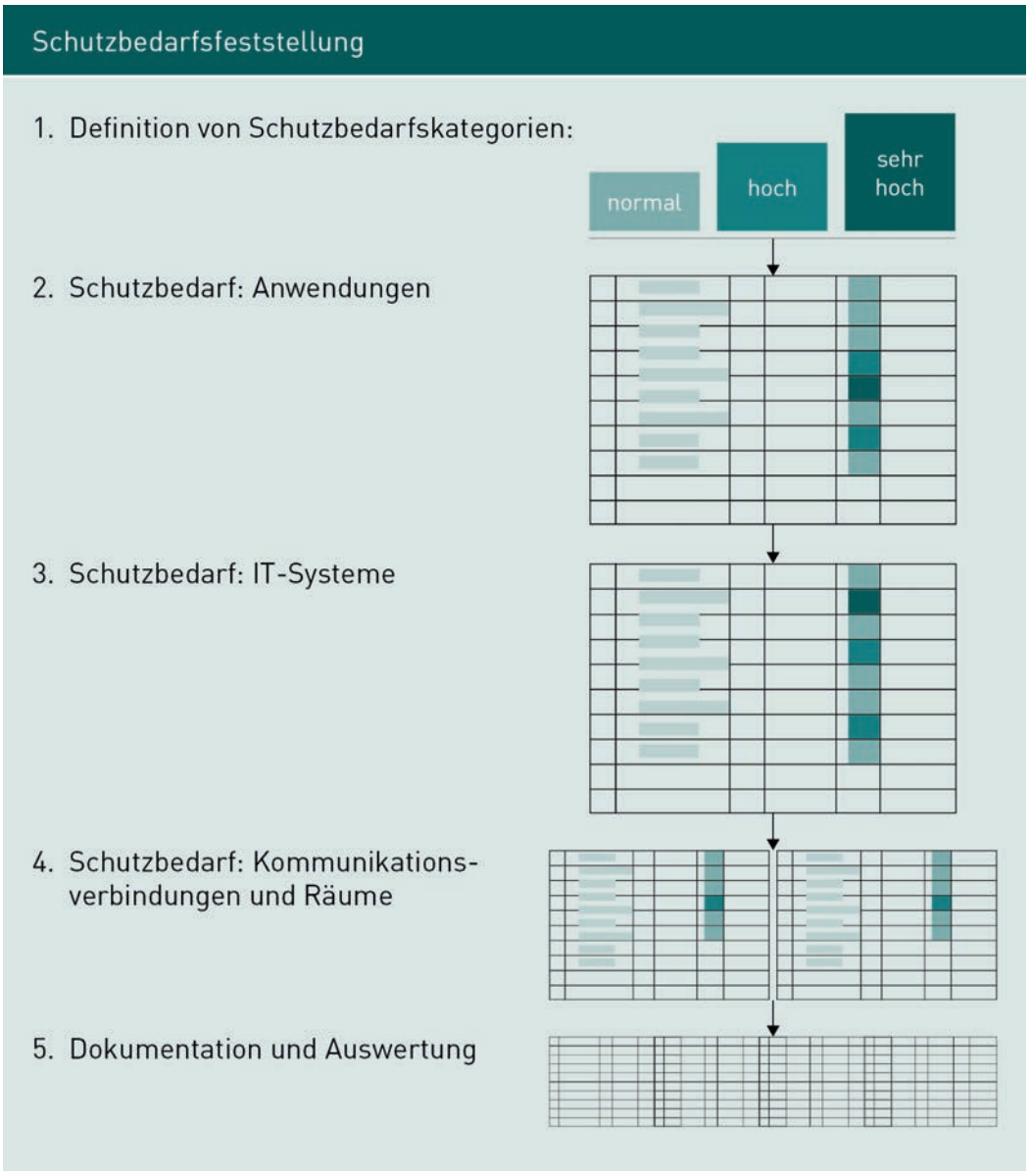
Nr.	Anwendung	S-1	S-2	C-1	C-2	ITS-1	ITS-2	ITS-3	TK-1	TK-2	N-1
A-3	Externe Archiv-Datenträger		x								
A-4	Fernwartungssoftware	x									
A-5	Datenaustausch mit Labor	x		x					x	x	x
A-6	Datenaustausch mit KV	x		x							x
A-7	Datenaustausch mit Privatärztlicher Verrechnungsstelle	x		x							x
A-8	Datenaustausch mit Krankenhäusern und anderen Praxen	x		x					x	x	
A-9	Kommunikation mit Patienten	x		x			x		x	x	

5.2 Schutzbedarfsfeststellung

Unter Schutzbedarf versteht der IT-GS die Bewertung der zu erwartenden Schäden, die bei einer Beeinträchtigung der Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können, und deren Einordnung in Kategorien, z. B. normal, hoch und sehr hoch. Hierbei geht es allein um mögliche Auswirkungen im Schadensfall ohne (zumindest zunächst) zu beachten, wie wahrscheinlich ein solcher Schadensfall ist.

Die Schutzbedarfsfeststellung bedeutet dann die konkrete Bestimmung der Schutzbedarfe für:

- Anwendungen,
- IT-Systeme,
- Kommunikationsverbindungen,
- Räume.



Typischerweise lässt sich der Schutzbedarf allerdings nicht quantifizieren: Welchen Schaden in Euro könnte man beispielsweise einer fehlenden Röntgenaufnahme in der Arztpraxis zuweisen? Oder wie wäre eine falsche Dosierungsangabe auf einem Rezept mit Geld zu bewerten? Und wie groß ist der Schaden bei einem Wassereinbruch im Serverraum der Arztpraxis?

Der IT-GS beschränkt sich daher auf qualitative Aussagen und definiert die drei folgenden Schutzbedarfskategorien:

- normal: Die Schäden sind begrenzt und überschaubar.
- hoch: Die Schäden können beträchtlich sein.
- sehr hoch: Die Schäden können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Um die Schutzbedarfskategorien institutionsspezifisch zu kategorisieren, schlägt das BSI im IT-GS typische Schadensszenarien vor, in die sich mögliche Schäden einordnen lassen:

1. Verstoß gegen Gesetze/Vorschriften/Verträge („Gesetze“),
2. Beeinträchtigung des Grundrechts auf informationelle Selbstbestimmung („Datenschutz“),
3. Beeinträchtigung der persönlichen Unversehrtheit („Gefahr für Leib und Leben“),
4. Beeinträchtigung der Aufgabenerfüllung („Aufgabenerfüllung“),
5. negative Innen- oder Außenwirkung („Außenwirkung“),
6. finanzielle Auswirkungen („Finanzielle Auswirkungen“).

Diese institutionsspezifische Kategorisierung soll am Beispiel der Arztpraxis verdeutlicht werden:

Es ist dabei allerdings zu beachten, dass sich Schäden oft mehreren Schadensszenarien zuordnen lassen. So ist z. B. die Offenlegung von Patientendaten oft ein Verstoß gegen den Datenschutz. Dies wirkt sich wiederum negativ auf das Ansehen des Arztes aus und kann finanzielle Auswirkungen zur Folge haben, sollte es zu einem Strafverfahren kommen.

Um die Schutzbedarfskategorien normal, hoch und sehr hoch voneinander abzugrenzen, müssen die Grenzen für die einzelnen Schadenszenarien bestimmt werden. Für die Stufe „hoch“ könnte dies in der Arztpraxis etwa so erfolgen:

Schadensszenario für die Schutzbedarfskategorie „hoch“	
Gesetze	Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen. Vertragsverletzungen mit hohen Konventionalstrafen.
Datenschutz	Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.
Gefahr für Leib und Leben	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
Aufgabenerfüllung	Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. Ein Systemausfall ist nur bis zu acht Stunden tolerabel.

Schadensszenario für die Schutzbedarfskategorie „hoch“	
Außenwirkung	Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	Der finanzielle Schaden liegt zwischen 1.000 und 10.000 Euro.

Mit dieser und den weiteren Festlegungen kann dann für jede Anwendung der Arztpraxis der Schutzbedarf, also das gewünschte Ausmaß an Vertraulichkeit, Integrität und Verfügbarkeit, festgelegt werden. Beispielhaft aufgeführt ist dies hier für die Anwendungen A-1 und A-9:

Beispiel Arztpraxis: Schutzbedarf der Anwendungen A-1 und A-9

Kürzel	Name	Vertraulichkeit	Integrität	Verfügbarkeit
A-1	Praxisverwaltungssystem (PVS)	Sehr Hoch	Sehr Hoch	Hoch
		Es werden besonders schutzbedürftige Patientendaten verarbeitet, deren Bekanntwerden die Betroffenen erheblich beeinträchtigen kann. Daher ist der Schutzbedarf sehr hoch	Es werden medizinische Daten verarbeitet. Da eine Veränderung nicht sofort auffällt und korrigiert werden kann, ist der Schutzbedarf sehr hoch.	Ist das PVS nicht verfügbar, so kann nicht auf die Patientenakte zugegriffen werden. Mittels analoger Dokumentation kann ein Ausfall überbrückt werden. Die Dokumentation muss später in das PVS übertragen werden. Der Schutzbedarf ist hoch.
A-9	Kommunikation mit Patienten	Sehr Hoch	Normal	Normal

Kürzel	Name	Vertraulichkeit	Integrität	Verfügbarkeit
		Siehe A-1.	Es werden medizinische Daten verarbeitet. Eine Veränderung würde auffallen und kann korrigiert werden. Der Schutzbedarf ist normal.	Fällt eine Telekommunikationsverbindung aus, so kann das persönliche Gespräch gesucht werden. Der Schutzbedarf ist normal.

IT-Systeme werden eingesetzt, um Anwendungen auszuführen. Der Schutzbedarf eines IT-Systems hängt damit im Wesentlichen von dem Schutzbedarf derjenigen Anwendungen ab, für deren Ausführung es benötigt wird. Der Schutzbedarf der Anwendungen bestimmt demnach den Schutzbedarf der IT-Systeme. Bei dieser Bestimmung kann man typisch die folgenden drei Fälle unterscheiden:

- In vielen Fällen lässt sich der höchste Schutzbedarf aller Anwendungen, die das IT-System benötigen, übernehmen **(Maximumprinzip)**.
- Der Schutzbedarf des IT-Systems kann höher sein als der Schutzbedarf der einzelnen Anwendungen **(Kumulationseffekt)**. Ein solcher höherer Schutzbedarf kann durch die Kumulation mehrerer Schutzbedarfe entstehen. Wenn beispielsweise auf einem Server mehrere Anwendungen laufen, die jeweils für sich einen normalen Schutzbedarf haben, dann kann der Server durch Kumulation dieser normalen Schutzbedarfe trotzdem einen hohen Schutzbedarf haben.
- Der Schutzbedarf kann niedriger sein als der Schutzbedarf der zugeordneten Anwendungen, wenn eine Anwendung mit hohem Schutzbedarf auf mehrere Systeme verteilt ist oder auf dem betreffenden IT-System nur weniger wichtige Teile dieser Anwendung ausgeführt werden **(Verteilungseffekt)**.

Für das Beispiel der Arztpraxis könnte sich also u. a. Folgendes ergeben:

Beispiel Arztpraxis: Schutzbedarf der IT-Systeme

Kürzel	Name	Vertraulichkeit	Integrität	Verfügbarkeit
S-1	Server für Praxisverwaltungssystem (PVS)	Sehr Hoch	Sehr Hoch	Hoch

Kürzel	Name	Vertraulich-keit	Integrität	Verfügbarkeit
		Maximum-prinzip	Maximum-prinzip	Maximumprin-zip
S-2	Server für Archi-vierungssystem	Sehr Hoch	Sehr Hoch	Normal
		Maximum-prinzip	Maximum-prinzip	Maximumprin-zip
C-1	Arbeitsplatzrech-ner	Sehr Hoch	Sehr Hoch	Hoch
		Maximum-prinzip	Maximum-prinzip	Maximumprin-zip
C-2	Laptop	Sehr Hoch	Sehr Hoch	Normal
		Maximum-prinzip	Maximum-prinzip	Das System ist im Praxisalltag nicht relevant.
		Maximum-prinzip	Maximum-prinzip	Maximumprin-zip
ITS-1	Kartenterminal	Sehr Hoch	Sehr Hoch	Hoch
		Maximum-prinzip	Maximum-prinzip	Maximumprin-zip
ITS-2	Switch	Sehr Hoch	Sehr Hoch	Normal
		Maximum-prinzip	Maximum-prinzip	Es ist ein Ersatz-gerät vorhan-den.
ITS-3	Drucker	Sehr Hoch	Sehr Hoch	Hoch
		Maximum-prinzip	Maximum-prinzip	Maximumprin-zip

In einem letzten Arbeitsschritt muss gemäß IT-GS der Schutzbedarf für die Kommunikationsverbindungen festgestellt werden. Es gibt Verbindungen, die gefährdeter sind als andere und beispielsweise durch doppelte Auslegung oder durch andere Maßnahmen gegen Angriffe von außen oder innen geschützt werden müssen. Daher werden Kommunikationsverbindungen bei IT-GS anhand der **Kritikalität** bewertet. In der Arztpraxis etwa wie folgt:

Kritikalität
Die Kritikalität bedeutet Wertung (Klassifizierung) von Prozessen oder Produkten anhand ihrer Bedeutung für eine Institution.

Beispiel Arztpraxis: Kritikalität der Kommunikationsverbindungen			
Kürzel	Name	Kritikalität	Extern. Netz
N-1	DSL-Modem und Router	K1, K2, K5	

In diesem Beispiel wurden die folgenden Kritikalitäten definiert:

- K1: kritisch aufgrund Außenverbindung;
- K2: kritisch aufgrund hoher Vertraulichkeit;
- K3: kritisch aufgrund hoher Integritätsanforderungen;
- K4: kritisch aufgrund hoher Verfügbarkeitsanforderungen;
- K5: Informationen mit hoher Vertraulichkeit dürfen nicht übertragen werden;
- K6: Informationen mit hohen Integritätsanforderungen dürfen nicht übertragen werden;
- K7: Informationen mit hohen Verfügbarkeitsanforderungen dürfen nicht übertragen werden.

Für den Schutzbedarf der Räume der Arztpraxis mag sich schließlich ergeben:

Beispiel Arztpraxis: Schutzbedarf der Räume				
Kürzel	Name	Vertraulichkeit	Integrität	Verfügbarkeit
R-1	Serverraum	Sehr Hoch	Sehr Hoch	Hoch
		Maximumprinzip	Maximumprinzip	Maximumprinzip
R-2	Büro Arzt	Sehr Hoch	Sehr Hoch	Hoch
		Maximumprinzip	Maximumprinzip	Maximumprinzip

Kürzel	Name	Vertraulichkeit	Integrität	Verfügbarkeit
R-3...8	Behand-lungsraum	Sehr Hoch	Sehr Hoch	Hoch
		Maximumprin-zip	Maximumprin-zip	Maximumprin-zip
R-9	Rezeption	Sehr Hoch	Sehr Hoch	Hoch
		Maximumprin-zip	Maximumprin-zip	Maximumprin-zip
R-10	Teeküche	Normal	Normal	Normal
		Nur der Laptop (C-2) ist betrof-fen und dieser wird wegge-schlossen, wenn er nicht in Betrieb ist.	Nur der Laptop (C-2) ist betrof-fen und dieser wird wegge-schlossen, wenn er nicht in Betrieb ist.	Nur der Laptop (C-2) ist betrof-fen und dieser wird wegge-schlossen, wenn er nicht in Betrieb ist.

5.3 Modellierung (Auswahl der Sicherheitsanforderungen)

Bei der Modellierung bildet man den IT-Verbund und seine einzelnen Komponenten mithilfe der Bausteine des IT-GS nach. Das Ergebnis ist ein IT-GS-Modell. Dafür greift man auf die Ergebnisse der beiden vorangegangenen Schritte zurück:

- Aus der Strukturanalyse erhält man die einzelnen Objekte des konkreten IT-Verbun-des.
- Die Ergebnisse der Schutzbedarfsfeststellung geben zusätzliche Hinweise auf die relevanten Anforderungen der betroffenen Bausteine, werden aber vor allem für die weiteren Schritte benötigt, wenn es Bausteine gibt, die bei einem der drei Schutz-ziele einen erhöhten Schutzbedarf haben.

Dieses IT-GS-Modell kann dann für die existierenden Teile des IT-Verbundes als Prüf-plan verwendet werden und für die geplanten Teile als Entwicklungskonzept.

Die Bausteine aus IT-GS bilden den Kern des IT-GS-Kompendiums. Durch sie ermittelt man sowohl die Gefährdungen, denen ein Objekt ausgesetzt ist, als auch die Anforderungen an geeignete Schutzmaßnahmen. Alle Bausteine sind gleichartig gegliedert:

- **Beschreibung:** Jeder Baustein beginnt mit einer kurzen Beschreibung und Abgrenzung der betrachteten Objekte.
- **Gefährdungslage:** Dieser Abschnitt zeigt auf, welchen Gefährdungen die im Baustein betrachteten Objekte ausgesetzt sein können. Die Gefährdungslage wird pauschal betrachtet, also ohne Berücksichtigung von Eintrittswahrscheinlichkeiten. Die Gefährdungen referenzieren ihre ausführlichen Beschreibungen in den Gefährdungskatalogen und sind gegliedert anhand der möglichen Ursachen „Höhere Gewalt", „Organisatorische Mängel", „Menschliche Fehlhandlungen", „Technisches Versagen" und „Vorsätzliche Handlungen".
- **Anforderungen:** Danach folgen die zu erfüllenden Anforderungen untergliedert nach Basisanforderungen, Standardanforderungen sowie beispielhafte Anforderungen bei erhöhtem Schutzbedarf.
- **Weiterführende Informationen:** Dieser Abschnitt enthält Literaturhinweise, meist auf relevante andere Standards zum jeweiligen Thema.
- **Anlage Kreuzreferenztabelle zu elementaren Gefährdungen:** Abschließend wird in dieser Anlage der Bezug hergestellt zwischen den für diesen Baustein relevanten Gefährdungen und den zugehörigen Anforderungen.

Zudem sind alle Bausteine einer von zehn Schichten zugeordnet, die wie folgt definiert sind:

Prozess- und System-Bausteine	
Prozess-Bausteine	System-Bausteine
ISMS (Sicherheitsmanagement)	INF (Infrastruktur)
ORP (Organisation und Personal)	NET (Netze und Kommunikation)
CON (Konzepte und Vorgehensweisen)	SYS (IT-Systeme)
OPS (Betrieb)	APP (Anwendungen)
DER (Detektion und Reaktion)	IND (Industrielle IT)

Die in den Prozess-Baustein-Schichten beschriebenen Bausteine haben die Besonderheit, dass die darin vorgeschlagenen Konzepte und Regelungen für den ganzen IT-Verbund einheitlich gelten sollten und daher meistens nur einmal angewendet werden müssen.

Dazu gehört zuerst die Schicht ISMS, die nur aus einem Baustein besteht. Sie enthält beispielsweise für eine Arztpraxis die Basisanforderungen ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene, ISMS.1.A7 Festlegung von Sicherheitsmaßnahmen und ISMS.1.A8 Integration der Mitarbeiter in den Sicherheitsprozess.

Auch übergreifend wichtig für die Arztpraxis ist der Baustein CON.2 Datenschutz, der vom BfDI (Bundesbeauftragter für den Datenschutz) beigesteuert wurde. Dieser Baustein ergänzt die allgemeinen Gefährdungen der anderen Bausteine um zusätzliche Gefährdungen und Anforderungen aus Sicht des Datenschutzes.

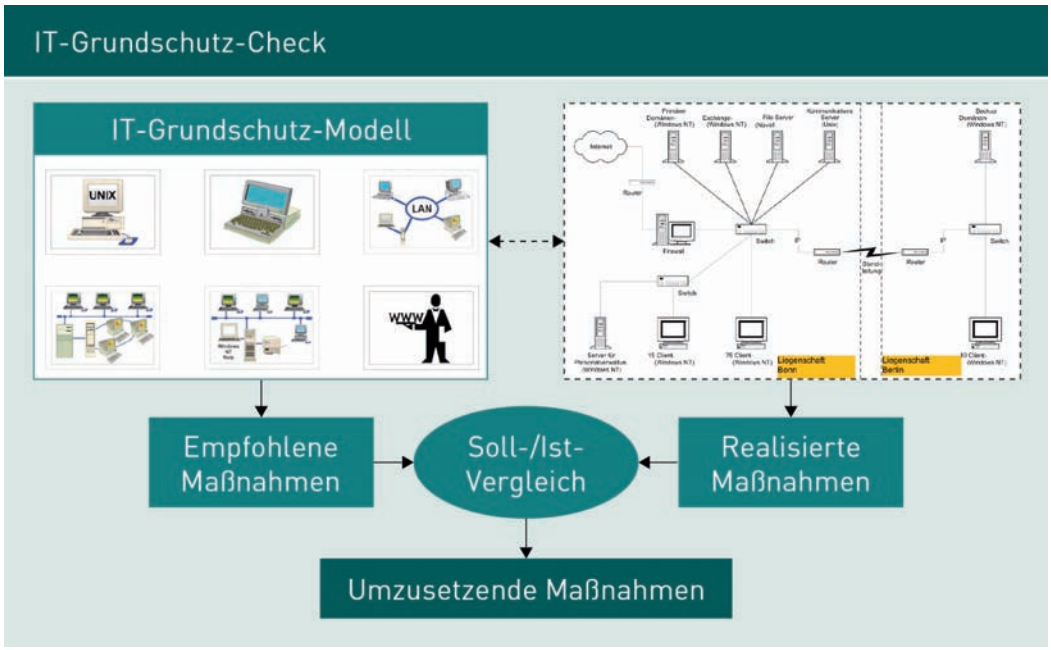
Während die Prozess-Bausteine in der Regel für einen IT-Verbund nur einmal anzuwenden sind, sind die System-Bausteine differenzierter zu betrachten. So sollte der Baustein INF.1 Allgemeines Gebäude der Schicht „Infrastruktur“ immer dann gesondert für jedes Gebäude angewendet werden, wenn sich die Gebäude in wesentlichen Merkmalen unterscheiden. Zum Beispiel unterscheiden sich die Gebäude „Praxis“ und „Praxisinhaber“ (vgl. Abb. „Räume der Arztpraxis“) wahrscheinlich in ihrer Struktur so sehr, dass sie auch bezüglich Sicherheit gesondert betrachtet werden müssen. Zusätzlich sind hier die Bausteine INF.7 Büroarbeitsplatz bzw. INF.8 Häuslicher Arbeitsplatz relevant.

Die Bausteine der Schicht SYS: IT-Systeme sind für jedes IT-System oder jede Gruppe von IT-Systemen gesondert zu berücksichtigen. Für die in der Arztpraxis vorhandenen Computer sind dies z. B. die Bausteine SYS.12.2 Windows Server 2012, SYS.3.1 Laptop und SYS.2.2.2 Client unter Windows 8.1, für jeden Server zusätzlich der Baustein SYS.1.1 Allgemeiner Server sowie für alle Clients der Baustein SYS.2.1 Allgemeiner Client.

Für das IT-System ITS-1: Kartenterminal der Arztpraxis enthält der Bausteinkatalog allerdings (zumindest derzeit) keinen geeigneten Eintrag. In solchen Fällen muss man einen neuen („benutzerdefinierten“) Baustein anlegen. Die in 5.5 beschriebene ergänzende Sicherheitsanalyse auf Basis von IT-GS kann die Auswahl zweckmäßiger Maßnahmen für einen solchen selbst definierten Baustein unterstützen.

5.4 IT-Grundschutz-Check

Beim IT-Grundschutz-Check werden die bereits realisierten Sicherheitsmaßnahmen mit den Empfehlungen der IT-GS-Kataloge verglichen, um das erreichte Sicherheitsniveau zu identifizieren und Verbesserungsmöglichkeiten aufzuzeigen:



Am Beispiel der Arztpraxis soll dies für den Serverraum R1 demonstriert werden. Diesem wird sinnvollerweise der Baustein INF.2 Rechenzentrum sowie Serverraum zugeordnet. In diesem Baustein finden sich die nachfolgenden Basisanforderungen, wobei die verantwortlichen Rollen jeweils in Klammern benannt sind:

- INF.2.A1 Festlegung von Anforderungen (Planer, IT-Betrieb, Haustechnik, Informationssicherheitsbeauftragter [ISB]);
- INF.2.A2 Bildung von Brandabschnitten (Planer) (*);
- INF.2.A3 Einsatz einer unterbrechungsfreien Stromversorgung (Haustechnik);
- INF.2.A4 Notabschaltung der Stromversorgung (Haustechnik);
- INF.2.A5 Einhaltung der Lufttemperatur und -feuchtigkeit (Haustechnik);
- INF.2.A6 Zutrittskontrolle (IT-Betrieb, Informationssicherheitsbeauftragter [ISB], Haustechnik);
- INF.2.A7 Verschließen und Sichern (Mitarbeiter, Haustechnik);
- INF.2.A8 Einsatz einer Brandmeldeanlage (Planer);
- INF.2.A9 Einsatz einer Lösch- oder Brandvermeidungsanlage (Planer) (*);
- INF.2.A10 Inspektion und Wartung der Infrastruktur (IT-Betrieb, Haustechnik, Wartungspersonal);
- INF.2.A11 Automatisierte Überwachung der Infrastruktur (IT-Betrieb, Haustechnik).

Die beiden mit (*) markierten Anforderungen sind im Falle von Serverräumen nur Soll-Anforderungen, keine Muss-Anforderungen.

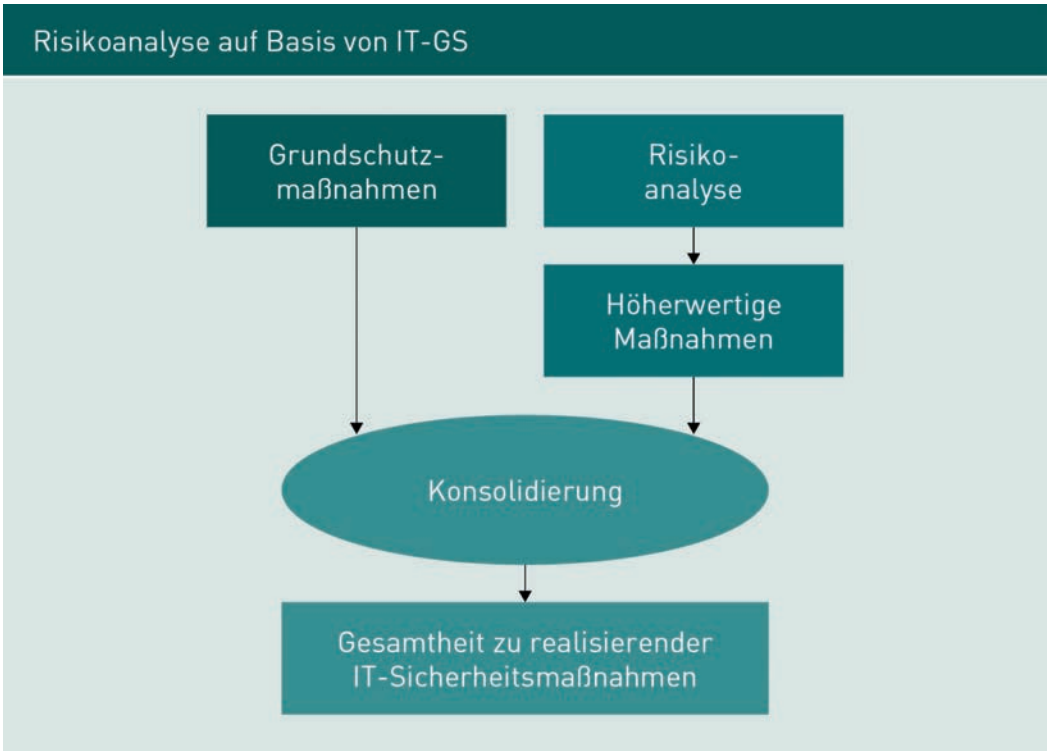
Der Praxisinhaber muss nun für diese Maßnahmen prüfen, ob und gegebenenfalls wieweit diese realisiert sind. Er hat demnach einen „Prüfplan“, mit dem er das bestehende Sicherheitsniveau ermitteln und bewerten kann.

5.5 Risikoanalyse

Der IT-GS leistet zumindest für typische IT-Verbünde mit durchschnittlichem Schutzbedarf ein angemessenes und (meist) kostengünstiges Sicherheitsniveau. Insbesondere bei hohem und sehr hohem Schutzbedarf kann es allerdings sein, dass die IT-GS-Maßnahmen keinen ausreichenden Schutz bieten. Ohne eine sorgfältige Prüfung, ob zusätzliche oder wirksamere Maßnahmen erforderlich sind oder nicht, geht man dann möglicherweise unvertretbare Risiken ein.

In diesen Fällen ist es daher notwendig, in einer ergänzenden Risikoanalyse zu prüfen, wie diejenigen Objekte zu behandeln sind, die einen hohen oder sehr hohen Schutzbedarf haben. Entsprechende Überlegungen können zu dem Ergebnis führen, dass die Umsetzung der IT-GS-Maßnahmen genügt und kein zusätzlicher Handlungsbedarf besteht. Sie können aber auch einen Bedarf an zusätzlichen oder höherwertigen Maßnahmen aufzeigen.

Zur Beurteilung von Gefährdungsszenarien ist die Risikoanalyse ein weitverbreitetes und in vielen Fachgebieten angewendetes Verfahren. Bei der Risikoanalyse auf der Basis von IT-GS verwendet man die Gefährdungen im Kompendium zusammen mit den Ergebnissen der Schutzbedarfsfeststellung als Ausgangspunkt dieses Verfahrens und prüft, ob gegebenenfalls weitere Gefährdungen zu berücksichtigen sind, aus denen höherwertige Maßnahmen abgeleitet werden können.



Das allgemeine Vorgehen soll am Beispiel der Rezeption R9 in der Arztpraxis erläutert werden: Hier ist der Schutzbedarf hinsichtlich Vertraulichkeit sehr hoch. In der ergänzenden Sicherheitsanalyse ergibt sich neben den allgemeinen Gefährdungen, denen ein Büroraum gemäß INF.8 Büroarbeitsplatz ausgesetzt ist, im Bereich „Vorsätzliche Handlungen" u. a. die neue Gefährdung: „Neugierige Patienten", die davon herrührt, dass Patienten oft nur schwer auf Distanz gehalten werden können.

Als notwendige Zusatzmaßnahme mag es dann u. a. erforderlich sein, den Empfangsbereich deutlich vom Wartebereich zu trennen sowie Bildschirme für Patienten nicht einsehbar aufzustellen.

Um die Bedeutung einer Gefährdung zu klären, wurde in der neuen Version des IT-GS deren Bewertung anhand eines Matrix-Ansatzes auf Basis von Eintrittswahrscheinlichkeiten und Schadenshöhen eingeführt. Die Bewertung erfolgt über die zu erwartende Häufigkeit des Eintretens und die Höhe des Schadens, der bei Eintritt der Gefährdung entsteht. Aus diesen beiden Anteilen ergibt sich dann das Risiko.

Zusammenfassung

Herausstechendes Merkmal der Erstellung eines IT-Sicherheitskonzepts auf Basis von IT-Grundschutz ist der weitgehende Verzicht auf eine detaillierte Risikoanalyse: Es wird grundsätzlich von pauschalen Gefährdungen ausgegangen und somit auf die differenzierte Einteilung nach Schadenshöhe und Eintrittswahrscheinlichkeit zunächst verzichtet.

Dieses Vorgehen nach IT-Grundschutz bietet folglich ein einfaches „Kochrezept" für ein grundlegendes Schutzniveau (daher der Name Grundschutz). Durch die Verwendung des mitgelieferten Kompendiums entfällt zunächst eine aufwendige Risikoanalyse, die meist Expertenwissen erfordert. Auch einem Laien ist es so möglich, die zu ergreifenden Standard-Sicherheitsmaßnahmen zu identifizieren und in Zusammenarbeit mit Fachleuten umzusetzen.

Durch Standard-Sicherheitsmaßnahmen in den Bereichen Organisation, Personal und Technik wird somit bekannten Gefährdungen begegnet und dadurch ein Standard-Sicherheitsniveau erreicht.

Aber auch für sensiblere Bereiche wird damit ein brauchbares Fundament gelegt: Die bei erhöhtem Schutzbedarf zusätzlich notwendigen Maßnahmen werden durch eine ergänzende Risikoanalyse ermittelt. Hierzu beschreibt der IT-GS Methoden, wie für bestimmte Objekte festgestellt werden kann, ob und in welcher Hinsicht über den IT-GS hinaus Handlungsbedarf besteht, um Risiken für die IT-Sicherheit zu reduzieren.

Wissenskontrolle

Haben Sie diese Lektion verstanden?

Dann haben Sie jetzt die Möglichkeit, das Gelernte auf unserer Lernplattform zu überprüfen.

Viel Erfolg!

Lektion 6

Bewährte Schutz- und Sicherheitskonzepte für IT-Geräte

LERNZIELE

Nach der Bearbeitung dieser Lektion werden Sie wissen, ...

- ... welche Handlungsempfehlungen für IT-Geräte nach dem heutigen Stand der Technik für Datenschutz und IT-Sicherheit sorgen.
- ... wie man sich vor Diebstählen schützen kann.
- ... wie Daten sicher gespeichert und vernichtet werden können.

6. Bewährte Schutz- und Sicherheitskonzepte für IT-Geräte

Einführung

Im November 2005 erschien in den Nachrichten der Universität Bern folgende Anzeige:

Suchanzeige

Gesucht wird: Inhalt eines G4 PowerBooks

Der Inhalt repräsentiert hunderte von Arbeitsstunden und enthält auch alle digitalen Bilder und Videoclips der Kinder des Besitzers des Lap-tops [sic!]. Der seit letztem Samstag (12.11.05) durch Einschlagen einer Autoscheibe neue Besitzer ist höflichst gebeten, diesen Inhalt per DVD an folgende Adresse zu retournieren: [...]

In dieser Lektion werden einige bewährte Vorgehensweisen und Handlungsempfehlungen für den Schutz von stationären und mobilen IT-Geräten im Überblick vorgestellt. Dabei geht es u. a. sowohl um den Schutz vor Schadsoftware als auch die sichere Speicherung von Daten hinsichtlich der Grundsätze Verfügbarkeit, Vertraulichkeit und Integrität. Außerdem stellt sich zuletzt noch die Frage, wie Daten sicher vernichtet werden können.

6.1 Schutz vor Diebstahl

Sowohl stationäre IT-Geräte (wie Desktops und externe Festplatten-Arrays) als auch mobile IT-Geräte (wie Laptops, Notebooks, Tablets, Smartphones und USB-Sticks) sind vor allem Datenträger, die schon allein deshalb meist nicht in die Hände Unbefugter gelangen dürfen. Zudem ist im Falle eines Diebstahls trotz des stetigen Preisverfalls bei IT-Geräten auch der materielle Schaden oft nicht unerheblich.

Clean-Desk-Prinzip
Das Clean-Desk-Prinzip beschreibt Benutzerrichtlinien für den Arbeitsplatz, die insbesondere festlegen, wie der Arbeitsplatz auszusehen hat, wenn ein Arbeitnehmer sein Büro verlässt.

In der Wohnung oder am Arbeitsplatz lässt sich Diebstahlschutz durch Beachtung des sogenannten **Clean-Desk-Prinzips** erreichen, das durch die folgenden zwei Regeln charakterisiert ist:

- **Aufräumen:** Ordnung ist nicht nur etwas, das eine Suche erleichtert. Wer Ordnung hält, senkt auch das Risiko, dass IT-Geräte in die Hände Unbefugter gelangen. Durch Aufräumen sind die Geräte und Daten weniger leicht für andere zugänglich, und man sieht andererseits schneller, wenn etwas fehlt.
- **Abschließen:** Alle mobilen IT-Geräte sollten immer dann in einem Behältnis (Schrank, Schublade, Rollcontainer, ...) weggeschlossen sein, wenn sie im Rahmen der aktuellen Arbeitsaufgabe nicht erforderlich sind. Wenn man länger abwesend ist, beispielsweise, weil man Feierabend hat, sollten Räume und Behältnisse, die IT-Geräte beherbergen, abgeschlossen und der Schlüssel abgezogen werden.

In den USA ist das Clean-Desk-Prinzip nicht selten schriftlicher Bestandteil des Arbeitsvertrages mit allen Konsequenzen, die für Verstöße vorgesehen sind.

Unterwegs sollte man IT-Geräte nach Möglichkeit immer so aufbewahren, dass sie für Dritte nicht sichtbar sind. Dies bedeutet etwa, dass ein Laptop während der Fahrt im Auto nur im Kofferraum transportiert werden sollte. Auch im Hotel sollten IT-Geräte sicher verstaut werden. Steht etwa ein Safe zur Verfügung, sollte dieser unbedingt genutzt werden.

Bei Tagungen, Zugreisen, Besprechungen etc. kann es sinnvoll sein, das Notebook oder den Laptop mittels eines Sicherheitsschlosses (Kensington-Schloss) an Gegenständen (z. B. einem Möbelstück oder einem Heizkörper) zu befestigen. Dann braucht man sich auch meist keine Sorgen machen, wenn man abgelenkt wird oder den Bereich kurz verlässt. Auf Reisen sollte man nur diejenigen IT-Geräte mitführen, die man unbedingt benötigt. Was man nicht dabei hat, kann nicht verloren gehen!

Kommt es doch einmal zum Diebstahl, so kann man – bei entsprechender Ausstattung – zumindest noch reaktiv tätig werden. Mobile IT-Geräte mit einer sogenannten Computrace - Funktionalität (auch LoJack-Funktionalität genannt) sind nämlich sozusagen stets an einer langen, virtuellen Leine, indem regelmäßig der aktuelle Standort des Gerätes ermittelt und an einen zentralen Computrace-Server geschickt wird. Kommt das mobile IT-Gerät abhanden, meldet der Besitzer dies an den Computrace-Dienst, der das Gerät dann lokalisiert. Optional lassen sich dann beispielsweise auch Benutzerdateien aus der Ferne löschen. Allerdings ist dem Computrace-Dienst folglich auch stets der aktuelle Standort des legitimen Besitzers bekannt, was hinsichtlich Datenschutz durchaus problematisch zu sehen ist.

6.2 Schutz vor Schadsoftware (Malware)

Auch wenn es einem Unbefugten nicht gelingt, ein IT-Gerät physisch in Besitz zu nehmen, besteht die Gefahr, dass ein Angreifer die Kontrolle über ein IT-Gerät erlangt und somit Zugriff auf die Daten und die Funktionen des IT-Gerätes hat. Diese unerwünschte Übernahme durch Dritte kann technisch auf unterschiedliche Weise durch Schadsoftware (Malware) geschehen: durch Viren, durch Würmer, durch Trojaner oder durch Exploits.

Generell gilt, dass viele der mit Schadsoftware verbundenen Nachteile erst durch die mangelhafte Konfiguration von IT-Geräten ermöglicht werden. Dies betrifft insbesondere private Anwender, die weder das Wissen noch die finanziellen Möglichkeiten haben, um ihre IT-Geräte sicher einzurichten und sicher zu betreiben.

Der erste Schritt zu einem sicheren IT-Gerät ist nämlich der Einsatz aktueller Software, um bekannt gewordene und durch den Hersteller beseitigte Sicherheitslücken zeitnah zu schließen. Dabei ist es absolut notwendig, insbesondere das Betriebssystem stets aktuell zu halten, was durchaus bedeuten kann, mehrmals täglich Aktualisierungen einzuspielen.

Der zweite Schritt zu einem sicheren System besteht dann in dem Anpassen der Sicherheitseinstellungen des IT-Gerätes. Grundsätzlich sollte gelten, den Anwendern eines IT-Gerätes immer nur die Rechte einzuräumen, die sie benötigen, um ihre Aufgaben erfüllen zu können. Erst wenn diese Konfigurationsempfehlungen befolgt werden, hat man überhaupt eine Chance, sich gegen Schadsoftware erfolgreich zu wehren.

Die folgenden Erläuterungen zu Ausprägungen von Schadsoftware orientieren sich eng an Spindler (2007).

Viren

Grundsätzlich werden in der IT unter Viren sich selbst verbreitende Softwarefragmente verstanden. Viren treten niemals alleine auf, sondern benötigen einen Wirt, um ausgeführt zu werden, sich zu verbreiten und gegebenenfalls vorhandene Schadfunktionen auszuführen. Bei einem Wirt handelt es sich um eine ausführbare Datei, die von einem Virus infiziert wurde oder infiziert werden kann. Durch eine sogenannte „Infektion“ wird der Wirt so verändert, dass mit seiner eigenen Ausführung auch die Funktionen des Virus ausgeführt werden, wobei Viren stets versuchen, die eigene Existenz zu verheimlichen und gleichzeitig möglichst viele weitere Wirte zu infizieren.

Virenscanner sind, wie der Name bereits nahelegt, eine effektive Maßnahme, um die Infektion mit Viren zu verhindern, indem sie jeden Dateizugriff überwachen und – regelmäßig – alle vorhandenen Dateien auf Infektionen überprüfen. Dabei ist es extrem wichtig die sogenannten Virendefinitionsinformationen stets aktuell zu halten. Alle wichtigen Anbieter haben dafür standardmäßig eine automatische, webbasierte Updatefunktion in ihre Produkte eingebaut, sodass der Anwender sich nach der erstmaligen Einrichtung kaum noch persönlich darum kümmern muss. Wichtig ist natürlich, dass diese Automatik nicht abgestellt wird. Gefährlich ist aber ein falsches Sicherheitsbewusstsein, wenn Benutzer glauben, dass ihnen mit einem Virenscanner nichts mehr passieren könne und sie gegen Angriffe geschützt seien. Ein Virenscanner kann nur gegen bekannte Viren schützen und (mit erheblichen Einschränkungen) gegen weitere Viren, soweit diese nach einem bekannten Schema agieren. Vorsicht, beispielsweise nicht auf unbekannte Links zu klicken, bleibt auch bei Nutzung eines Virenscanners erforderlich.

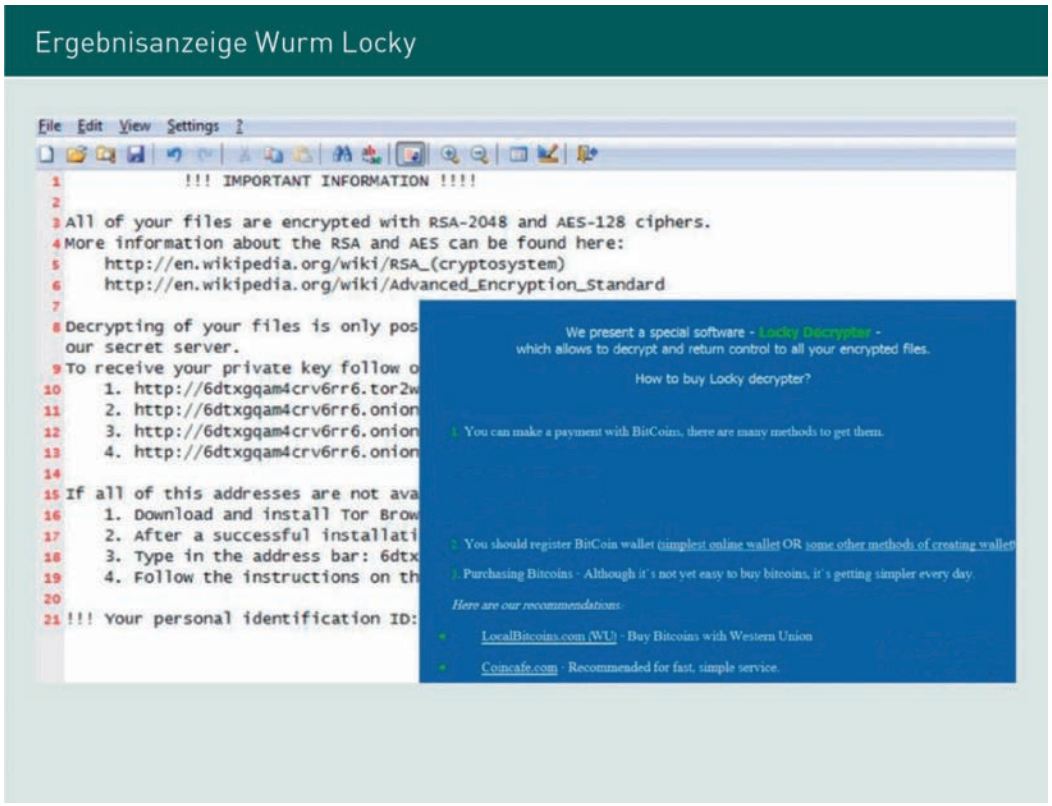
Würmer

Während Viren darauf ausgelegt sind, möglichst viele ausführbare Dateien zu infizieren, und auf eine Verbreitung dieser infizierten Dateien durch den Anwender angewiesen sind, nutzen Würmer die IT-Infrastruktur, um sich selbst zu verbreiten, etwa als Anhang einer E-Mail. Von Würmern sind auch Plattformen (z. B. Smartphones) betroffen, die von Viren lange verschont geblieben sind.

Als Beispiel sei der seit Anfang 2016 kursierende Wurm „Locky“ erwähnt. Dabei handelt es sich um sogenannte Ransomware (engl. „ransom“ – Lösegeld). Das Funktionsprinzip ist einfach: Die Schadsoftware wird als Anhang einer E-Mail versendet. Klickt ein

Anwender auf einen entsprechend präparierten Anhang, installiert sich die Schadsoftware und beginnt ihr Werk. Im Hintergrund verschlüsselt Locky dann alle Dateien. Dabei beschränkt sich Locky nicht nur auf die lokal gespeicherten Daten. Locky verschlüsselt alles, was er erreichen kann, und daher gegebenenfalls auch Cloudspeicher. Anschließend wird der Anwender aufgefordert, ein Lösegeld in der Internetwährung **Bitcoin** zu bezahlen, wenn er das Kennwort zur Entschlüsselung erhalten möchte.

Bitcoin
Das ist ein verschlüsseltes, digitales Zahlungsmittel für geschäftliche und private Geldtransaktionen im Internet.



Ein weiteres Beispiel ist der sogenannte „Stuxnet“-Wurm, der eigens entwickelt wurde, um Industrieanlagen zu befallen. Er ist (wahrscheinlich) der erste Wurm, der gezielt Zentrifugen einer Industrieanlage angreifen kann.

Neben dem standardmäßigen Einsatz von Virenscannern, die neben Viren auch Würmer erkennen und deren Ausführung verhindern können, erfordert der Schutz vor Würmern vor allem, dem Anwender nur die Rechte einzuräumen, die er für seine aktuelle Arbeitsaufgabe wirklich benötigt, was sich bei allen modernen Plattformen einfach dadurch realisieren lässt, normalerweise ohne Administratorrechte zu arbeiten. Zudem sollten Anhänge von E-Mails, die unbekannter Herkunft sind, niemals geöffnet werden. Schließlich sind alle bei Office-Produkten möglichen Ausführungen von Makros über Systemeinstellungen generell zu unterbinden.

Trojaner

Als Trojanische Pferde (auch Trojaner) werden Programme bezeichnet, die als nützliche Anwendung getarnt sind, aber zusätzliche Funktionen beinhalten, die ohne Wissen und Zutun des Anwenders ausgeführt werden. Das Ziel besteht darin, heimlich Aktionen auf dem System auszuführen, sodass diese vom Anwender nicht bemerkt werden. Trojaner verbreiten sich ähnlich wie Viren oft mithilfe des Anwenders, der, im Glauben eine sinnvolle Anwendung zu installieren, gleichzeitig den Trojaner installiert.

Meist operieren Trojaner nach dem Client-Server-Prinzip. Der eigentliche Trojaner ist dabei der Server. Er nistet sich – als nützliche Anwendung getarnt – auf dem IT-Gerät ein und sorgt für seinen automatischen Start beim Booten des Betriebssystems. Der Angreifer kann nun mittels eines passenden Clients aktiv über diesen Server bei seinem Opfer Schaden anrichten oder Daten ausspionieren.

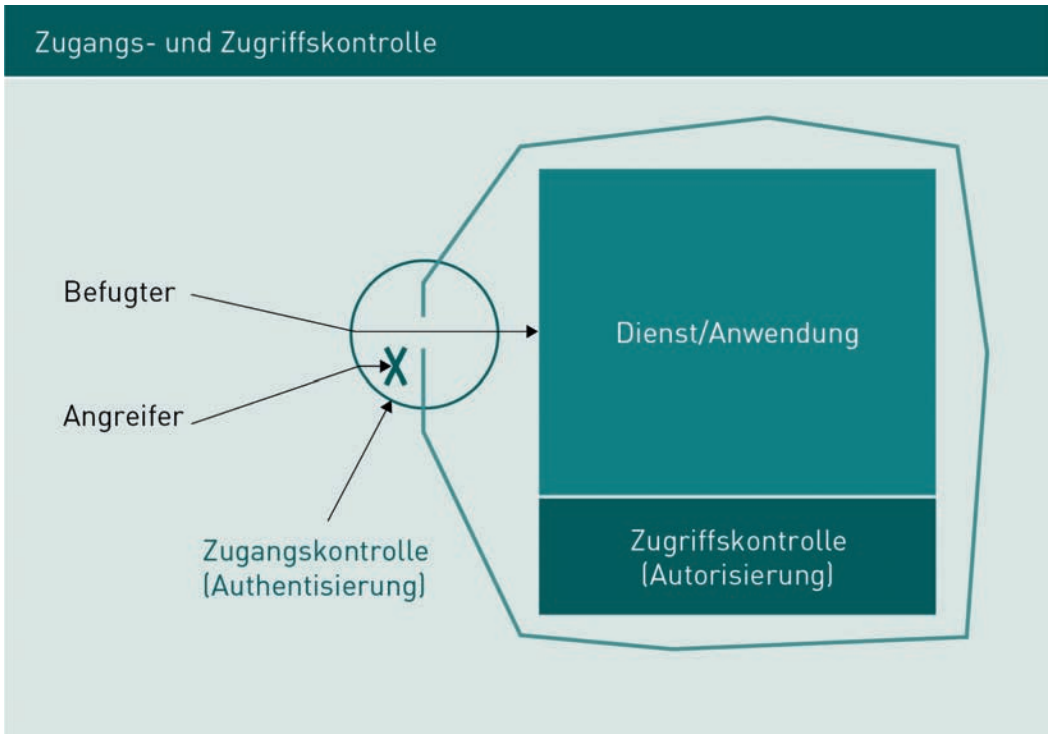
Zusätzlich zu den bereits oben genannten Schutzmöglichkeiten durch Virenscanner sorgt der generelle Verzicht auf Programme aus unbekannten oder unsicheren Quellen für einen Schutz gegen Trojaner. Am Arbeitsplatz sollte es – durch entsprechende Beschränkung der Rechte – dem Anwender grundsätzlich nicht möglich sein, selbst Software zu installieren oder Software auszuführen, die nicht explizit freigegeben wurde.

Exploits

Durch nicht geschlossene Sicherheitslücken in Programmen, die Netzwerkdienste erbringen und daher über das Netzwerk ansprechbar sind, sind auch externe Angreifer in der Lage, ein IT-Gerät zu kompromittieren. Eine solche Sicherheitslücke kann gegebenenfalls bewirken, dass eine Software ausfällt oder dass eingeschleuste Schadsoftware auf dem IT-System ausgeführt werden kann. Derartige Lücken werden beispielsweise häufig von Würmern ausgenutzt, um sich in einem IT-Gerät einzunisten. Erwähnt sei an dieser Stelle etwa der Wurm „Sasser“, welcher ab Mai 2004 einen Systemdienst in Microsoft-Betriebssystemen dazu missbrauchte, den Rechner zufällig auszuschalten.

6.3 Sichere Anmeldeverfahren

Um die Vertraulichkeit der Daten und Funktionen eines IT-Gerätes sicherzustellen, bedarf es einer Zugangskontrolle, die ausschließlich Befugten die Möglichkeit eröffnet, Zugriff auf die Daten und Funktionen des IT-Gerätes zu erlangen:



Bei einer Anmeldung für einen Dienst oder eine Anwendung werden drei wesentliche Schritte unterschieden:

- Identifizierung: Angabe der Identität (je nach Kontext auch ohne Nachweis) ,
- Authentifizierung: Überprüfen und Bestätigen der Identität,
- Autorisierung: Zuordnung von Rechten auf Basis der (geprüften) Identität.

Wie in der realen Welt erfordert auch in einem IT-Verbund die wirksame Unterscheidung von Entitäten einen (eindeutigen) Namen, der hier aber aus einer Bitfolge repräsentiert durch eine alphanumerische Zeichenkette besteht. Man nennt derartige Namen eine (digitale) Identität. Sie sind bei natürlichen Personen sozusagen der Benutzername, unter dem sie im IT-Verbund bekannt sein wollen.

Der Nachweis einer solchen (digitalen) Identität wird als Authentisierung und der dazu erforderliche Prozess zur Bestätigung der Identität wird als Authentifizierung bezeichnet.

Authentisiert wird meist mittels bestimmter Eigenschaften der zu authentisierenden Entität oder einem Geheimnis, welches nur dieser Entität bekannt ist, oder eines konkreten Gegenstandes, welcher im Besitz dieser Entität ist.

Bei natürlichen Personen werden als Eigenschaften gerne biometrische Merkmale (Gesichtsgeometrie, Irisstruktur, Fingerabdruck, Stimme, ...) oder Fähigkeiten (Tippcharakteristik auf einer bestimmten Tastatur) verwendet. Die Nutzung derartiger biometrischer Merkmale scheint auf den ersten Blick besonders sicher, aber auch hier bestehen deutliche Risiken. Dazu gehört zuerst einmal das deutliche Risiko einer fehlerhaften

Ablehnung oder fehlerhaften Annahme, da beispielsweise auch zwei Fingerabdrücke des gleichen Fingers der gleichen Person bestenfalls sehr ähnlich, aber nie identisch sind. Dazu kommen neue Angriffsformen, beispielsweise die Simulation der Irisstruktur einer anderen Person durch eine entsprechende Kontaktlinse. Derartige Angriffe sind besonders gravierend, da eine Person ihre biometrischen Merkmale nicht einfach ändern kann, wenn die originalen Merkmale in irgendeiner Form gestohlen wurden.

Natürliche Personen können sich auch Bitfolgen in Form alphanumerischer Zeichenketten als Geheimnisse für die Zwecke einer Authentisierung merken, wenn diese nicht zu kompliziert sind. Derartige Geheimnisse werden als **Kennwort** (Passwort) bezeichnet.

Offensichtlich ist es vorteilhaft, wenn statt das Geheimnis bei einer Authentifizierung weiterzugeben, nur der Beweis erbracht werden muss, dass man das Geheimnis kennt – **Challenge-Response-Verfahren** beruhen beispielsweise genau darauf.

Smartcards
Dies sind kontaktbehaftete Plastikkarten mit eigenem Prozessor und Speicher.

Der Besitz eines Gegenstandes und die Kenntnis eines Geheimnisses können z. B. in Form einer **Smartcard** mit Kennworten im Speicher kombiniert werden. Eine solche Kombination mehrerer Authentifizierungsverfahren bezeichnet man als 2-Faktor-Authentifizierung (2FA) oder Mehr-Faktor-Authentifizierung (MFA). Mit ihr kann man - meist mit nur wenig Zusatzaufwand für die Benutzer - die Sicherheit einer Authentifizierung oft wesentlich erhöhen.

Ergebnis einer erfolgreichen Authentisierung ist eine Aussage wie „Das ist die Entität XYZ“. Diese Aussage kann aber in einem IT-Verbund so nicht wirklich sinnvoll weitergegeben und genutzt werden. In der digitalen Welt wird die Authentisierung daher meist von einem sogenannten **Login-Prozess** geleistet, der mehr oder weniger komplexe Algorithmen ausführt und als Ergebnis ein Datenpaket, meist Ticket oder Token genannt, erstellt. Dieses Ticket hat dann eine gewisse Gültigkeit und kann in dem dadurch vorgegebenen Zeitraum dazu verwendet werden, den Zugriff auf gewisse Daten und Funktionen des IT-Gerätes zu erlangen, wobei der Zugriff gegebenenfalls noch autorisiert werden muss.

Die **Angriffe auf Authentisierungen**– also versuchte Diebstähle digitaler Identitäten – sind vielfältig:

1. Die relevanten Eigenschaften, Geheimnisse oder Besitztümer einer natürlichen Person (also sein Kennwort, sein Fingerabdruck, seine Smartcard, ...) können gestohlen oder dupliziert werden. Beispielsweise können sogenannte **KeyLogger** hardware- oder softwareseitig in ein IT-Gerät eingeschleust werden und Kennworte beim Tippen auf der Tastatur im Klartext abgreifen.
2. Ein Ticket (also das Ergebnis einer Authentisierung) kann gestohlen werden. Hierfür kann man im Internet beispielsweise spezielle **Angriffssoftware** (Mimikatz, Pass-The-Hash, ...) frei herunterladen.

3. Die Authentifizierung kann von einem Angreifer verfälscht angeboten werden und die so erhaltenen Authentisierungsinformationen können dann an die echte Authentisierungsapplikation weitergegeben werden. Der Angreifer erhält dabei ein echtes Ticket. Angriffe dieser Form werden als **man-in-the-middle** bezeichnet.
4. Bei der Authentisierung mittels Kennworten kann die Datenbasis mit den (typisch) einfach oder mehrfach verschlüsselten bzw. gehashten Kennworten gestohlen werden. Eine **Brute Force-Attacke** prüft dann alle möglichen Zeichenketten gegen eine solche Datenbasis und kann daher früher oder später alle Kennworte im Klartext ermitteln. In sogenannten **Rainbow-Tabellen** sind die hierfür erforderlichen Hashwerte schon vorberechnet, sodass die Zeiten zur Bestimmung eines Kennwortes im Klartext recht kurz werden. Sehr erfolgreich für derartige Angriffe kann beispielsweise die frei erhältliche Software Ophcrack eingesetzt werden, die zudem Heuristiken für die typische Bildung von Kennworten berücksichtigt.

Identitätsdiebstahl ist eines der massivsten Risiken, denen ein IT-Verbund ausgesetzt ist. Effektiven Schutz auf der technischen Ebene bietet lediglich eine durchgehende Vertrauenskette, die mit einer „sicheren" Tastatur beginnt und alle an der Authentisierung beteiligten Elemente sowie das Ergebnis der Authentisierung geeignet schützt. Dazu gehören u. a.: eine „starke" Authentisierung von Eingabegeräten, der Schutz vor doppelten Eingabegeräten, das Verbot von unbekannten Prozessen zum Zeitpunkt der Authentisierung und die sichere Übergabe von Tickets und Kennworten an die Applikation bzw. das Login.

Zudem sind bei der Nutzung von Kennworten strenge Regeln (möglichst) zu erzwingen. Dazu gehören nach dem heutigen Stand der Technik u. a.:

1. Niemals Informationen (Vorname, Geburtsdatum, ...), die mit der eigenen Person oder einem Familienmitglied zusammenhängen, als Kennwort oder Teil des Kennwortes verwenden.
2. Begriffe vermeiden, die aus einem Buch stammen (könnten).
3. Verschiedene Arten von Zeichen kombinieren, also Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen (wie !@#%$*~;).
4. Dem Kennwort eine Länge von mindestens 8 (besser 10 oder 12) Zeichen geben.
5. Niemals dasselbe Kennwort für verschiedene Applikationen nutzen.
6. Keine kurzen Kennwortzyklen zulassen, also eine Wiederverwendung eines alten Kennwortes zeitlich z. B. für einige Monate auszuschließen.

In der Vergangenheit wurde außerdem empfohlen, Kennworte regelmäßig, beispielsweise alle ein bis drei Monate, zu ändern. Davon ist man mittlerweile abgekommen und Institutionen wie das BSI (in Anforderung ORP.4.A8 des IT-Grundschutz-Kompendiums) empfehlen nur noch dann, eine Kennwortänderung zu fordern, wenn ein entsprechendes Datenleck bekannt geworden ist. Grund dafür ist, dass Menschen sich nicht regelmäßig gute Kennworte ausdenken und merken können. Es gilt daher als wesentlich sicherer, wenn ein gutes Kennwort langfristig genutzt wird, als wenn Nutzer regelmäßig neue schlechte, aber gut merkbare Kennwörter festlegen.

Organisatorisch ist es dringend erforderlich, dass Zugangsdaten nicht schriftlich aufbewahrt werden. Dies gilt auch dann, wenn Kennwörter etwa in Adressbüchern oder Telefonlisten „versteckt“ werden sollen: Profis können solche „versteckten“ Kennwörter leicht ausfindig machen. Dabei ist klar, dass das Auswendiglernen gerade bei komplexen Kennworten schwierig ist. Es bietet sich dann beispielsweise an, Eselsbrücken zu nutzen.

Zudem darf man dem sogenannten **Social Engineering** keine Chance geben. Hinter diesem Begriff verbergen sich das geschickte zwischenmenschliche Beeinflussen und Manipulieren, welche darauf abzielen, den anderen zu einem bestimmten Verhalten zu verleiten. Meist geht es darum, vertrauliche Informationen (z. B. Betriebs- oder Geschäftsgeheimnisse) zu erhalten oder eine Person zu bestimmten Handlungen (z. B. Preisgabe von Kennwörtern) zu bewegen.

6.4 Sichere Speicherung von Daten

Viele Anwender glauben, dass ihre Daten auf ihren Datenträgern sicher gespeichert sind. Dies ist sowohl hinsichtlich Verfügbarkeit als auch hinsichtlich Vertraulichkeit und Integrität häufig ein Irrglaube.

Verfügbarkeit

Nicht selten werden Daten überhaupt nicht oder nur sehr unregelmäßig auf andere Datenträger kopiert. Die Folge: Kommt es beispielsweise zu einem Ausfall der lokalen Festplatte, existiert meist eine viel zu alte Datensicherung – das sogenannte Backup. Ohne ein zeitnahes Backup haben aber auch Experten wenig Chancen, die verlorenen Daten wiederherzustellen.

Je nach Häufigkeit der Datenänderungen empfiehlt es sich, bestimmte Datenbestände sogar mehrmals täglich zu sichern. Empfehlenswert ist allemal die Erstellung eines Datensicherungskonzeptes. Dieses sollte u. a. festlegen, welche Daten wann wie oft und wohin gesichert werden. Die Datensicherungsprozesse laufen idealerweise automatisiert ab. Dabei ist es wichtig, dass auch die Datensicherungen regelmäßig überprüft werden. Schließlich sind auch Speichermedien für die Datensicherungen nicht ausfallsicher.

Für das Backup kleinerer Datenbestände reichen meist die Speicherkapazitäten von DVDs oder USB-Sticks. Bei größeren Datenbeständen sind externe Festplatten oder Bandlaufwerke angezeigt. Cloud-Produkte ermöglichen es Anwendern, ihre Daten in einem Netzwerk zentral zu sichern bzw. automatisch synchronisierte Datenbestände zu verwenden.

Im Übrigen empfiehlt sich neben der Sicherung ausgewählter Daten auch die regelmäßige Sicherung des gesamten Systems (Systembackup). Kommt es nämlich beispielsweise zu einem Totalverlust der lokalen Festplatte, kann diese schnell durch eine neue

ersetzt und das Systembackup innerhalb weniger Stunden wiedereingespielt werden. Damit gelingt nicht nur das Wiederherstellen der Daten, sondern man erspart sich auch die aufwendige Neuinstallation des Betriebssystems und aller installierten Programme.

Vertraulichkeit

Der beste Weg, sensible Daten gegen einen unbefugten Zugriff durch Dritte zu schützen, ist die Verschlüsselung. Dabei nutzt man typisch ein Kennwort, welches die konkreten Parameter der Verschlüsselung nur Befugten und ihren Prozessen zugänglich macht. Dieses Kennwort ist natürlich besonders sicher zu hinterlegen. Geht es verloren, sind auch die Daten auf immer verloren.

Aktuelle Betriebssysteme (Windows, Linux, Mac OS X, Android, iOS, ...) bieten zur Verschlüsselung von Dateien bereits integrierte Verschlüsselungsmechanismen an. Alternativ kann auch kostenlose, quelloffene Software wie beispielsweise TrueCrypt (bzw. dessen „Nachfolger" VeraCrypt) oder AESCrypt genutzt werden.

Bei Verwendung eines Trusted Platform Module (TPM) bietet die Verschlüsselung von Daten die größtmögliche Vertraulichkeit. Das TPM ist eine Hardwarekomponente ähnlich einer Smartcard, die von den Herstellern in vielen neuen IT-Geräten integriert wird. Das TPM kann dann mit integrierten Verschlüsselungsmechanismen verwendet werden, um einerseits Daten zu schützen und um andererseits u. a. sicherzustellen, dass ein IT-Gerät nicht manipuliert wurde, während es ausgeschaltet war.

Cloud-Services ermöglichen es Anwendern, ihre Daten vollständig auf externen Servern zu speichern. Sie erlauben dadurch den Zugriff auf ihre Daten zu jeder Zeit und von jedem Ort der Welt mit unterschiedlichsten IT-Geräten, was die Flexibilität natürlich erheblich erhöht.

Das bringt aber auch neue Risiken mit sich: Das Auslagern der Daten auf externe Server und der Zugriff darauf über „Third-Party-Software" birgt ein hohes Vertraulichkeitsrisiko. Der effektivste Weg, dieses Risiko abzumildern, ist die Verschlüsselung von Daten vor dem Senden in die Cloud. Damit ist gewährleistet, dass auch bei Diebstahl oder Spionage die erlangten Daten nicht verwendet werden können.

Integrität

Integrität von Daten bedeutet die Konsistenz des Datenbestandes, damit darauf zugreifende Applikationen verlässlich arbeiten können. Diese kann organisatorisch etwa durch die Nutzung des Biba-Modells gefördert werden.

Technische Maßnahmen zur Sicherstellung der Integrität zielen darauf ab, fehlerhafte Daten als solche zu erkennen und gegebenenfalls (automatisch) zu korrigieren. Hier kommen oft sogenannte File Integrity Checker zum Einsatz, die unter Nutzung eines Hashverfahrens eine digitale Signatur einer Datei erstellen. Der Klassiker ist in diesem

Zusammenhang das Produkt Tripwire. Diese digitalen Signaturen von Dateien werden dann separat gespeichert und in der Folge genutzt, um Veränderungen schnell und zuverlässig zu erkennen.

6.5 Sichere Vernichtung von Daten

Sollen Speichermedien wie etwa Festplatten, USB-Sticks, DVDs oder Speicherkarten entsorgt werden, muss sichergestellt sein, dass gegebenenfalls noch vorhandene Daten nicht in falsche Hände geraten. Dies kann dadurch ausgeschlossen werden, dass Datenträger mechanisch zerstört werden. Bei optischen Speichermedien reichen zwar theoretisch einige Sekunden in der Mikrowelle, aber wegen Funkenflug und entstehender gefährlicher Dämpfe sollte besser ein CD/DVD-Shredder oder Zerschneiden bzw. Zerkratzen verwendet werden. Bei magnetischen Festplatten kann man diese vor der Entsorgung aufschrauben und die magnetischen Scheiben zerstören.

Ist dies nicht möglich, muss der Datenträger effektiv gelöscht werden. Aus Untersuchungen weiß man jedoch, dass nahezu 90 Prozent aller ausgemusterten Festplatten noch wiederherstellbare Daten enthalten. Bei einem Formatieren oder Löschen werden die Speicherorte der Daten auf einem Datenträger nämlich nur freigegeben. Die Daten befinden sich jedoch weiterhin auf dem Datenträger und können, sofern der scheinbar freigewordene Speicherplatz noch nicht mit neuen Daten überschrieben wurde, mit geeigneten Programmen wiederhergestellt werden.

Angezeigt ist folglich die Verwendung von Spezial-Software zum Löschen von Daten und zum Formatieren von Datenträgern. Diese überschreiben den frei gewordenen Speicherplatz einmal oder mehrfach mit unterschiedlichsten Bitmustern. Danach können die alten Daten nicht wiederhergestellt werden. Neben kommerziellen Angeboten gibt es kostenfreie Alternativen, die Daten sicher löschen. Dazu gehören unter anderem Eraser, CBL Datenschredder, Secure Eraser und Darik's Boot and Nuke (DBAN).

Zusammenfassung

IT-Geräte können bereits mit wenigen, bewährten Maßnahmen ziemlich sicher genutzt werden. Zu diesen Maßnahmen gehören insbesondere:

1. Software und Hardware stets auf dem neuesten Stand halten.
2. Virenscanner verwenden und regelmäßig aktualisieren.
3. Komplexe Kennworte verwenden und diese sicher aufbewahren.
4. Prinzipiell nicht mit Administratorrechten arbeiten.
5. Vorsicht bei unbekannten E-Mail-Anhängen.
6. Daten regelmäßig sichern.
7. Sensible Daten durch Verschlüsselung schützen.
8. Sensible Informationen nicht leichtfertig preisgeben.

Wissenskontrolle

Haben Sie diese Lektion verstanden?

Dann haben Sie jetzt die Möglichkeit, das Gelernte auf unserer Lernplattform zu überprüfen.

Viel Erfolg!

Lektion 7

Ausgewählte Schutz- und Sicherheitskonzepte für IT-Infrastrukturen

LERNZIELE

Nach der Bearbeitung dieser Lektion werden Sie wissen, ...

- ... wie – auf konzeptioneller Ebene – wesentliche Teile von IT-Infrastrukturen sicher beschafft, konfiguriert und betrieben werden können.
- ... wie unerlaubte Datenübertragung verhindert werden kann.
- ... was Notfallpläne für Datenschutz und IT-Sicherheit leisten können.

7. Ausgewählte Schutz- und Sicherheitskonzepte für IT-Infrastrukturen

Einführung

Prism ist ein System, mit dessen Hilfe staatliche Einrichtungen die Internetaktivitäten von Menschen lückenlos überwachen können. Genauer gesagt: die Daten all jener, die Produkte und Dienstleitungen von u. a. Google, YouTube, Facebook, Microsoft, Skype, AOL, Yahoo und Apple nutzen. Aufgedeckt hat Prism der Whistleblower Edward Snowden im Jahre 2013. Der Kern von Prism ist eine Schnittstelle zum Aufschalten auf Verkabelungen, über die dann Daten von den Firmen an die staatlichen Einrichtungen übermittelt werden. Die staatliche Einrichtung schickt einfach einen Gerichtsbeschluss mit der Datenanforderung, in dem der Firma zugleich unter Strafandrohung verboten wird, diese Datenübermittlung publik zu machen.

Täter aus dem linken Spektrum stiegen im Oktober 2014 in Berlin-Charlottenburg in einen gesicherten Schacht, in dem bündelweise Glasfaserkabel der Firma Kabel Deutschland lagen. Etwa 400 Leitungen wurden durchtrennt. Nach Angaben der Polizei waren 160.000 Haushalte danach ohne Fernsehen, Internet und Telefon.

Um dem Staub in den von ihnen angemieteten Serverräumen Herr zu werden, machten sich die Mieter eines Rechenzentrums selbst an die Reinigungsarbeiten. An ein kleines, aber – wie sich herausstellte – bedeutendes Detail dachten sie dabei leider nicht: Zur Ausstattung der Serverräume gehörte auch eine spezielle Löschanlage, die mit einem nicht ganz billigen Edelgas befüllt war. Die Mieter des Rechenzentrums vergaßen, die Löschanlage vor dem Putzen auszuschalten. Und so kam es wie es kommen musste: der aufgewirbelte Staub löste die Löschanlage aus. Am Ende ergab sich ein Sachschaden in Höhe von über 80.000 Euro.

Die vorangegangenen Beispiele verdeutlichen die Bandbreite möglicher Sicherheitsprobleme für IT-Infrastrukturen. Diese Lektion gibt einen ersten Einblick in Sicherheitskonzepte für deren Schutz, insbesondere für den Schutz von Netzwerken.

7.1 Objektschutz

Objektschutz ist der Schutz von Gebäuden, Räumen und Inventar vor Ereignissen, die einen Verlust oder Schaden verursachen können. Dazu gehört der Schutz vor Feuer, Naturkatastrophen, Einbrüchen, Diebstahl, Vandalismus und – neuerdings auch bei uns – Terrorismus.

Schützenswerte Räume einer IT-Infrastruktur sind z. B. der Serverraum, das Datenträgerarchiv und die Klimazentrale. Solche Räume sollten niemals Hinweise auf ihre Nutzung tragen. Türschilder wie „SERVERRAUM“ geben einem potenziellen Angreifer wertvolle Hinweise, um seine Aktivitäten gezielter und damit Erfolg versprechender durchzuführen.

Der Zutritt zu schützenswerten Räumen ist verbindlich zu regeln und lückenlos zu kontrollieren. Die Zutrittsregelungen sind nach Tageszeiten, Orten und Rollen zu differenzieren. Die möglichen Systeme zur Zutrittskontrolle reichen dabei von einem einfachen Schloss bis zu aufwendigen Zutrittssystemen etwa mit Fingerabdruckscannern. Die Ausgestaltung dieser Systeme sollte jedoch dem Grundsatz folgen, dass einfache und praktikable Lösungen oft ebenso effizient sind wie aufwendige Technik. Die eingesetzten Systeme zur Zutrittskontrolle müssen gegen Manipulationen geschützt werden. Daneben müssen diese so angebracht werden, dass Vertraulichkeit bei der Eingabe von Daten gewährleistet ist.

Ein Serverraum ist – wie bereits erwähnt – ein besonders schützenswerter Raum, daher sollten dort nur die Administratoren der dort vorhandenen IT-Geräte Zutritt haben. In einem Serverraum sollten sich zudem auf keinen Fall Geräte befinden, die den Zutritt für einen großen Benutzerkreis erforderlich machen, wie z. B. Drucker oder Fotokopierer. Brennbare Materialen wie Druckerpapier sollten ebenfalls nicht in einem Serverraum gelagert werden.

7.2 Schutz vor unerlaubter Datenübertragung

Netzwerke auf TCP/IP-Basis sind heute nahezu unverzichtbare Bestandteile von IT-Verbünden. Sie dienen vor allem der zeitnahen Übertragung von beliebigen Daten, bergen somit aber auch die Gefahr, dass nicht autorisierte Datenübertragungen stattfinden und so beispielsweise Geschäftsgeheimnisse abfließen.

In TCP/IP-Netzwerken ist eine Firewall wie ein Router ein eigenständiges Gerät, das mehrere (einheitliche) Netzwerke miteinander verbindet. Zusätzlich zu den Funktionalitäten eines Routers bietet aber eine Firewall auch Schutz vor unerlaubter Datenübertragung, indem sie jedes ein- und ausgehende Datagramm analysiert und – entsprechend vordefinierter Regeln – die Weiterleitung des Datagramms vornimmt oder unterbindet.

In der Regel kontrolliert eine Firewall den Datenverkehr an besonders kritischen Stellen in Netzwerken. Firewalls, die jedes ein- und ausgehende Datagramm mittels einer sorgfältigen Analyse einem Datenstrom zuordnen, das Anwendungsprotokoll verifizieren, sowohl den Absender als auch den Empfänger zweifelsfrei bestimmen und – darauf basierend – ihre Regeln anwenden, sind heutzutage Stand der Technik und können – bei gezieltem Einsatz von Whitelisting – sehr effektiv schützen, wobei Whitelisting bekanntlich bedeutet, dass alles, was nicht ausdrücklich erlaubt ist, verboten ist. Um zudem unerlaubte Datenübertragungen auch über verschlüsselte Tunnel zu erkennen, ist die Fähigkeit des Aufbrechens von TLS/SSL-Verbindungen durch eine Firewall mit anschließender Regelanwendung heutzutage meist unverzichtbar.

Als somit zentralem Bestandteil einer sicheren IT-Infrastruktur muss der Beschaffung, der Konfiguration und dem Betrieb einer Firewall besondere Aufmerksamkeit zukommen. Firewalls sollten nur von autorisierten und vertrauenswürdigen Lieferanten bezo-

gen werden. Im besten Fall sind die Geräte ohne Umweg direkt vom Hersteller zu beschaffen. Nur vom Hersteller einer verlässlichen Firewall kann man schnelle Reaktionen auf Sicherheitslücken erwarten.

Im Betrieb muss eine Firewall die Möglichkeit bieten, die Vertraulichkeit der durchgeleiteten Daten sicherzustellen. Dazu muss sie Verschlüsselungen mit modernen Algorithmen und sicheren Parametern ermöglichen. Sie muss zudem die Möglichkeit bieten, dass Sende- und Empfangsaktivitäten nur nach einer „starken" Authentisierung des Anwenders gestattet werden. Der Zugang zur Konfiguration der Firewall muss durch verschiedene Maßnahmen besonders geschützt werden. Diese sollten einen verschlüsselten Übertragungskanal mit einer sicheren Authentifizierung (z. B. HTTPS bei einem Webzugang, SSH für einen Konsolenzugang) umfassen.

Zur Wahrung der Integrität der durchgeleiteten Daten einer Firewall ist vor allem eine besonders „gehärtete" Plattform entscheidend. Zusätzlich ist beim Einsatz von SSL eine gründliche Prüfung von SSL-Zertifikaten notwendig, um Man-in-the-middle-Angriffe auszuschließen.

Um die Verfügbarkeit einer Firewall sicherzustellen, sind entsprechende Anforderungen an die Hardware zu stellen. Hier muss der Hersteller nachweisen können, dass die Plattform entsprechend konzipiert wurde. Dies verlangt zum Beispiel redundante Netzteile, **RAID** für Massenspeicher und eine Lüfter-Konfiguration, bei der ein einzelner Ausfall nicht zu einem Ausfall des Gerätes führt. Da diese Maßnahmen alleine in der Praxis aber gelegentlich noch nicht ausreichen, um einen Ausfall der Hardware zu verhindern, sollte die Möglichkeit eines redundanten Betriebs gegeben sein. Die Überwachung einer Firewall spielt ebenfalls eine zentrale Rolle, damit defekte Hardware rechtzeitig erkannt wird. Hier muss der Hersteller ein entsprechendes Monitoring z. B. mittels SNMP anbieten.

RAID (Redundant Array of Inexpensive bzw. Independent Disks) ist die Sammelbezeichnung für verschiedene Konzepte, die durch einen geschickten Einsatz von Festplatten für ausfallsichere, hochleistungsfähige Systeme sorgen.

7.3 Schutz vor unerwünschtem Datenverkehr

DoS (Denial of Service)-Angriffe zielen darauf ab, Netzwerke und damit auch die in Netzwerken angebotenen Dienste lahmzulegen. Dies wird typischerweise dadurch erreicht, dass ein im anzugreifenden Netzwerk angebotener Dienst so stark mit Anfragen „bombardiert" wird, dass er regulären Anfragen nicht mehr nachkommen kann. Im Zusammenhang mit DoS-Angriffen werden oft Datenraten von über 300 Gigabit pro Sekunde beobachtet.

Bei Distributed DoS-Angriffen (DDoS) wird ein DoS-Angriff von mehreren Teilnehmern gleichzeitig ausgeführt. DDoS-Angriffe können auch von einem Bot-Netz ausgeführt werden. Ein Bot-Netz ist eine Gruppe von Netzwerkgeräten, die sich aus der Ferne steuern lassen. Meistens wissen die Besitzer gar nicht, dass ihre Geräte Teil eines Bot-Netzes sind. DoS- und DDoS-Angriffe sind nach deutschem Recht strafbar (§ 303b StGB Computersabotage).

Leider ist es schwierig, sich gegen DoS-Angriffe zu schützen: Dienste können reguläre Anfragen nur selten von „bösen“ unterscheiden. Daher gilt es vor allem, unnötige Dienste (wie etwa den Echo-Dienst auf Port 7) vollständig abzuschalten. Bei Überlastungen eines Dienstes, die nur von einem oder wenigen Angreifern verursacht werden, kann eine Dienstverweigerung mithilfe von einfachen Sperrlisten vollzogen werden, die von einer Firewall erzwungen werden (Blacklisting). Blacklisting ist allerdings weniger sicher als Whitelisting, und beispielsweise das BSI fordert daher im IT-Grundschutz-Kompendium, Baustein NET.1.1, dass Firewalls nach dem Prinzip des Whitelistings arbeiten. Eine weitere mögliche Gegenmaßnahme gegen Überlastungen ist die sogenannte Lastverteilung, bei der der betroffene Dienst auf mehreren IT-Geräten ausgeführt wird. Letztere Maßnahme wäre auch bei DDoS-Angriffen wirksam.

Je nach Bedrohungslage empfiehlt sich die Installation von Systemen, die Angriffe aufgrund typischer Angriffsmuster erkennen und entsprechende Gegenmaßnahmen auslösen können. Zu diesen Systemen gehört u. a. ein Intrusion-Prevention-System (IPS). Es wird in einem Netzwerk installiert und sammelt dann kontinuierlich Informationen über das Netzwerk und dessen aktuellen Zustand, um anhand von in einer Datenbank hinterlegten Mustern bzw. Heuristiken Angriffe zu erkennen und dann zuvor definierte Gegenmaßnahmen auszulösen. Als Maßnahme gegen einen DoS-Angriff kann ein IPS beispielsweise nach Erkennen einer erhöhten Netzwerkaktivität automatisch Firewall-Regeln so anpassen, dass der Angriff abgemildert oder gar gestoppt wird.

7.4 Schutz durch Notfallplanung

Zu der Notfallplanung eines IT-Verbundes gehört jegliche Vorsorge zur Aufrechterhaltung oder Wiederherstellung von IT-Anwendungen im Falle unvorhergesehener Ereignisse oder Störungen.

Notfallplanung erfordert ein systematisches Vorgehen. Am Anfang sollte stets eine sogenannte Business Impact Analysis (BIA) stehen. Die zentrale Aufgabe einer BIA ist es zu verstehen, welche IT-Anwendungen wichtig für die Aufrechterhaltung des Geschäftsbetriebs und damit für die Institution sind und welche Folgen ein Ausfall dieser IT-Anwendungen haben kann. Es existieren viele Methoden und Wege, eine BIA durchzuführen. Wie die erforderlichen Ergebnisse ermittelt werden, kann jede Institution für sich entscheiden. In BSI-Standard 100–4 (vgl. Bundesamt für Sicherheit in der Informationstechnik 2008) wird beispielsweise eine Methode vorgestellt, die an die Schutzbedarfsfeststellung nach BSI-Standard 200–2 (vgl. Bundesamt für Sicherheit in der Informationstechnik (2017b) angelehnt ist.

Die gewählte Methode zur Durchführung einer BIA sollte mindestens folgende Arbeitsschritte enthalten:

- Es ist zu analysieren und zu bewerten, wie sich ein Ausfall von IT-Anwendungen auf die Institution auswirken und wie sich Schäden während dieser Zeit entwickeln können.
- Für die IT-Anwendungen sind die Wiederanlaufparameter zu identifizieren bzw. festzulegen. Dazu zählen:
  - die maximal tolerierbare Ausfallzeit,
  - die Wiederanlaufzeit,
  - das Wiederanlaufniveau und
  - der maximal zulässige Datenverlust.

Mit den Ergebnissen der BIA erfolgt anschließend eine Risikoanalyse, die eine Maßnahmenauswahl und eine Priorisierung dieser Maßnahmen zum Ziel hat. Diese münden in eine Notfallplanung, die es umzusetzen gilt. Jede konkrete Vorsorgemaßnahme muss sich letztlich auf die Notfallplanung zurückführen lassen. Aus diesem Grund muss diese sorgfältig erstellt und umgesetzt werden.

Bei der Notfallplanung sind selbstverständlich der Datenschutz und die IT-Sicherheit zu berücksichtigen. Es ist sicherzustellen, dass im Falle eines Ausfalls, bei der Inbetriebnahme und dem Betrieb von Ausweichlösungen und bei der Wiederaufnahme des Normalbetriebs sowohl Datenschutz als auch IT-Sicherheit gewährleistet sind. Dazu gehört unter anderem die Gewährleistung der Vertraulichkeit von Daten (z. B. Zugriffsrechte, Verschlüsselung), Einhaltung der Minimalanforderungen an die Datensicherung und die Einhaltung gesetzlicher Vorgaben (z. B. Archivierung von geschäftsrelevanten Daten).

Die Möglichkeiten zur Überprüfung der eigenen Notfallplanung sind vielfältig. Sie reichen von einfachen Überprüfungen von Einzelmaßnahmen bis hin zu komplexen Übungen.

Beispiele für mögliche Notfälle in der Arztpraxis Dr. med. Heilemacher sind etwa:

- Feuer im Gebäude,
- Stromausfall,
- Ausfall des Servers für das Praxisverwaltungssystem S-1.

Zu diesen und weiteren Notfällen müsste dann eine Notfallplanung konkrete Verhaltensmaßnahmen aufführen. Diese könnten etwa bei „Feuer im Gebäude“ das RRR-Prinzip „Retten-Räumen-Raus“ vorschreiben, in dem – bei gebotener Eigensicherung – Patienten aus der Praxis schnellstmöglich ins Freie geschafft werden. Voraussetzung hierfür ist natürlich, dass regelmäßig geprüft wird, ob Fluchtwege nicht verstellt sind. Zudem sind regelmäßig entsprechende Räumungsübungen durchzuführen.

Bei „Stromausfall“ wäre die Benachrichtigung der technischen Hilfsdienste (Hausmeister etc.) angezeigt, deren Kontaktinformationen (auf einem Kommunikationsweg, der auch bei Stromausfall noch funktioniert) gut sichtbar in der Praxis anzubringen wären.

Zusammenfassung

IT-Infrastrukturen erfordern aus Sicht des Datenschutzes und der IT-Sicherheit vielfältige Schutzmaßnahmen. Minimal gilt es ...

1. ... den Zugang zu Gebäuden und Räumen wirksam zu reglementieren.
2. ... den Datenverkehr in Netzwerken durch Firewalls einschlägig zu kontrollieren.
3. ... Überlastungen von Netzwerken zu erkennen und gegenzusteuern.
4. ... auf Notfälle bestens vorbereitet zu sein.

Wissenskontrolle

Haben Sie diese Lektion verstanden?

Dann haben Sie jetzt die Möglichkeit, das Gelernte auf unserer Lernplattform zu überprüfen.

Viel Erfolg!

HERZLICHEN GLÜCKWUNSCH

Sie sind nun am Ende dieses Kurses angelangt. Wenn Sie Ihr Wissen auf der Lernplattform unter Beweis gestellt haben, führen Sie bitte die abschließende Evaluierung des Kurses durch. Für die Abschlussprüfung wünschen wir Ihnen viel Erfolg.

Anhang 1

Literaturverzeichnis

Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik (2008): *BSI-Standard 100–4. Notfallmanagement.* (URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard04/ITGStandard04_node.html [letzter Zugriff: 06.03.2018]).

Bundesamt für Sicherheit in der Informationstechnik (2017a): *BSI-Standard 200–1. Managementsysteme für Informationssicherheit.* (URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard201/ITGStandard201_node. [letzter Zugriff: 30.01.2018]).

Bundesamt für Sicherheit in der Informationstechnik (2017b): *BSI-Standard 200–2. IT-Grundschutz-Vorgehensweise.* (URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard202/ITGStandard202_node. [letzter Zugriff: 30.01.2018]).

Bundesamt für Sicherheit in der Informationstechnik (2017c): *BSI-Standard 200–3. Risikoanalyse auf der Basis von IT-Grundschutz.* (URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard203/ITGStandard203_node. [letzter Zugriff: 30.01.2018]).

Bundesamt für Sicherheit in der Informationstechnik (2018): *IT-Grundschutz-Kompendium – Edition 2018* (URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html) [letzter Zugriff: 20.03.2018]).

Bundesministerium der Finanzen (2014): *Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD).* (URL: http://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/Datenzugriff_GDPdU/2014–11–14-GoBD.pdf?__blob=publicationFile&v=1 [letzter Zugriff: 23.01.2017]).

Davies, D. (2019): *Edward Snowden Speaks Out: 'I Haven't And I Won't' Cooperate With Russia.* (URL: https://text.npr.org/761918152 [letzter Zugriff: 22.04.2021]).

Doe, J. (2016): *Locky. Richtig entfernen? (Anleitung für die Deinstallation).* (URL: https://dieviren.de/locky/ [letzter Zugriff: 14.02.2018]).

Eckert, C. (2014): *IT-Sicherheit: Konzepte – Verfahren – Protokolle.* 9. Auflage, De Gruyter Oldenbourg, München.

Fraunhofer-Institut für Sichere Informationstechnologie (SIT) (2011): *Webkurs IT-Grundschutz.* Bundesamt für Sicherheit in der Informationstechnik (URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzAbout/ITGrundschutzSchulung/SchulungdesBSI/webkurs.html [letzter Zugriff: 06.03.2018]).

Literaturverzeichnis

Kassenärztliche Bundesvereinigung (KBV) (2016): *Anforderungen an Hard- und Software in der Praxis. Hinweise zum Datenschutz.* (URL: http://www.kbv.de/media/sp/KBV_ITA_SIEX_Anforderungen_Praxis.pdf [letzter Zugriff: 14.02.2018]).

Spindler, G. (2007): *Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären.* Bundesamt für Sicherheit in der Informationstechnik (URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=2 [letzter Zugriff: 14.02.2018]).

Anhang 2

Abbildungsverzeichnis

Abbildungsverzeichnis

IU Internationale Hochschule GmbH
IU International University of Applied Sciences
Juri-Gagarin-Ring 152
D-99084 Erfurt

Postanschrift:
Albert-Proeller-Straße 15-19
D-86675 Buchdorf