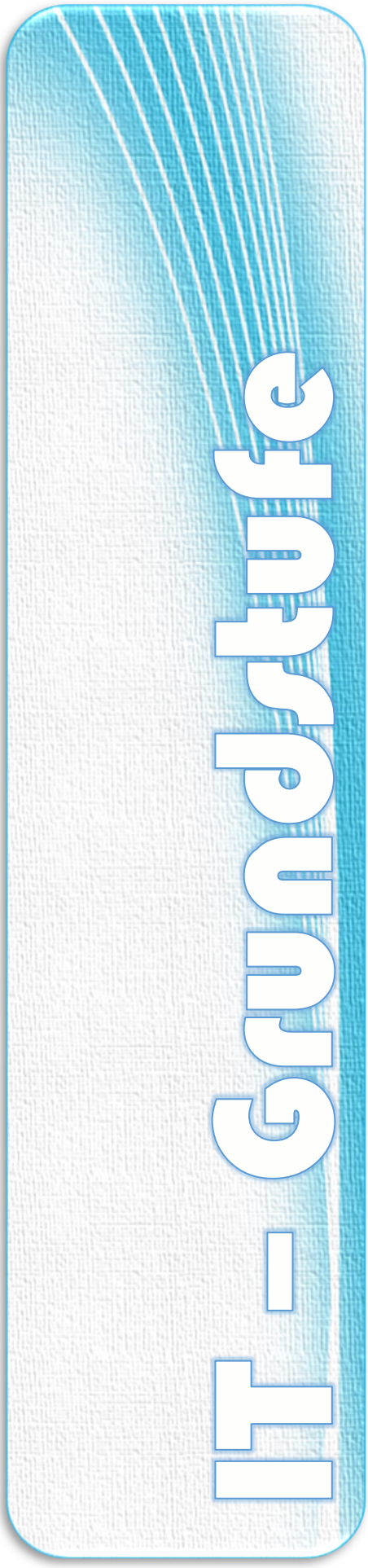


bfw
Unternehmen für Bildung.

Schutzbedarfsanalyse im eigenen Arbeitsbereich durchführen

Modul: **ITG / D**

Version: 1.0
Oktober 2021

Erstellt von: Markus Bohnenkamp

Modul: **ITG / D - Schutzbedarfsanalyse im eigenen Arbeitsbereich durchführen**

Version, Datum: 1.0, Oktober 2021

Erstellt von: Markus Bohnenkamp

Alle Rechte vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotokopie oder einem anderen Verfahren) ohne Genehmigung des Herausgebers reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Die Modulunterlage und alle ihre Bestandteile wurden mit großer Sorgfalt erstellt und geprüft. Dennoch können Fehler nicht vollkommen ausgeschlossen werden. Der Herausgeber und die Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Literaturhinweis

Titel: IT-Berufe Grundstufe

ISBN: 978-3-14-220000-2

Verlag: Westermann Gruppe

Inhalt

TAG 1 - Grundlagen zur Informationssicherheit erarbeiten 6
LE 1 - Einführung, Verantwortung, Zuständigkeiten und Sicherheitsbereiche beschreiben 6
(1) Sensibilisierung der Verantwortlichen 7
(2) Einführung und geeignete Informationsquellen 7
(3) Verantwortliche Stellen 8
LE 2 - Gesetze und Standards zur Informationssicherheit unterscheiden 10
(1) IT-Sicherheit (IT-Security) 11
(2) Datenschutz - Schutz personenbezogener Daten 12
(3) Urheberrecht, Copyright, Markenrecht und Lizenzrecht 13
Lernzielkontrolle TAG 1 17
TAG 2 - IT-Grundschutz, Schutzziele, Gefährdungen, Schadensszenarien unterscheiden 22
LE 1 - IT-Grundschutz nach dem BSI 23
LE 2 - Schutzziele nach IT-Grundschutz 25
LE 3 - Gefährdungen und Anforderungen 27
LE 4 - Schadenszenarien und Schadenskategorien 29
Lernzielkontrolle TAG 2 31
TAG 3 - Aktuelle Bedrohungen zur IT-Sicherheit von Unternehmen präsentieren 34
LE 1 - Aktuelle Sicherheitsmeldungen in Portalen 34
LE 2 - Malware unterscheiden 36
LE 3 - APT, Botnetze und DDoS-Angriffe 38
Lernzielkontrolle TAG 3 40
TAG 4 - Identitätsdiebstahl und Social Engineering begegnen 41
Lernzielkontrolle TAG 4 47
TAG 5 - Technisch-organisatorische Maßnahmen und Beiträge zum Sicherheitskonzept erstellen 50
Lernzielkontrolle TAG 5 53
TAG 6 - Schutzbedarfsfeststellungen anhand eines Beispielunternehmens des BSI vorbereiten 56
LE 1 - Phasen des Sicherheitsprozesses nach dem BSI-Grundschutz beschreiben 56
LE 2 - Den Prozess von der Sicherheitsleitlinie zur Schutzbedarfsfeststellung beschreiben 57
(1) Entwicklung einer Sicherheitsleitlinie 57
(2) Sicherheitskonzept 58
(3) Strukturanalyse 59
(4) Schutzbedarfsfeststellung 60
LE 3 - Elemente der Schutzbedarfsfeststellungen im Beispielunternehmen präsentieren 61
Lernzielkontrolle TAG 6 64
TAG 7 und 8 - Schutzbedarfsfeststellung in Arbeitsbereichen von JIKU IT-Solutions durchführen 65
LE 1 - Den Schutzbedarf bezüglich der Arbeitsplatzsoftware feststellen 65
(1) Gefährdungslage 65
(2) Schutzbedarf 66
(3) Generelle Schutzmaßnahmen 68
(4) Beispielhafte Schutzmaßnahmen für Betriebssysteme 69
(5) Schutzmaßnahmen für Office-Produkte 70
(6) Gefährdungslage und Schutzmaßnahmen beim Einsatz von (Software-)Containern 71

LE 2 - Den Schutzbedarf bezüglich der Clients eines Arbeitsplatzes feststellen 73
(1) Gefährdungslage 73
(2) Schutzbedarfsfeststellung 74
(3) Schutzmaßnahmen 76
LE 3 - Den Schutzbedarf bezüglich des Austausches von Daten mithilfe von mobilen Datenträgern feststellen 78
(1) Gefährdungslage 79
(2) Schutzbedarfsfeststellung 80
(3) Schutzmaßnahmen 81
Lernzielkontrolle TAG 7 und 8 83
TAG 9 – Lernsituationen und Aufgaben bearbeiten 85
TAG 10 - Vertiefung des Wissens und Modulprüfung 86
LE 2 - Modulprüfung 86
Lösungen: 87
TAG 1 87
TAG 5 88
TAG 3 89
TAG 4 90
TAG 5 90
TAG 6 90
TAG 7 und 8 91
TAG 9 91

In Modul D werden Gesetze, Standards und Maßnahmen zur Sicherstellung eines IT-Grundschutzes vorgestellt. Die wichtigsten Gesetze zur Informationssicherheit werden herausgestellt und Anforderungen zum IT-Grundschutz, Schutzziele und Schadensszenarien präsentiert. Dabei wird ein Fokus auf aktuelle Bedrohungen wie Identitätsdiebstahl und Social Engineering gelegt. Zur Gewährleistung von IT-Sicherheit ist ein auf das Unternehmen zugeschnittene Sicherheitskonzept zentral, weswegen in diesem Lernfeld besonders auf technisch-organisatorische Maßnahmen und die Schutzbedarfsfeststellung eingegangen wird. Dabei orientiert sich das vorgestellte Konzept am IT-Grundschutzkurs des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Informationssicherheit ist in einem Ausbildungsbetrieb wie der JIKU IT-Solutions sehr wichtig. Die Eingangstüren sind gesichert und Kameras zeigen den Besuchern an, dass dieses Gelände videoüberwacht wird. Bei Erstbesuchen werden Auszubildende wie andere Besucher zunächst in den Warteraum begleitet und dürfen die weiteren Räume nicht ohne Begleitung von JIKU-Mitarbeitern betreten. Bis auf die Geschäftsführung sind alle Mitarbeiter einheitlich gekleidet, sodass man fremde Personen im Haus schnell erkennen kann. Alle Mitarbeiter erhalten regelmäßige Sicherheitsschulungen.

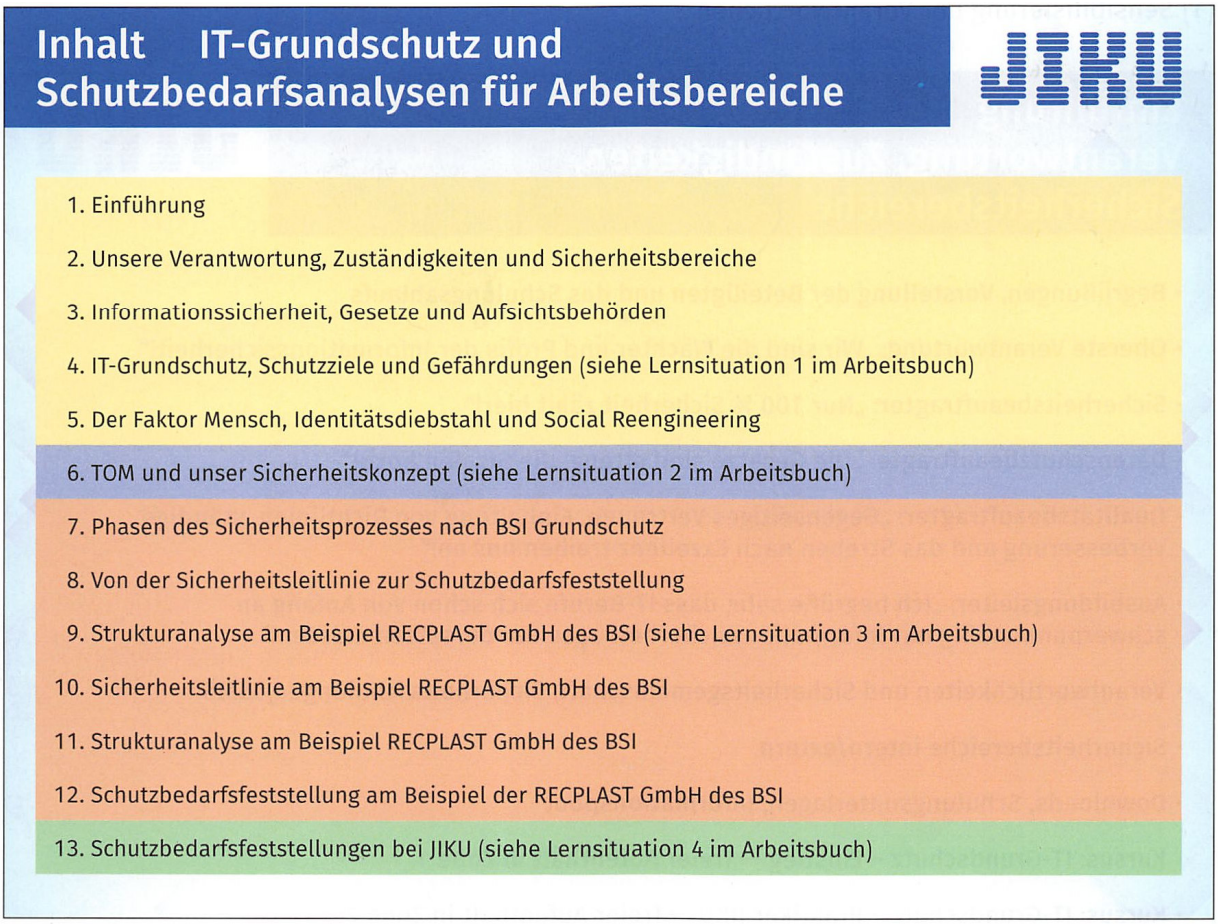
Eine ständige Arbeitsgruppe unter der Leitung eines IT-Sicherheitsbeauftragten tagt regelmäßig, um die Sicherheitslage im Systemhaus sowie die Systeme der Kunden auf dem neuesten Stand zu halten und Änderungen je nach Lage schnell vornehmen zu können.

Alle Mitarbeiter dürfen sich erst dann selbstständig in den Sicherheitszonen aufhalten, wenn sie verschiedene Grundschutzschulungen erfolgreich absolviert haben. Hierbei lernen sie auch alle Beauftragten kennen, die in Fragen der Informationssicherheit zuständig sind.

TAG 1 - Grundlagen zur Informationssicherheit erarbeiten

Sie sollen Gesetze, Standards und Maßnahmen zur Sicherstellung eines IT-Grundschutzes kennenlernen.

Grundschutzschulungen, wie sie in Systemhäusern wie der JIKU IT-Solutions für alle Mitarbeiter durchgeführt werden, dienen der Einführung in den IT-Grundschutz, in wichtige Gesetze und Schutzziele. Die folgende Übersichtsfolie zeigt den Ablauf beispielhaft.



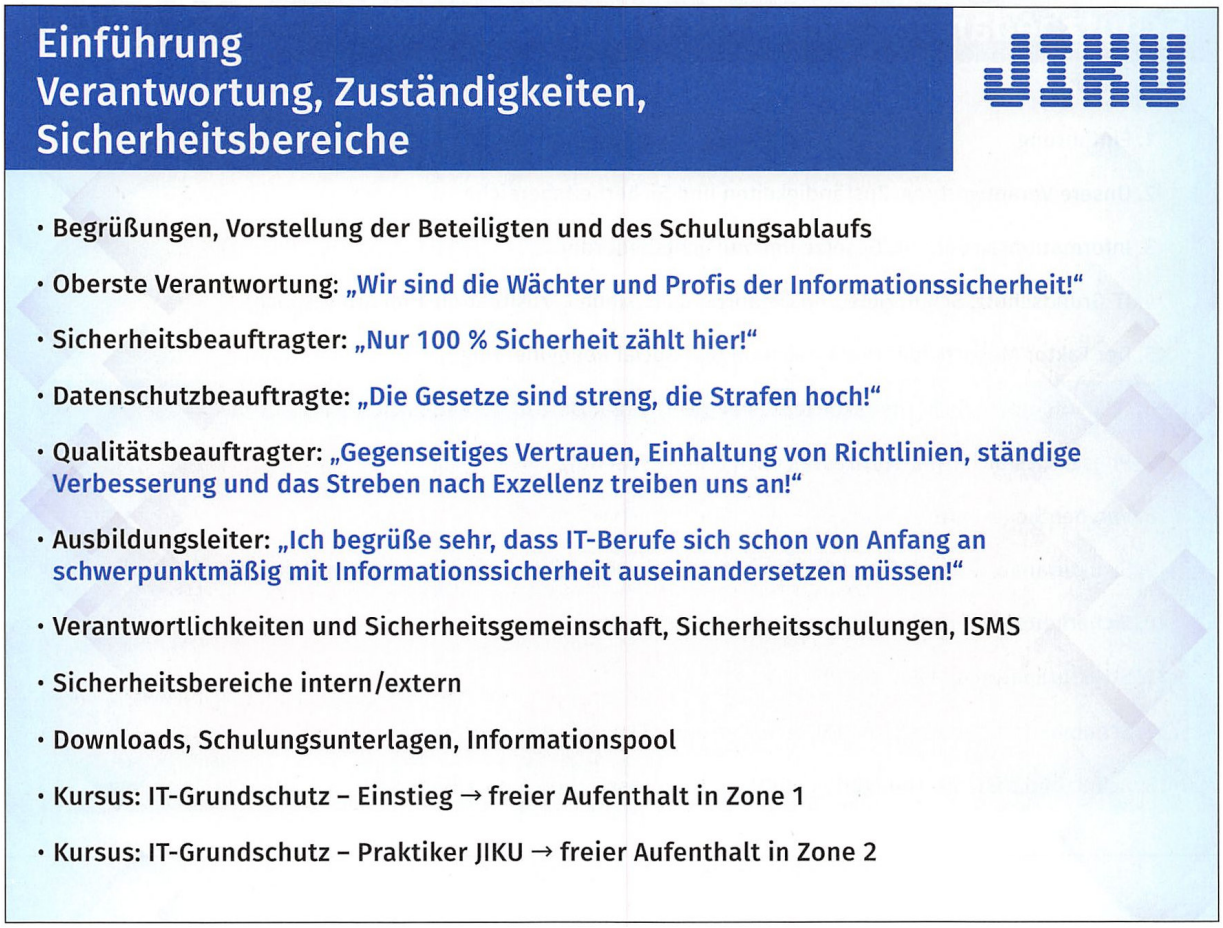
LE 1 - Einführung, Verantwortung, Zuständigkeiten und Sicherheitsbereiche beschreiben

Sie wollen die Verantwortlichkeits-, Zuständigkeits- und Sicherheitsbereiche kennenlernen.

In Sicherheitsfragen hohe Anerkennung bei Kunden zu erfahren ist ein wichtiges Anliegen für IT-Unternehmen. Laufend muss die Sicherheitslage im Blick behalten werden, um in Notfällen sofort eingreifen zu können. Die Sammlung an Notfallplänen und die Datenbank an Bedrohungen werden laufend ergänzt und angepasst.

In der IT-Sicherheit darf man sich nicht viele Fehler leisten und es muss ständig Vorsorge getroffen werden, damit es nicht zu existenzgefährdenden Notfällen im Haus und bei den Kunden kommen kann. Von allen Mitarbeitern wird erwartet, dass sie aktiv mitarbeiten und sensibel darauf achten, dass keine Sicherheitslücken entstehen.

(1) Sensibilisierung der Verantwortlichen



Viele Mitarbeiter sind an einem gelingenden Konzept beteiligt und die Bedeutung der IT-Sicherheit für ein Systemhaus wie JIKU IT-Solutions und die Kunden-IT kann nicht genug hervorgehoben werden.

In einem Systemhaus werden Sicherheitsregeln für viele Anwendungsbereiche erstellt, die die Mitarbeiter beachten müssen. Nur ausgebildete Mitarbeiter dürfen allein zu Kunden. Auch hier ist es wichtig, die zuständigen Beauftragten für Sicherheit zu kennen und die Sicherheitsregeln der Kunden zu befolgen.

(2) Einführung und geeignete Informationsquellen

Gefährdungen der Informationstechnik sowie die technischen und organisatorischen Maßnahmen sind zahlreich. Mitarbeiter müssen sich immer auf dem aktuellen Stand halten und sich selbstständig informieren. Der IT-Sicherheitsbeauftragte der JIKU IT-Solutions, Herr Franke, wird zentral fast täglich Sicherheitsmeldungen bekannt machen. Hunderte von Informations- und Beratungsstellen und viele Anbieter stellen Leistungen zur IT-Sicherheit zur Verfügung. Nur ein Netzwerk aller Beteiligten kann sich heute der Herausforderung der Cyberkriminalität erfolgreich stellen. Bei JIKU werden daher immer wieder weitere Informationsquellen genannt.

Die wichtigste Informationsquelle der Informationstechnik ist das **Bundesamt für Sicherheit in der Informationstechnik (BSI)**. Hier arbeiten täglich viele Mitarbeiter daran, die in Deutschland genutzte Informationstechnik sicherer zu machen. Es gibt eine Sammlung von Informationen und Beiträgen im Internet, die sich ausschließlich diesen Schwerpunktthemen widmen. Soweit es möglich ist, werden bei JIKU auch Schulungen des BSI und anderer Vereine wie Deutschland sicher im Netz e.V. (DsiN) verwendet, um zu ergänzenden Recherchen anzuregen.

Wichtige Informationsquellen zur Informationssicherheit (Auswahl)	
Bundesamt für Sicherheit in der Informationstechnik (BSI)	Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft; weitere Informationen unter www.bsi.bund.de,www.bsi-fuer buerger.de,www.cert-bund.de
Deutschland sicher im Netz e.V. (DsiN)	DsiN ist ein gemeinnütziger Verein, unter der Führung des Bundesinnenministeriums, und bietet Verbrauchern und Unternehmen konkrete Hilfestellungen im sicheren Umgang mit dem Internet. Weitere Informationen unter www.sicher-im-netz.de,www.dsin-sicherheitscheck.de, www.sicher-im-netz.de/it-sicherheit-am-arbeitsplatz,www.dsin-blog.de, https://dsin-berufsschulen.de
Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI)	Der BfDI ist eine unabhängige Datenschutzbehörde gemäß Art. 51 Absatz 1 der Datenschutz-Grundverordnung (DSGVO). Er ist zuständig für die Informationsfreiheit und Überwachung des Datenschutzes bei öffentlichen Stellen des Bundes und bei Unternehmen, die Telekommunikations- und Postdienstleistungen erbringen. Weitere Informationen unter www.bfdi.bund.de
Bundesverband IT-Sicherheit e.V. (TeleTrusT)	Der Bundesverband TeleTrusT ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Weitere Informationen unter www.teletrust.de
Antispam e.V.	Gemeinnütziger deutscher Verbraucherschutzverein, der sich hauptsächlich mit dem Thema „Spam" und dessen Vermeidung beschäftigt. Weitere Informationen unter www.antispam-ev.de
AV-TEST GmbH	Unabhängiger Anbieter für Services im Bereich IT-Sicherheit und Anti-Viren- Forschung, mit Fokussierung auf die Ermittlung und Analyse der neuesten Schadsoftware und deren Einsatz in umfassenden Vergleichstests. Weitere Informationen unter www.av-test.org, portal.av-atlas.org

(3) Verantwortliche Stellen

In den Informationen des BSI (siehe Downloads in Abschnitt (2), S. 393) wird die Verantwortung der einzelnen Stellen für die Informationssicherheit herausgestellt. Das BSI erläutert in seinen Materialien und Schulungen den IT-Grundschutz mit Beispielen. Für die Darstellung der Verantwortlichen hat das BSI beispielhafte Rollen (siehe Infobox unten) vergeben. Das erleichtert den Unternehmen, in der Ausgestaltung ihres IT-Systems für sich ähnliche Stellen festzulegen, mit ähnlichen Zuständigkeiten. Wenn Mitarbeiter in Fremdfirmen beauftragt sind, können sie leichter nach zuständigen Stellen fragen und kennen auch die üblichen Zuständigkeiten dieser Rollen.

Hinsichtlich der Übernahme von Verantwortung zur Gewährleistung von IT-Sicherheit wird bei JIKU IT- Solutions nach den Vorgaben des BSI betont, dass alle im gleichen Boot sitzen. Das heißt, kein Mitarbeiter kann seine Verantwortung auf den anderen schieben, sondern jeder sollte sich grundsätzlich zuständig fühlen und der Verpflichtung nachkommen, etwaige Vorfälle mitzuteilen. Wird bei der Formulierung der Anforderungen das Wort „Muss" eingesetzt, ist dies nach Auffassung des BSI eine sehr dringliche Aufforderung und Verpflichtung, bei der Beschreibung mit „soll" eine Aufforderung, dass dies in der Regel so umzusetzen ist.

Verantwortliche Stellen der Informationssicherheit

Oberste Leitungsebene
Die oberste Leitungsebene des Unternehmens und jeder Organisation ist dafür verantwortlich, dass alle Geschäftsbereiche zielgerichtet und ordnungsgemäß funktionieren, Risiken frühzeitig erkannt und minimiert werden. Sie ist somit die Instanz, die die Entscheidung über den Umgang mit allen Risiken und damit auch den Sicherheitsrisiken trifft und entsprechende Ressourcen zur Verfügung stellt. Da sie für die strategische Ausrichtung zuständig ist, legt sie in der Leitlinie zur Unternehmenssicherheit ihre Position zur Erreichung der Informationssicherheitsziele auf allen Ebenen der Organisation fest. Sie initiiert den Informationssicherheitsprozess und behält auch die Gesamtverantwortung für die laufende Umsetzung. Hat sie Aufgaben delegiert, wird sie laufend von unterstellten Sicherheitsstellen über mögliche Risiken und Konsequenzen und den Status des Informationssicherheitsmanagementsystems (ISMS) informiert. Ein Informationssicherheitsmanagementsystem (ISMS) definiert Verfahren und Regeln, mit denen sich die Informationssicherheit steuern, kontrollieren und fortlaufend optimieren lässt.

IT-Sicherheitsbeauftragte, Informationssicherheitsbeauftragte, Datenschutzbeauftragte
Operative Aufgaben der Informationssicherheit werden i.d. R. an IT-Sicherheitsbeauftragte (ISB) und Datenschutzbeauftragte bzw. Informationssicherheitsbeauftragte sowie Stellvertreter delegiert. Die Benennung eines Datenschutzbeauftragten ist nach Art. 37 DSGVO und § 38 BDSG (neu) für Unternehmen Pflicht, soweit sie in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.
In Industrieunternehmen werden aufgrund der immer stärkeren Digitalisierung in der Produktionskette spezielle Sicherheitsbeauftragte ISB-ICS (ICS = Industrial Control System) berufen. Ist der Verantwortliche nicht erreichbar, hat der Stellvertreter die notwendigen Informationen und Kompetenzen, um Maßnahmen einzuleiten und erfolgreich abzuschließen.
Die Beauftragten sind für die Erstellung und Aktualität der Sicherheitsleitlinien und des Informationssicherheitssystems (ISMS, siehe S. 397) mit seinen Sicherheitsrichtlinien für die Mitarbeiter verantwortlich.

Rollen laut GSK, S. 29 ff.: „Grundsätzliche Zuständige“ und „Weitere Verantwortliche“
Das BSI gibt jährlich ein aktualisiertes IT-Grundschutz-Kompendium (GSK) mit Standard-Sicherheitsmaßnahmen heraus (siehe www.bsi.bund.de/gshb). Im GSK sind beispielhaft Zuständige für die Initiierung bzw. für die Erfüllung von Anforderungen genannt und näher beschrieben. In den Bausteinbeschreibungen werden die Zuständigkeiten in grundsätzlich zuständig und zusätzlich zuständig beschrieben. Im GSK werden auch beispielhaft Rollen benannt und beschrieben. Die Bezeichnungen der Rollen zu kennen ist beispielsweise auch von Bedeutung, wenn man in fremden Unternehmen (bei Kunden) tätig ist und sich nach zuständigen Personen (Rollen, Zuständigkeiten) erkundigen möchte. Als Auswahl werden folgende Rollen genannt und erläutert: Archivverwalter, Auditteam, Benutzer, Bereichssicherheitsbeauftragter, Beschaffer, Brandschutzbeauftragter, Datenschutzbeauftragter, Entwickler, Fachabteilung, Haustechnik, ICS-Administrator, Informationssicherheitsbeauftragter (ISB), IS-Revisionsteam, Leiter IT, Leiter Netze etc., Mitarbeiter, Notfallbeauftragter, Telearbeiter usw.

LE 2 - Gesetze und Standards zur Informationssicherheit unterscheiden

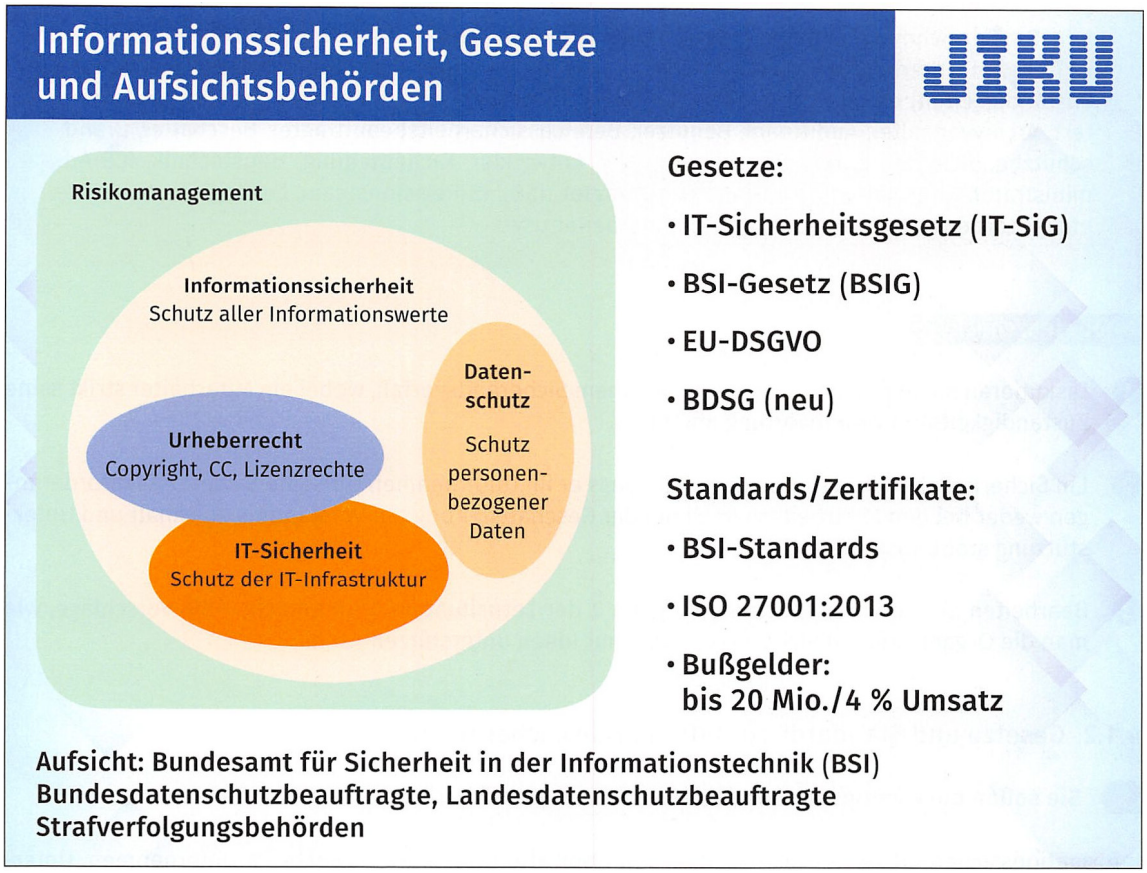
Sie sollen die wichtigsten Gesetze zur Informationssicherheit unterscheiden können.

Informationssicherheit ist der **Schutzanspruch über alle Informationswerte** im Unternehmen. Unternehmen müssen aus gesetzlichen Gründen insbesondere die personenbezogenen Daten schützen, die ihnen zur Verarbeitung anvertraut wurden. Daneben sind aber auch alle anderen Unternehmensdaten wichtig, um den Unternehmenszweck erfüllen und sich im Markt behaupten zu können. Ohne eine elektronische Datenverarbeitung sind Unternehmensprozesse heute kaum denkbar. In Schadensfällen können so hohe Schäden (Schadenersatz, Rechtskosten, Bearbeitungskosten, Umsatzeinbußen, Reputationsschäden etc.) entstehen, dass insbesondere größere Unternehmen ein differenziertes Risikomanagement einsetzen, um diese Vorfälle zu vermeiden.

Beim Datenschutz geht es um den Schutz **personenbezogener Daten**, die im Unternehmen auftragsbedingt oder zu Werbezwecken verwaltet werden. Dazu kommen personenbezogene Daten der Mitarbeiter und anderer Geschäftsbeteiligte. Aufgrund der Sensibilisierung auf die rechtssichere Speicherung und Verarbeitung sind im BDSG (Bundesdatenschutzgesetz) und in der DSGVO (Datenschutz-Grundverordnung) Rechte der Betroffenen und erhebliche Pflichten der Unternehmen festgelegt, die personenbezogene Daten verarbeiten.

Was die technische Sicherheit bzw. die IT-Sicherheit der IT-Infrastruktur anbelangt, sind das IT-Sicherheitsgesetz, die DSGVO und auch die **Standards des BSI** zu beachten.

Über das **Urheberrecht** entstehen Ansprüche insbesondere der Softwarehersteller, Lizenzeinnahmen für die Nutzung ihrer Betriebssysteme, Anwenderprogramme, Apps und Onlinedienste (SaaS = Software as a Service) zu erhalten. Aufbauend auf deutschem und internationalem Urheberrecht haben die Anbieter sehr unterschiedliche **EULA**- oder **Lizenzvertragsbedingungen** erstellt und passen sie nicht selten laufend an.



Bezogen auf die Sicherheit von Systemen und Software bieten Hersteller nicht nur laufend Softwareupdates an, um ihre Sicherheitslücken zu schließen, sondern häufig auch spezielle Tools und Dienste. Viele Unternehmen verbessern daher ihr Informationssicherheitssystem (ISMS) bis hin zu einem kompletten Risikomanagementsystem.

(1) IT-Sicherheit (IT-Security)

IT-Sicherheitsbeauftragte und Mitarbeiter, die sich mit Sicherheitstechnik, -Software und -Organisation beschäftigen, haben das IT-SiG, die DSGVO und das BSI-Gesetz zu beachten. Geht es um den Aufbau und die Zertifizierung eines Sicherheitssystems, so sind die ISO 27001 und die Standards des BSI wichtige Grundlagen.

IT-Sicherheitsgesetz, IT-Sicherheit in der DSGVO, BSI-Gesetz und ISO 27001

IT-Sicherheitsgesetz (IT-SiG)
Ziel des IT-Sicherheitsgesetzes ist es, die Informationssicherheit von Unternehmen, Verwaltungen und Institutionen sowie die digitalen Infrastrukturen besser zu sichern und zu schützen, ebenso die Bürgerinnen und Bürger im Internet. Das Gesetz stellt sich den Herausforderungen an Sicherheit aufgrund einer wachsenden Digitalisierung von Gesellschaft, Wirtschaft und Staat. Das IT-Sicherheitsgesetz richtet sich an Unternehmen mit kritischer IT-Infrastruktur und digitalen Diensten. Dazu gehören beispielsweise Unternehmen der Informationstechnik und der Telekommunikation. Das IT-Sicherheitsgesetz verpflichtet zudem Unternehmen mit kritischer Infrastruktur der Informationstechnik und Telekommunikation dazu, ihre Kunden zu warnen und Abhilfe zu leisten, sollten sie feststellen, dass deren persönliche Daten missbraucht wurden. Zu digitalen Diensten zählen beispielsweise Online-Marktplätze, Suchmaschinen und Anbieter von Cloud-Computing-Diensten. Die Betreiber haben nach dem IT-Sicherheitsgesetz geeignete Maßnahmen zu treffen, um die Daten und Systeme ihrer Kunden zu schützen. Auch wird hier das BSI in die Pflicht genommen.

EU-Datenschutz-Grundverordnung (EU-DSGVO)
Vorgaben der Datenschutz-Grundverordnung lassen sich nicht ohne eine gute IT-Sicherheit erfüllen. Zu beachten ist insbesondere Art. 24 der DSGVO, der alle Unternehmen verpflichtet, die personenbezogene Daten verarbeiten, technische und organisatorische Maßnahmen zum Datenschutz zu ergreifen. In Art. 32 der DSGVO wird die Pseudonymisierung und Verschlüsselung personenbezogener Daten gefordert. Es sind nach Art. 83 Bußgelder bis zu 20 Millionen Euro oder 4% des Jahresumsatzes möglich.

BSI-Gesetz (BSIG)
Das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) regelt die rechtliche Arbeitsgrundlage und Befugnisse des BSI als Aufsichtsbehörde. So wird dem BSI eingeräumt, IT-Produkte auf ihre Sicherheit hin zu untersuchen. Unternehmen, die als kritisch gelten, müssen ihre IT-Systeme nach dem aktuellen Stand der Technik absichern und ihre Informationssicherheit mindestens alle zwei Jahre überprüfen lassen (§ 8 a BSIG). In § 8 c BSIG sind besondere Anforderungen an Anbieter digitaler Dienste formuliert. Kleinstunternehmen und andere Unternehmen sind nach § 8 d BSIG davon befreit.
Das BSI ist nach § 8 b BSIG die zentrale Meldestelle für die IT-Sicherheit kritischer Infrastrukturen. Die Betreiber müssen dem BSI erhebliche Störungen ihrer IT melden, sofern sie Auswirkungen auf die Verfügbarkeit kritischer Dienstleistungen haben können.

IT-Grundschutz-Kompendium des BSI
Für den Aufbau eines Informationssicherheitssystems (ISMS) in Unternehmen, Organisationen und Behörden sind im IT-Grundschutz-Kompendium und anderen Quellen des BSI (Stichwort: ISMS) wichtige Umsetzungshinweise gegeben.

IS-Management nach ISO 27001
Für die Implementierung eines Informationssicherheitssystems (ISMS) und die Zertifizierung nach ISO/1EC 27001 werden in der ISO Bausteine zur Beachtung der drei Sichten definiert: Governance- Sicht (Beachtung der Unternehmensziele), Risikosicht (Beachtung der Risiken und Chancen) und Compliance-Sicht (Einhaltung der Vorgaben); dazu Vorgaben für Audits und Zertifizierungen.

(2) Datenschutz - Schutz personenbezogener Daten

Das BDSG (deutsche Bundesdatenschutzgesetz) regelt zusammen mit den Datenschutzgesetzen der Länder, der DSGVO und anderen bereichsspezifischen Regelungen den Umgang mit personenbezogenen Daten in Unternehmen.

Datenschutz personenbezogener Daten

EU-DSGVO, BDSG und Landesdatenschutzgesetze
EU-DSGVO, das BDSG und die Landesdatenschutzgesetze sind Gesetze zum Schutz von Personen, deren personenbezogene Daten verwendet werden:

- Die **EU-Datenschutz-Grundverordnung (EU-DSGVO**) gilt seit 2018 für alle EU-Länder verbindlich.
- Das **Bundesdatenschutzgesetz (BDSG**) ist seit 2018 mit der Datenschutz-Grundverordnung (DSGVO) anwendbar, das BDSG konkretisiert und spezifiziert Vorgaben der DSGVO, die DSGVO ist im Zweifel vorrangig anzuwenden. Die Länder haben zusätzlich eigene Datenschutzgesetze beschlossen.
- Eine zukünftige ePrivacy-Verordnung (ePVO) soll die E-Privacy-Richtlinie (etwa ab 2023) ablösen, die der deutsche Gesetzgeber größtenteils im Telemediengesetz (TMG) und Telekommunikationsgesetz (TKG) umsetzte. Sie soll personenbezogene Daten in der öffentlichen elektronischen Kommunikation und Werbung noch besser schützen.
- Gesetze zur Informationsfreiheit, siehe www.bfdi.bund.de

Die Aufsicht haben der Bundesdatenschutzbeauftragte und Landesdatenschutzbeauftragte, BSI.

Telekommunikationsgesetz
Um einen besseren Schutz der Bürgerinnen und Bürger zu erreichen, sind Telekommunikationsanbieter dazu verpflichtet,

- IT-Sicherheitsmaßnahmen nach dem „Stand der Technik" nicht nur zum Schutz personenbezogener Daten, sondern auch zum Schutz vor unerlaubten Eingriffen in die Infrastruktur einzusetzen und zu erhalten (§ 109 Abs. 1 und 2 TKG),
- ihre Nutzer über Schadprogramme und ihre Erkennung und Beseitigung zu informieren (§ 109a Abs. 4 TKG) und
- erhebliche IT-Störungen sowohl an das BSI als auch an die Bundesnetzagentur zu melden (§ 109 Abs. 5 TKG).

Telemediengesetz (TMG)
Telemedien-Diensteanbieter sind verpflichtet, IT-Sicherheitsmaßnahmen nach dem „Stand der Technik" nicht nur zum Schutz personenbezogener Daten, sondern auch zum Schutz vor unerlaubten Eingriffen in die Infrastruktur einzusetzen und zu erhalten (§ 13 Absatz 7 TMG).

Datenschutz-Grundverordnung (EU-DSGVO)
Sie regelt den Schutz und Grundrechte natürlicher Personen bei der Verarbeitung personenbezogener Daten in Unternehmen aller EU-Länder. Formuliert ist neben Rechten und Pflichten beispielsweise die Rechenschaftspflicht von Unternehmen, die personenbezogene Daten verarbeiten: Sie müssen nachweisen (können), dass sie als Verantwortliche angemessene und wirksame Maßnahmen ergreifen, um die datenschutzrechtlichen Grundsätze und Verpflichtungen der DSGVO umzusetzen (§ 5 a DSGVO).

Allgemeinen Prinzipien der Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 DSGVO)

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung: Erhebung für festgelegte, eindeutige und rechtmäßige Zwecke
- Datenminimierung: Beschränkung auf den Zweck der Verarbeitung
- Richtigkeit: sachlich richtig und auf dem neuesten Stand
- Speicherbegrenzung: Speicherung nur so lange wie erforderlich
- Integrität, Vertraulichkeit: geeignete technisch-organisatorische Maßnahmen

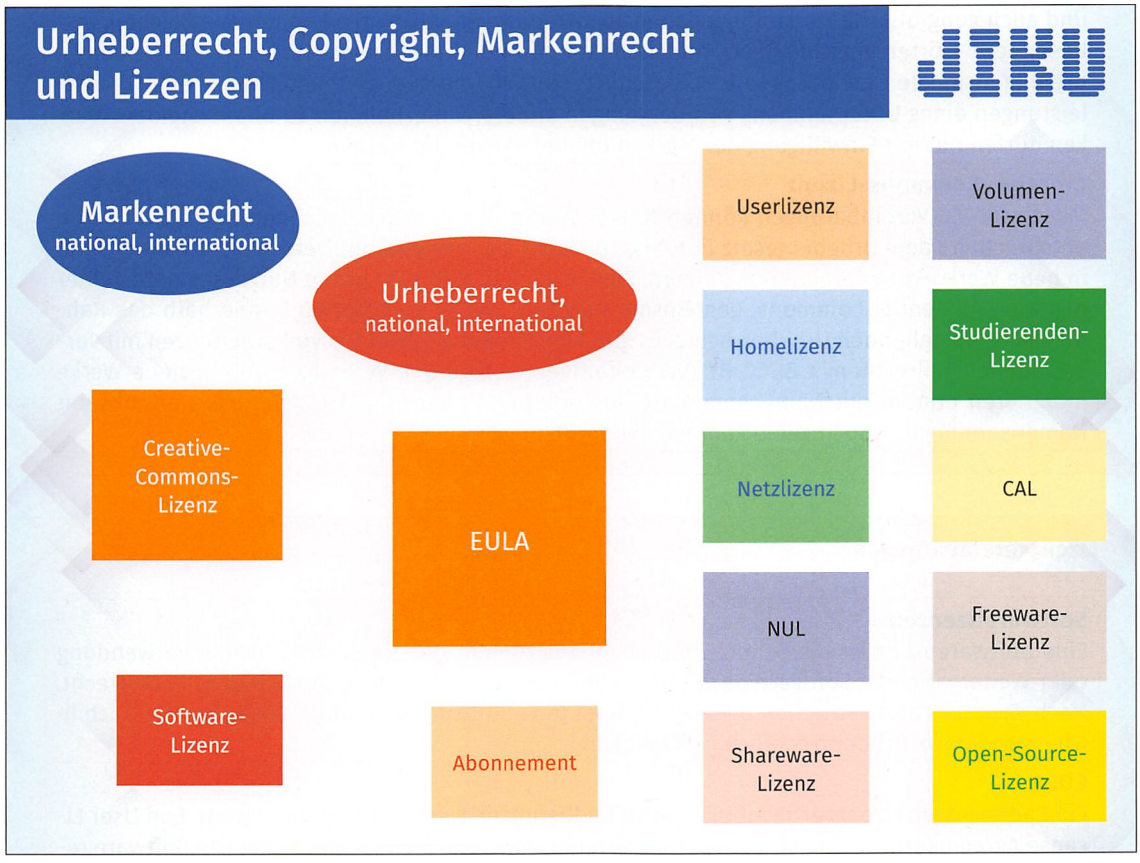
Datenschutz personenbezogener Daten

Beispiele für erforderliche interne Maßnahmen (Art. 26 ff. DSGVO)
- Verzeichnis aller Verarbeitungstätigkeiten, ähnlich dem Verfahrensverzeichnis des BDSG
- Dokumentationspflicht der Vorgänge
- Bestellung eines Datenschutzbeauftragten nach Art. 37 DSGVO und § 38 BDSG

Rechte der betroffenen Personen: DSGVO Art. 1-23 (§§ 32-37 BDSG)
- Art. 12: Transparente Information, Kommunikation und Modalitäten zur Ausübung der Rechte
- Art. 13: Informationspflicht bei Erhebung von personenbezogenen Daten
- Art. 14: Informationspflicht, wenn die Daten nicht bei der betroffenen Person erhoben wurden
- Art. 15: Auskunftsrecht der betroffenen Person
- Art. 16: Recht auf Berichtigung
- Art. 17: Recht auf Löschung, „Recht auf Vergessenwerden“
- Art. 18: Recht auf Einschränkung der Verarbeitung
- Art. 19: Mitteilungspflicht im Zusammenhang mit Berichtigung, Löschung, Einschränkung
- Art. 20: Recht auf Datenübertragbarkeit
- Art. 21: Widerspruchsrecht
- Art. 22: Automatisierte Entscheidungen im Einzelfall einschließlich Profiling
- Art. 23: Beschränkungen der Rechte verhältnismäßig in besonderen Fällen

(3) Urheberrecht, Copyright, Markenrecht und Lizenzrecht

Urheberrechte und Marken sind ein wesentliches Wirtschaftsgut erfolgreicher Unternehmen. Verstöße gegen Urheberrechte können Unternehmen erhebliche Schäden verursachen.



So verwenden Mitarbeiter arglos in ihren Geschäftsunterlagen oder Websites Markenbezeichnungen von Herstellern und erhalten Abmahnungen. Auch passiert es, dass Verwender von Google Ads (früher AdWords) abgemahnt werden, wenn sie fremde Marken sowie Produkt- oder Geschäftsbezeichnungen der Konkurrenz als Keywords verwendet haben.

Softwarehersteller bieten ihre Produkte über Nutzungslizenzen an. Diese basieren rechtlich auf Urheber- und Markenrechten. Aufbauend darauf haben sie sehr unterschiedliche Lizenzverträge gestaltet und bieten je nach Marktlage veränderte Versionen an. Daher wird es auch erschwert, Vergleiche der Anbieter durchzuführen. Vor der Installation von Programmen muss geprüft werden, welche Lizenzen vorhanden sind und welche zusätzlich beschafft werden müssen. Bei zusätzlichen Lizenzen kann es sinnvoll sein, insgesamt auf ein ganz anderes Lizenzmodell zu wechseln. Die folgenden Übersichten zeigen, wie vielfältig die Anwendungen des Urheberrechts sind.

Urheberrecht, Markenrecht, Creative-Commons-Lizenz

Urheberrecht/Copyright
Im Urheberrechtsgesetz (UrhG) als zentrales Gesetz sind die Rechte der geistigen Schöpfer (schutzwürdiges Werk) und mögliche Maßnahmen bei Urheberrechtsverletzungen festgelegt. Es gilt für Lichtbildwerke, Darstellungen, Sprach- und Schriftwerke und auch Computerprogramme. Der Urheber hat Persönlichkeitsrechte sowie die Nutzungs- und Verwertungsrechte. Werke können unter bestimmten Voraussetzungen auch ohne eine Zustimmung genutzt werden, z. B. für Unterricht und Forschung. Urheberrechtsverletzungen werden nach dem Strafrecht geahndet.

Markenrecht
Nach dem Markengesetz (MarkenG) können Unternehmen Marken, geschäftliche Bezeichnungen und auch geografische Herkunftsangaben schützen lassen. Als Marke können alle Zeichen, insbesondere Wörter einschließlich Personennamen, Abbildungen, Buchstaben, Zahlen, Klänge, dreidimensionale Gestaltungen u.a., geschützt werden, die geeignet sind, Waren oder Dienstleistungen eines Unternehmens von denjenigen anderer Unternehmen zu unterscheiden. Marken dürfen nur mit Einwilligung der Markeninhaber verwendet werden.

Creative-Commons-Lizenz
Mit diesen CC-Vereinbarungen können Nutzer Werke (Texte, Musik, Zeichnungen etc.) anderen entsprechend dem Urhebergesetz überlassen, damit sie vervielfältigt, verbreitet, verändert und in neue Werke integriert werden können. Ziel ist es, dadurch eine große Nutzergemeinde einer digitalen Allmende (Commons, gemeinsam nutzbare Werte) zu schaffen - innerhalb des Rahmens des bestehenden Urheberrechts. Es gibt verschiedene Schichten von CC-Lizenzen mit verschiedenen Teilrechten, z.B. CC BY (Vervielfältigen, Verbreiten, Verändern und in neue Werke integrieren erlaubt mit Namensnennung des Urhebers) oder CC BY-NC (wie oben erlaubt mit Namensnennung, jedoch keine kommerzielle Nutzung).

Lizenzvereinbarungen

Softwarelizenzen
Eine Softwarelizenz ist ein Schutz- und Rechtsinstrument des Herstellers für die Verwendung oder Weitergabe von Software nach dem Urheberrecht, eventuell auch nach dem Patentrecht. Nach dem US-amerikanischen Urheberrecht ist jede Software sowohl im Quellcode als auch in Objektcodeform urheberrechtlich geschützt.

EULA
Ein Endbenutzer-Lizenzvertrag (EULA), auch Endbenutzer-Lizenzvereinbarung (engl. End User Li- cense Agreement), ist eine spezielle Lizenzvereinbarung, welche die Benutzung von Software regeln soll. Texte mit einer EULA werden oftmals zu Beginn der Installation der Software angezeigt.

Sonstige Lizenzen
Allgemein unterschieden werden beispielsweise rechnergebundene Lizenzen (Nodelocked License), benutzergebundene Lizenzen (Named User License) oder Netzwerklizenzen (Floating License, Concurrent Use License). Es wird unterschieden in proprietäre Software, Freeware, Shareware, Open Source Software, Public Domain Software.

Fachbegriffe aus dem Lizenzrecht	
Nutzer-/User-Lizenz	Bei einer User-Lizenz muss jeder Softwarebenutzer lizensiert werden. Wie ein Benutzer definiert wird, kann unterschiedlich sein.
Client Access License (CAL)	Client-Access-Lizenzen sind Zugriffslizenzen und werden in Client/Server- Umgebungen benötigt (siehe auch Concurrent Access License).
Named User Licence (NUL)	Eine Named User Licence ist auf einen benannten Benutzer im Unternehmen lizensiert, der die Software ausschließlich nutzen darf.
Concurrent Access Licence	Das Gegenstück zu NUL ist die Concurrent Access Licence, bei der die maximal gleichzeitige Anzahl an Zugriffen auf beliebig vielen Rechnern lizensiert wird, auch Floating- oder Netzwerklizenzen genannt.
Key Management Service (KMS)	Optionen der Aktivierung von Volumenlizenzen (z. B. Windows Desktop- Betriebssystem und Windows Server, Office 20xx). KMS erlaubt es Organisationen, Betriebssysteme innerhalb des eigenen Netzwerks zu aktivieren.
CPU-Klauseln	CPU-Klauseln werden oft in Lizenzbestimmungen führender Softwarehersteller wie Oracle, Microsoft, VMware oder IBM verwendet. Microsoft lizensiert beispielsweise auch nach Prozessorkernen.
OEM	OEM-Lizenzen, vorinstalliert, häufig eingeschränkte Rechte, in Deutschland auch ohne Systembindung erhältlich
Maintenance	So werden i.d. R. Wartungs- und Support-Verträge bezeichnet, die von verschiedenen Herstellern zu ihren Produkten angeboten werden.
SPLA von CSP	Service-Provider-Lizenzen (SPLA) über Cloud-Solution Provider
Zweitkopierecht	Es bezeichnet die Möglichkeit, Lizenzen oder Boxen jeweils auf einem Rechner und einem Notebook zu installieren.

Software-Lizenzportale

Lizenzunterschiede
Software, Abonnement, Versionen: 32 Bit oder 64 Bit, dauerhafte oder befristete Nutzung, Produktschlüsselvergabe, Lieferung auf USB-Stick oder Download, Security-Tools, Zusatzservices, z. B. Verbesserung der Sicherheit durch Enterprise Data Protection

Microsoft-Lizenzen (z.B. für Office)
Flome & Business, Professional, Standard, Professional Plus, z.B. mit Service Data Löss Prevention (DLP), Spreadsheet-Werkzeuge, Enterprise Voice, Archivierung

Gebrauchtlizenzen
Nach einem EuGH-Urteil kann sich ein Softwarehersteller dem Weiterverkauf von Lizenzen nicht widersetzen.

Portale
Gebrauchte Lizenzen lassen sich Weiterverkäufen. So gibt es seit einigen Jahren Internetportale, die mit Lizenzen zur Zweit- und Mehrfachverwendung handeln.

Lernzielkontrolle TAG 1

1. Ordnen Sie folgende Vorfälle mindestens einem Gesetz/einer Verordnung richtig zu:

a) Ein Virus legt einen Server lahm.

b) Der Informationssicherheitsbeauftragte (ISB) erhält die Anfrage, ob Kundendaten, die seit fünf Jahren nicht mehr gekauft haben, gelöscht werden müssen.

c) Ein Mitarbeiter möchte ein Programm nutzen, dass er bei einem Mitarbeiter gesehen hat.

2. Was ist richtig?

a) Die Informationssicherheit ist der IT-Sicherheit untergeordnet.

b) Das IT-SiG regelt insbesondere, wie Unternehmen mit kritischer IT-Infrastruktur sicherer sind.

c) Das IT-SiG muss ein Betreiber eines kleinen Onlineshops beachten.

d) Das BSIG ist nur für Mitarbeiter des BSI von Bedeutung.

e) Die DSGVO gilt nur für Deutschland und gilt nachrangig zum BDSG.

f) Prinzipien der DSGVO sind Speicherbegrenzung und Datenminimierung.

g) Menschen haben das Recht, dass veraltete persönliche Daten berichtigt werden.

3. Prüfen Sie Rechte Betroffener in Datenschutzfällen.

a) Überprüfen Sie, gegen welche Artikel (12 bis 23) der DSGVO hier verstoßen wurde.

Kundenbeschwerden	
1. Der Kunde erfährt nicht, bei welcher Behörde er sich beschweren kann.	
2. Das Unternehmen ist nicht bereit, Kundendaten auf Verlangen zu löschen.	
3. Das Unternehmen löscht Kundendaten nicht, die es zum Zweck nicht benötigt.	
4. Da Löschung nicht möglich ist, verlangt der Kunde eingeschränkte Datennutzung.	
5. Der Kunde erfährt nicht, welche Daten an Dritte weitergegeben wurden.	
6. Das Unternehmen lehnt die Mitteilung anderer über die Löschung ab.	
7. Das Unternehmen ist nicht bereit, auf Wunsch zusätzliche Daten zu erfassen.	
8. Das Unternehmen sendet Daten auf Kundenwunsch nicht anderen Unternehmen.	
9. Das Unternehmen verweigert dem Kunden, unrichtige Daten zu berichtigen.	
10. Dem Kunden wird die Auskunft verweigert, an wen die Daten gegeben wurden.	
11. Der Kunde habe nicht das Recht zur Auskunft über die Dauer der Speicherung.	
12. Der Kunde erhält keine Information, dass andere seine Daten verwenden.	
13. Der Kunde erhält nur die Information, dass die Daten elektronisch gespeichert wurden.	
14. Ein Kunde erhält auf elektronisches Verlangen keine Information.	
15. Der Kunde wird nicht über die werbliche Nutzung seiner Daten informiert.	
16. Die Kundendaten werden ohne Information über die Speicherung erfasst.	
17. Trotz Löschung senden anhängige Datenverarbeiter weiterhin Werbung.	
18. Ein älterer Kunde erhält eine englische Datenschutzvereinbarung ausgehändigt.	

b) Geben Sie an, welche Stellung das BDSG zur DSGVO hat

4. Geben Sie jeweils ein Beispiel an, wann gegen das folgende Prinzip der Verarbeitung personenbezogener Daten gemäß Art. 5 Abs. 1 DSGVO verstoßen wurde.

Prinzip	**Beispiel, bei dem gegen das Prinzip verstoßen wurde**
Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	
Zweckbindung	
Datenminimierung	
Richtigkeit	
Speicherbegrenzung	
Integrität, Vertraulichkeit	

5. Erläutern Sie Urheber-, Marken- und Lizenzbestimmungen auf Nachfragen.

   Finden Sie zum Urheber- und Markenrecht die richtigen Antworten unter Verwendung des UrhG und des MarkenG. Verwenden Sie dazu die Gesetzesauszüge im Anhang. Kreuzen Sie an, was zutrifft.

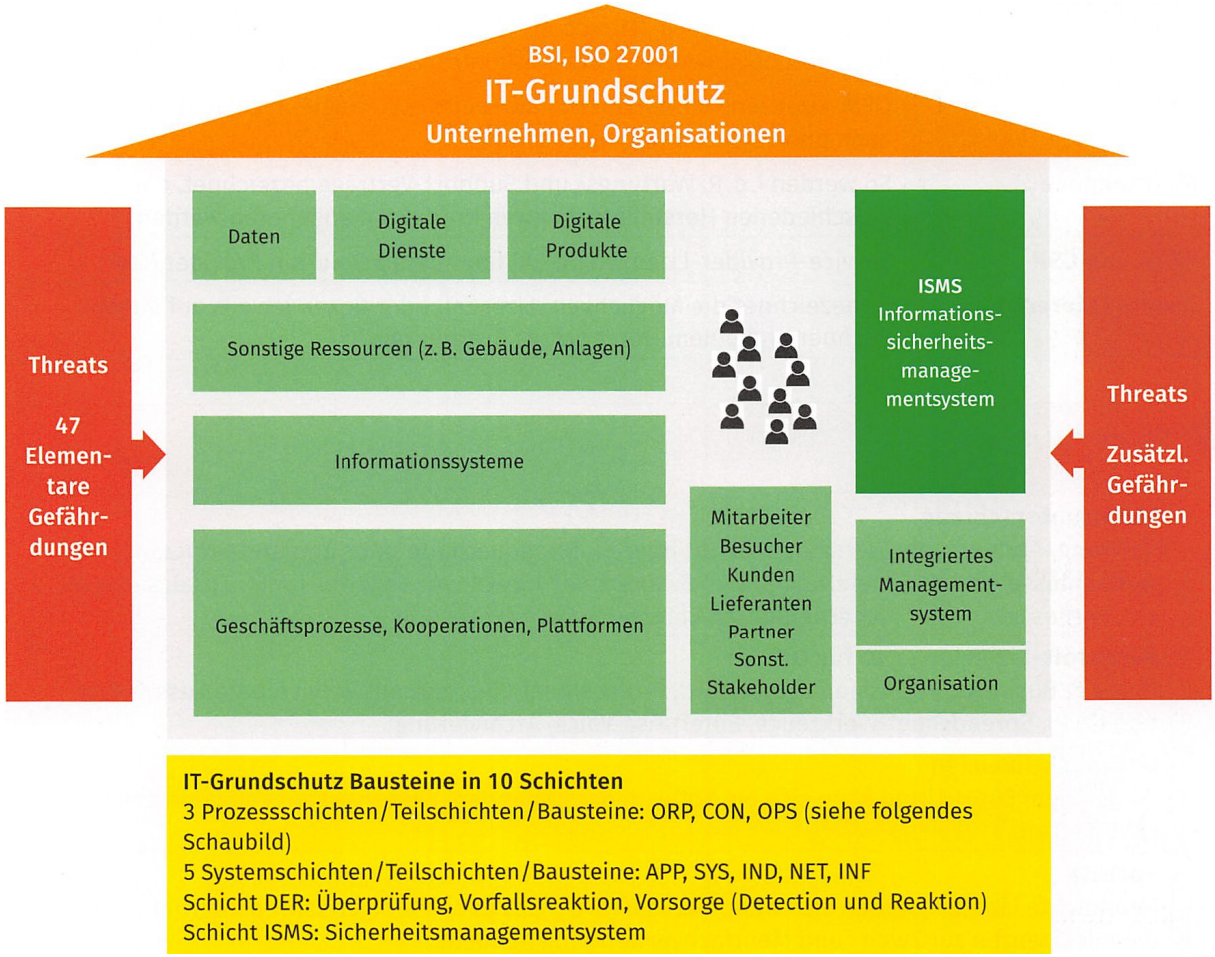
Urheber-, Marken- und Lizenzbestimmungen	
1. Für den Schutz selbst erstellter Computerprogramme, Bilder oder Darstellungen gilt:	
a) Sie sind nur dann nach UrhG geschützt, wenn sie persönliche geistige Schöpfungen sind.	
b) Computerprogramme sind im Vergleich zu Bildern nicht nach UrhG geschützt.	
c) Alle Bilder sind nur nach KunstUrhG geschützt.	
d) Webcasts sind nach UrhG nicht geschützt.	
e) Selbst erstellte Computerprogramme und Datenbanken mit geistiger Schöpfung sind nach UrhG geschützt.	
f) Wenn das Computerprogramm im Betrieb erstellt wurde, ist der Betrieb Urheber.	
g) Wenn ein Bild selbst erstellt wurde und keine anderen Rechte verletzt wurden, kann man es gegen Entgelt anderen anbieten.	
h) Man darf ein Bild mit einem Prominenten im beruflichen Wirkungskreis veröffentlichen.	
i) Ein Bild darf, auch wenn Menschen nur unwesentliches Beiwerk sind, nicht veröffentlicht werden.	
j) Bei Computerprogrammen unterliegen die Entwürfe nicht dem Urheberrecht.	
k) Bei einem Computerprogramm hat der Urheber gesetzlich für die Ideen und Grundsätze, die einem Element eines Computerprogramms zugrunde liegen, einschließlich der den Schnittstellen zugrunde liegenden Ideen und Grundsätze, Verwertungsrechte.	
l) Die Schutzfähigkeit von Computerprogrammen ist von qualitativen oder ästhetischen Bewertungen abhängig.	
2. Wer Urheber eines Bildes, einer Software oder einer Datenbank ist, für den gilt:	
a) Als Urheber darf man die Urheberbezeichnung bestimmen.	
b) Als Urheber kann man die Verbreitung nicht exklusiv einem Nutzer geben.	
c) Der Betrieb kann vertraglich verlangen, dass er die exklusiven Rechte an einer im dienstlichen Auftrag erstellten Software hat.	
d) Als Urheber kann man nicht einzelne, sondern nur alle Nutzungsarten anderen einräumen.	

3. Zur Prüfung der Verstöße gegen das UrhG gilt:	
a) Es ist nur mit Abmahnungen zu rechnen, die aber insgesamt beschränkt sind.	
b) Es ist auch mit Freiheitsstrafen, für Privatleute bis drei Jahre, gewerblich bis fünf Jahre, zu rechnen.	
c) Abmahnkosten sind gesetzlich nur gegenüber Privatleuten gedeckelt.	
d) Neben Abmahn-, Gerichts- und Anwaltskosten ist mit Schadensersatz zu rechnen.	
e) Unternehmen haften nicht für die Mitarbeiter, Mitarbeiter haften bei grober Fahrlässigkeit.	
f) Mitarbeiter dürfen fremde Programme öffentlich, z. B. auf Messen, vorführen.	
g) Bücher, die für Unterrichtszwecke erstellt wurden, dürfen nicht kopiert werden; zu nicht kommerziellen Zwecken aber bis zu 15 %.	
h) Solange man für fremde Bilder, die man ins Internet eingestellt hat, noch kein Geld erhalten hat, ist auch nicht mit einer Verurteilung zu rechnen.	
i) Bei fremden Bildern muss genau geprüft werden, ob und wie die Quellenangabe zu erfolgen hat.	
4. Zur Prüfung von Vorfällen im Markenrecht gilt:	
a) Ein einzigartiges Geschäftszeichen ist nur dann eine Marke, wenn es im Markenregister eingetragen ist.	
b) Eine Geschäftsmarke ist nur ein Logo, nicht eine Tonfolge oder ein Personenname.	
c) Der Markeninhaber hat weitgehende Rechte, sodass geschäftsübliches und nicht geschäftsschädigendes Handeln besonders zu beachten ist.	
d) Fremde Marken können im Geschäftsverkehr in engen Grenzen verwendet werden, wenn es um die Bezeichnung der Waren und insbesondere eines passenden	
e) Wenn fremde Marken für eigenes werbliches Handeln ohne Zustimmung des Rechteinhabers genutzt werden, kann es zu Markenrechtverletzungen kommen.	

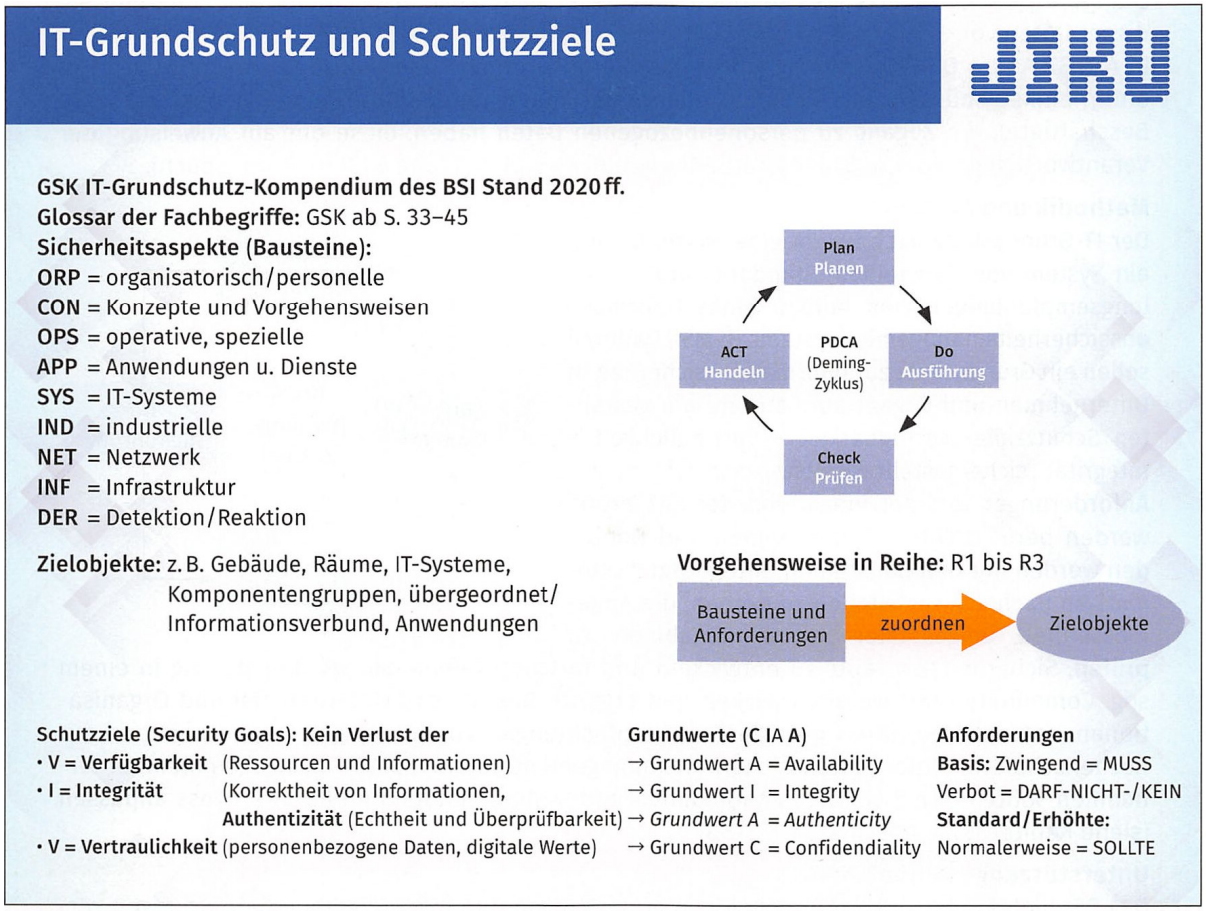
TAG 2 - IT-Grundschutz, Schutzziele, Gefährdungen, Schadensszenarien unterscheiden

Sie sollen Anforderungen zum IT-Grundschutz präsentieren.

Die folgenden beiden Schaubilder zeigen wichtige Grundzüge des IT-Grundschutzes des BSI im Zusammenhang auf. Mitarbeiter, die sich mit Informationssicherheit und IT-Grundschutz beschäftigen, und Mitarbeiter der IT-Berufe sollten in der Lage sein, diese Schaubilder zu erläutern. Das folgende Schaubild zeigt ein Strukturbild von Unternehmen oder Organisationen, die digitale Dienste oder Produkte anbieten und personenbezogenen Daten verarbeiten. Ihre Infrastruktur und der Betrieb eines sicheren Verarbeitungsbetriebs sind durch eine Vielfalt von Bedrohungen und laufend neue betriebliche Schwachstellen ständig gefährdet. Schutzziele bzw. Sicherheitsgrundwerte werden im Schadensfall nicht eingehalten. Hohe Strafen, Bußgelder und große wirtschaftliche Schäden aufseiten der Unternehmen und Organisationen sowie der Verlust von Persönlichkeits- und Freiheitsrechten der Betroffenen sind die Folge.



Das BSI hat Sicherheitsaspekte in Bausteinen zusammengefasst und 10 Sicherheitsbausteine im IT- Grundschutz festgelegt. Diese sind systematisch in Zielobjekten zu untersuchen. Dazu müssen Gefährdungen den Bausteinen zugeordnet und bewertet werden, welche Anforderungen zur Sicherstellung eines Basisschutzes, eines Standardschutzes und eines Schutzes bei erhöhten Anforderungen notwendig sind. Der Prozess der Überprüfung und Entwicklung des Sicherheitssystems ist ein laufender Prozess und unterliegt dem PDCA-Zyklus.

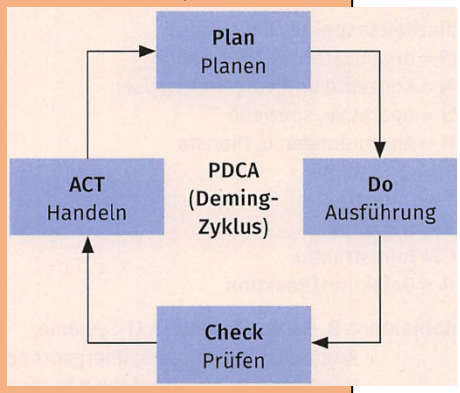


LE 1 - IT-Grundschutz nach dem BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist gesetzlich als Bundesbehörde für die Informationssicherheit auf nationaler Ebene zuständig (vgl. BSIG). Es hat daher auf der Basis der ISO 27001, weiterer Normen, Praxiserfahrungen und eines systematischen Entwurfsprozesses ein Konzept zur Sicherstellung des IT-Grundschutzes entworfen. Dieses Konzept sieht Schutzziele bzw. Grundwerte der IT-Sicherheit vor, deren Einhaltung auch in Informationssicherheitsgesetzen (IT-SiG, BDSG, LDSG, EU- DSGVO) gefordert wird. Ziele sind, die Betroffenen mit ihren personenbezogenen Daten zu schützen, die Aufsicht der solche Daten verarbeitenden Unternehmen sicherzustellen. Unternehmen und Organisationen wird vielfältige Unterstützung zum Aufbau und laufenden Fortschreibung eines Informationssicherheitssystem angeboten. Unternehmen sind verpflichtet, angemessene Informationssicherheitssysteme zu installieren, wenn sie personenbezogenen Daten verarbeiten. Die Informationssicherheitssysteme sind individuell den Anforderungen der Unternehmen entsprechend zu entwickeln. Sie sind daher sehr unterschiedlich, können manuell oder elektronisch über spezielle Content-Management-Systeme bzw. ISMS-Systeme eingerichtet werden.

IT-Grundschutz nach dem BSI
Gesetzliche Grundlage
Nach Art. 29 DSGVO dürfen Beschäftigte eines Verantwortlichen (eines Unternehmens, eines Vereins, eines Verbands, eines Selbstständigen, einer Behörde usw.) oder eines Auftragsverarbeiters personenbezogene Daten ausschließlich auf Weisung des Verantwortlichen oder Auftragsverarbeiters benutzen, es sei denn, eine gesetzliche Regelung schreibt eine Verarbeitung dieser Daten vor.
In Art. 32 Abs. 4 DSGVO ist vorgegeben, dass Verantwortliche oder Auftragsverarbeiter Schritte unternehmen müssen, um sicherzustellen, dass ihnen unterstellte Personen (insbesondere Beschäftigte), die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung der Verantwortlichen oder Auftragsverarbeiter benutzen.

Methodik und System
Der IT-Grundschutz nach BSI ist eine Methodik und ein System von Bausteinen, Standards und Handlungsempfehlungen zum Aufbau eines Informationssicherheitsmanagementsystems (ISMS). Dadurch sollen ein Grundschutz zur Informationssicherheit in Unternehmen und Organisationen und die gestellten Schutzziele „Verfügbarkeit - Vertraulichkeit -Integrität" sichergestellt werden.



Anforderungen aus der Praxis und der ISO 27001 werden berücksichtigt. Unternehmen und Behörden werden mit den Bausteinen unterstützt, systematisch nach Schwachstellen zu suchen, die Angemessenheit umgesetzter Schutzmaßnahmen zu prüfen, Sicherheitskonzepte zu entwickeln und fortzuschreiben. Sie werden ständig in einem sog. Community Draft weiterentwickelt und ergänzt. Das BSI soll Unternehmen und Organisationen unterstützen, ihren gesetzlichen Verpflichtungen zur Informationssicherheit und zur Rechenschaft im Informationssicherheitsmanagementsystem (ISMS) nachzukommen. Unternehmen sollten ihre Sicherheitsmaßnahmen und Systeme laufend im PDCA-Prozess anpassen.

Unterstützungsmaßnahmen
Das BSI bietet aufgrund der notwendigen Anpassungen durch ständig neue Gefährdungen verschiedene Unterstützungsmaßnahmen an, z. B.:

1. **IT-Grundschutz-Kompendium** (GSK, jährlich aktualisiert, Entwürfe als Drafts): Beschreibung von Elementaren Gefährdungen und Bausteinen zur Erstellung von Informationssicherheitssystemen (ISMS) in Unternehmen und Organisationen.
2. **Standards**:
   BSI-Standard 200-1 (alt 100-1): Managementsysteme für Informationssicherheit
   BSI-Standard 200-2 (alt 100-2): IT-Grundschutz-Vorgehensweise
   BSI-Standard 200-3 (alt 100-3): Risikoanalyse auf der Basis von IT-Grundschutz, Rahmenbedingungen, Zielobjekte, Gefährdungsübersicht, Risiken behandeln BSI-Standards 200-4 (alt 100-4): Notfallvorsorge, Business Continuity Management
3. **Weitere Unterstützungen**: Leitfaden Basisabsicherung für kleinere Unternehmen und Organisationen, Grundschutzprofile (Schablonen) für verschiedene Anwendungsgruppen (z. B. Handwerksbetriebe), Grundschutztools und Toolliste

IT-Grundschutz-Drafts, d. h. Veröffentlichung und Community von Entwürfen

Meldungen und Mitteilungen über aktuelle Gefährdungen u.v. m., siehewww.bsi.bund.de.

Inhalte des IT-Grundschutz-Kompendiums
Aufbau in zehn Schichten: Prozessbausteinschichten, System-Bausteinschichten, ISM, DER, z.B.

- Die **Schicht INF (**Infrastruktur) enthält Bausteine zum Gebäude, zu Räumen und weiterer Infrastruktur (für Lernfeld 4 INF.7 bis 10 - Büroarbeitsplatz, häuslicher Arbeitsplatz, mobiler Arbeitsplatz, Besprechungs-, Veranstaltungs- und Schulungsräume einzubeziehen).
- Die **Schicht NET** (Netze und Kommunikation) wird in Lernfeld 3 und in weiterführenden Jahrgängen behandelt.
- **SYS-Schicht (IT-Systeme**): Bezogen auf Arbeitsplätze sind hier insbesondere die Desktop- Systeme und mobilen Devices von Bedeutung. Die Schicht ORP befasst sich mit organisatorischen und personellen Sicherheitsaspekten, z. B. die Bausteine „Organisation" und „Personal" oder das Berechtigungsmanagement.
- Die **Schicht CON** enthält Bausteine, die sich mit Konzepten und Vorgehensweisen befassen. Typische Bausteine der Schicht CON sind u.a. Auswahl und Einsatz von Standardsoftware, Datenschutz und Datensicherungskonzept, Softwareentwicklung, Kryptokonzept.

Inhalte des IT-Grundschutz-Kompendiums

- **Anwendungsschicht (APP):** Hier sind für das Lernfeld 4 insbesondere die Bausteine „Client- Anwendungen" oder „Business-Anwendungen" von Bedeutung.
- Die **Schicht OPS** umfasst alle Sicherheitsaspekte des operativen IT-Betriebs, z.B. Bausteine zum Schutz vor Schadprogrammen, Cloud-Nutzung oder Telearbeit.
- In der **Schicht DER** finden sich alle Bausteine, die für die Überprüfung der umgesetzten Sicherheitsmaßnahmen, die Detektion von Sicherheitsvorfällen sowie die geeigneten Reaktionen darauf relevant sind, z. B. Bausteine zur Behandlung von Sicherheitsvorfällen (Security Incident Management) oder die Vorsorge für IT-Forensik (systematische Untersuchung krimineller Handlungen).
- **Schicht ISMS**: Hier sind Bausteine zum Aufbau und Betrieb eines Informationssicherheitsmanagementsystems aufgeführt. Diese werden in den Fachmodulen behandelt, im Modul D werden ausgewählte Systembestandteile (z. B. Sicherheitsleitlinie, Risikoanalyse) auf die Arbeitsplatzanalyse eingegrenzt einbezogen.

LE 2 - Schutzziele nach IT-Grundschutz

Im Modul A wurden das Unternehmensleitbild und allgemeine Ziele von Unternehmen behandelt. Ein Schaubild unterschiedlicher Unternehmensziele stellt neben wirtschaftlichen Zielen auch Qualitätsziele sowie Ziele zur IT-Sicherheit und zum Datenschutz vor. Auch in Modul B werden Ziele zur IT-Sicherheit und zum Datenschutz angesprochen sowie die Risikoanalyse bezogen auf Arbeitsplätze durchgeführt.

In der DSGVO werden aus der Sicht der Betroffenen insbesondere die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit ihrer personenbezogenen Daten gefordert.

Art. 32 Abs. 1 DSGVO - Sicherheit der Verarbeitung personenbezogener Daten

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Das BSI hat diese Schutzziele als Grundwerte der Informationssicherheit festgelegt.

Schutzziele und Grundwerte der Informationssicherheit nach BSI
Der IT-Grundschutz betrachtet die drei Schutzziele bzw. Grundwerte der Informationssicherheit: Verfügbarkeit (Availability) - Integrität (Integrity) - Vertraulichkeit (Confidendiality).
Jedem Anwender des IT-Grundschutzes steht es frei, bei der Schutzbedarfsfeststellung weitere Grundwerte zu betrachten, wenn dies im individuellen Anwendungsfall hilfreich ist. Weitere generische Oberbegriffe der Informationssicherheit sind beispielsweise Authentizität, Verbindlichkeit, Zuverlässigkeit und Nichtabstreitbarkeit.
Mit dem Begriff „Authentizität" wird eine Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartnertatsächlich derjenige ist, der er vorgibt zu sein. Dazu erfolgt i.d.R. eine Authentisierung (Authentication), z. B. durch Passwort-Eingabe, Chipkarte oder Biometrie. Das BSI sieht das Schutzziel bzw. den Grundwert Authentizität als Teilziel des Ziels nach Integrität (Integrity).

Das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze heben in ihren Gesetzen, in den Anforderungen an die Sicherheit der automatisierten Datenverarbeitung von personenbezogenen Daten, ebenfalls diese Schutzziele bzw. Grundwerte hervor (siehe fett gesetzte Worte im Gesetzestext) und ergänzen dazu weitere Anforderungen. Diese werden in der Recherche häufig als Gebote zum Datenschutz und zur Datensicherheit angezeigt.

Herausgestellt wird hierbei auch, dass es sich um technische und organisatorische Maßnahmen (TOM) an den Datenverarbeitungsanlagen handelt.

Datensicherheit und Datenschutz

Anforderungen an die Sicherheit bei automatisierter Datenverarbeitung personenbezogener Daten
Erforderliche technische und organisatorische Maßnahmen (TOM) an den Verarbeitungsanlagen, § 64 BDSG

14 Gebote für Datensicherheit und Datenschutz
Verantwortliche und der Auftragsverarbeiter haben nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken (Auszüge des Gesetzes, vgl. § 64 BDSG):

1. **Zugangskontrolle**: Verwehrung des Zugangs zu Verarbeitungsanlagen
2. **Datenträgerkontrolle: Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens** von Datenträgern
3. **Speicherkontrolle:** Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten
4. **Benutzerkontrolle:** Verhinderung der Nutzung mithilfe von Einrichtungen zur Datenübertragung durch Unbefugte
5. **Zugriffskontrolle:** Gewährleistung, dass ausschließlich Berechtigte zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben
6. **Übertragungskontrolle:** Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten übermittelt oder zur Verfügung gestellt wurden oder werden können
7. **Eingabekontrolle:** Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem eingegeben oder verändert worden sind
8. **Transportkontrolle:** Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden
9. **Wiederherstellbarkeit:** Gewährleistung, dass eingesetzte Systeme im Störungsfall wieder- hergestellt werden können
10. **Zuverlässigkeit:** Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden
11. **Datenintegrität:** Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können
12. **Auftragskontrolle:** Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können
13. **Verfügbarkeitskontrolle:** Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind
14. **Trennbarkeit:** Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können

Ein Zweck nach S. 1 Nr. 2-5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

LE 3 - Gefährdungen und Anforderungen

Aufgrund der Schutzziele bzw. der Grundwerte der Informationssicherheit gibt es einen hohen Schutzbedarf für die Verarbeitung von Personendaten in den Unternehmen und Organisationen. Das BSI hat dafür drei Stufungen im Schutzbedarf vorgesehen.

Das BSI hat auch eine Systematisierung von Gefährdungen vorgenommen und 47 elementare Gefährdungen abgegrenzt. Im IT-Grundschutz-Kompendium hat sie zu jedem Basisbaustein passende Gefährdungen und Gefährdungslagen mit Bedrohungen und Schachstellen ergänzt. Als Beispiel ist unten der Baustein „Allgemeiner Client" aufgeführt.



Gefährdungen

Begriff
Gefährdungen (Applied Threats) sind angewandte Bedrohungen (Threats), die über Schwach- steilen auf Objekte, hier Informationstechnik und andere IT-Ressourcen, einwirken. Bezogen auf die Informationstechnik können damit die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigt werden. Dadurch kann dem Besitzer und dem Benutzer der Informationen ein Schaden entstehen, siehe Folien S. 22f. und IT-Grundschutz-Kompendium.

47 elementare Gefährdungen
Das BSI nennt im IT-Grundschutzkompendium (S. 47 ff. GSK) 47 elementare Gefährdungen.

Gefährdungslagen
Im IT-Grundschutz-Kompendium ist zu jedem aufgeführten Baustein eine Gefährdungslage mit spezifischen Bedrohungen und Schwachstellen genannt. Dies hilft den Mitarbeitern bei der Schutzbedarfs- und Risikoanalyse, schneller Bedrohungen und Schwachstellen zu lokalisieren, z. B. Gefährdungslage „Allgemeiner Client", vgl. SYS.2.1: GSK, S. 515 ff.

Gefährdungen

Bedrohungen
Bedrohungen sind beispielsweise Schadprogramme, Datenverlust durch lokale Datenhaltung, unberechtigte IT-Nutzung, Installation nicht benötigter Betriebssystemkomponenten und Applikationen, Abhören von Räumen mittels Mikrofons und Kamera, fehlerhafte Administration oder Nutzung von Geräten und Systemen.

Schwachstellen
Schwachstellen sind beispielsweise Hardware-Defekte durch Fehlbedienung, Software-Schwachstellen oder -Fehler, aus denen Gefährdungslagen entstehen.

Betrachtungen der Gefährdungen und Gefährdungslagen erfolgen nach BSI in den Grundschutzbausteinen und insbesondere in der Risikoanalyse. Die Risikoanalyse erfolgt im Prozessablauf des BSI erst nach den Schutzbedarfsfeststellungen und nach der Modellierung. Modellierung bedeutet, dass für jeden Baustein der IT-Grundschutz-Bausteine festgestellt wird, auf welche Zielobjekte im realen Informationsverbund er anzuwenden ist.

Für jeden Baustein hat das BSI entsprechend den Gefährdungslagen Anforderungen festgelegt, die den Zielobjekten zuzuweisen sind.

Anforderungen, Maßnahmenempfehlungen und Kreuztabellen

Anforderungen
Die im IT-Grundschutz-Kompendium aufgeführten Anforderungen sollten erfüllt werden, um ein angemessenes Sicherheitsniveau zu erreichen. Die Anforderungen sind in Basis- und Standard- Anforderungen sowie Anforderungen für erhöhten Schutzbedarf unterteilt.
Die Basis-Anforderungen stellen das Minimum dessen dar, was vernünftigerweise an Sicherheitsvorkehrungen umzusetzen ist (MUSS-/DARF-Anforderungen). Als Einstieg können sich die Anwender auf die Basis-Anforderungen beschränken, um zeitnah die wirkungsvollsten Anforderungen zu erfüllen. Eine angemessene Sicherheit wird allerdings erst mit der Umsetzung der Standard-Anforderungen (SOLLTE-Anforderungen) erreicht. Maßnahmenempfehlungen und Umsetzungshinweise (Best-Practice-Hinweise, ergänzende Hinweise) ergänzen die Anforderungen.

Kreuzreferenztabellen
Zu jedem Baustein wird im Anhang eine Kreuztabelle dargestellt, die Gefährdungen des Bausteins und Anforderungen in einen Zusammenhang stellt. Zu den Gefährdungen werden jeweils auch die Grundwerte angegeben.

Zielobjekte
Dies sind die direkt betroffenen Objekte der Gefährdungslagen in den Unternehmen und Organisationen. Das BSI hat allgemein als Zielobjekttypen dieser Zielobjekte, z. B. IT-System, Anwendung oder Informationsverbund, übergeordnete Aspekte festgestellt. Diese sind in den Unternehmen speziell zu bezeichnen, z.B. das ERP-System in der kaufmännischen Verwaltung, das Datennetz in der Personalverwaltung, die Benutzerverwaltung aller Arbeitsplatzsysteme, alle USB-Schnittstellen der Arbeitsplatzcomputer.

Risikoanalyse
Zur Beurteilung von Gefährdungsszenarien werden Risikoanalysen als Verfahren häufig eingesetzt. Dabei werden i.d.R. Risiken, denen Zielobjekte ausgesetzt sind, in Abhängigkeit der Eintrittswahrscheinlichkeiten der Schadensereignisse und der möglichen Schadenshöhen bewertet (vgl. BSI-Standard 100-3).

LE 4 - Schadenszenarien und Schadenskategorien

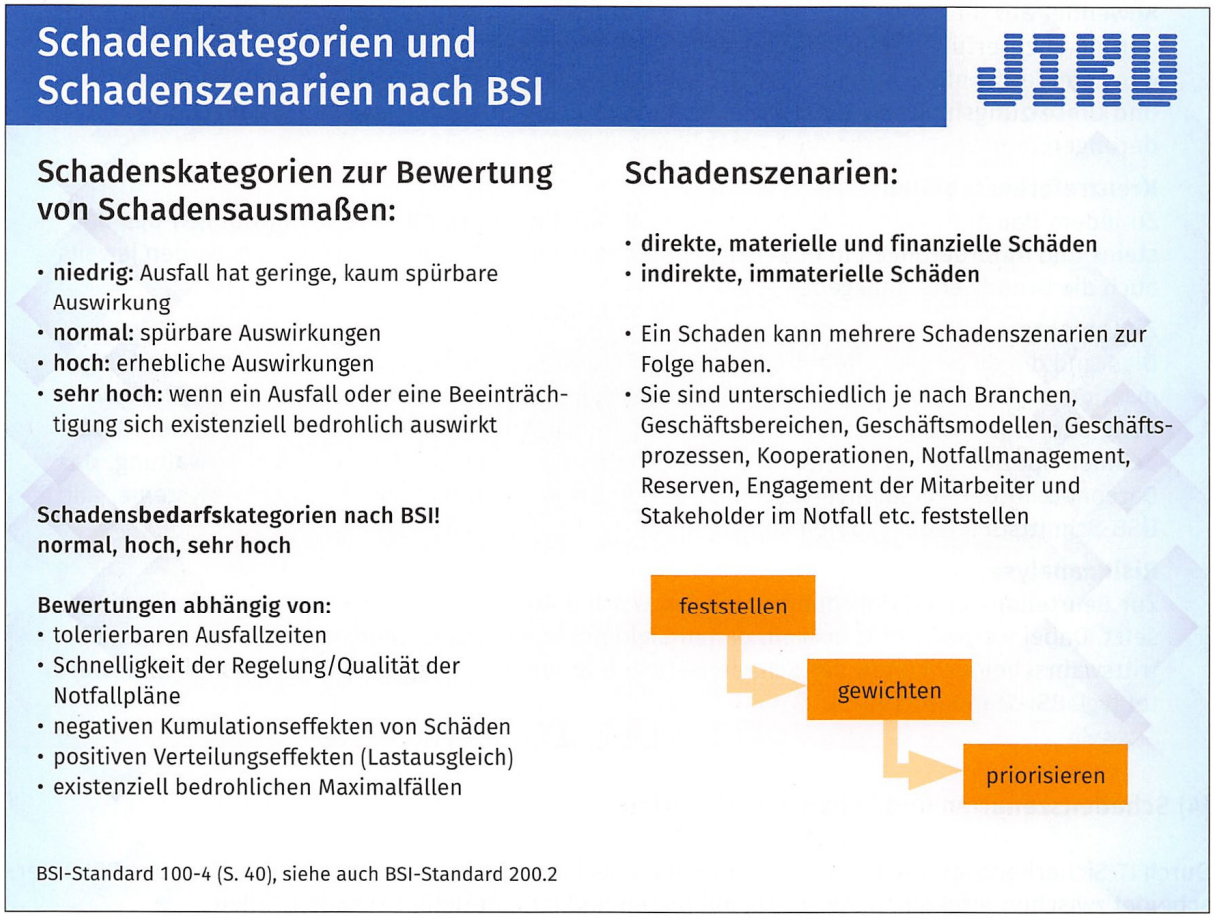
Durch IT-Sicherheitsvorfälle können Unternehmen bis hin zur Insolvenz Schaden erleiden. Das BSI unterscheidet zwischen direkten, materiellen, indirekten und immateriellen Schadensfällen.

Schadensszenarien

Direkte, materielle Schadensszenarien
Das sind beispielsweise finanzielle Auswirkungen wie Gewinn-/Umsatzrückgang, Verlust der Kreditwürdigkeit oder von Marktanteil, Beeinträchtigungen der Aufgabenerfüllung oder negative Auswirkungen, z.B. Absatz- und Umsatzeinbußen, Bußgelder, Rechtanwaltskosten und kostenintensive Sicherheitsdienstleistungen, kostenintensive Pressearbeit, Verlust von Kunden, Entlassungen, Geschäftsunterbrechungen und Geschäftsstillstand, Insolvenz.

Indirekte, immaterielle Schadenszenarien
Das sind beispielsweise fehlende Management- oder Steuerungsinformationen oder Verstöße gegen Gesetze, Vorschriften und Verträge, negative Innen- und Außenwirkung (Imageschaden), Beeinträchtigung der persönlichen Unversehrtheit und des informationellen Selbstbestimmungsrechts der Betroffenen bei personenbezogenen Daten, Rückgang der Mitarbeitermotivation.

Das BSI hat vier Schadenskategorien und vergleichbar drei Schutzbedarfskategorien in ihren Standards festgelegt. Unternehmen können auch differenzierter weitere Kategorien festlegen. Das BSI stellt heraus, dass es nicht immer möglich ist, die Festlegung quantitativ zu begründen, da es neben den direkten, materiellen Schutzbedarfskategorien keine materiellen, indirekten Kategorien gibt (siehe unten). Auch ist bei den Bewertungen zu beachten, dass es Gründe für eine Höher- oder Tieferstufung in der Schadenskategorie gibt.



Schadenskategorien		Schutzbedarfskategorien	
Bezeichnung	**Erläuterung**	**Bezeichnung**	**Erläuterung**
niedrig	Ausfall hat eine geringe, kaum spürbare Auswirkung.	-	
normal	Ausfall hat spürbare Auswirkungen.	normal	Die Schadensauswirkungen sind begrenzt und überschaubar.
hoch	Ausfall hat erhebliche Auswirkungen.	hoch	Die Schadensauswirkungen können beträchtlich sein.
sehr hoch	Ausfall oder Beeinträchtigung führen zu existenziell bedrohlichen Auswirkungen.	sehr hoch	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.
Die Bewertungen sind von verschiedenen Faktoren abhängig (siehe Schaubild S. 29).			

Quelle: BSI-Standard 100-4, S. 40

Lernzielkontrolle TAG 2

1. Rufen Sie das aktuell gültige Landesdatenschutzgesetz (LDSG) Ihres Landes auf und prüfen Sie, welche Maßnahmen hier zum Schutz der personenbedingten Daten aufgeführt sind.

2. Was ist richtig, was ist falsch?

a) IT-Grundschutz ist ein Fachbegriff des BSI.

b) Das IT-Grundschutz-Kompendium ist Teil des BDSG.

c) Die Systematik des BSI-Grundschutzes umfasst acht Basisbausteine.

d) Die Systematik des BSI-Grundschutzes umfasst zehn Schichten.

e) Die Schutzziele des BSI entsprechen fast den Grundwerten des BSI.

f) Authentizität ist nach BSI ein Teilziel des Integritätsziels.

3. Geben Sie die passenden Stichworte an.

a) Die drei Schutzziele des IT-Grundschutzes

b) Oberste Bundesbehörde für Datensicherheit

c) Systematische Untersuchung krimineller Aktivitäten

d) Tabelle mit Gefährdungen und Anforderungen

e) 14 TOM oder Gebote des BDSG

f) Deming-Zyklus zur geregelten Weiterentwicklung

g) Deutsches Wort für Threats.

4. Ordnen Sie Zielobjekte eines Unternehmens den folgenden Bausteinen richtig zu.
APPS - CON - DER - ISMS - IND - INF - NET - ORP - OPS - SYS

a) Arbeitsplatzrechner

b) Browser

c) WLAN-Zugang

d) Sicherheitsbeauftragter des Arbeitsplatzbereichs

e) Stromschwankungen im Stromnetz

f) IoT-Sensor beim kooperativen Roboter

g) Vergabe eines Passwortes eines Arbeitsplatzes an mehrere Personen

h) Notfallrichtlinie am Arbeitsplatz im Gefährdungsfall

i) Ausspähen von Daten bei Softwaretests

j) Datenverlust bei der Datensicherung am Arbeitsplatz

5. Beschreiben Sie in Kurzform Gefährdungen, die die Schutzziele „Verfügbarkeit“, „Vertraulichkeit" und „Integrität" betreffen und geben Sie passend Auswirkungen und passende Maßnahmen an.

Schutzziele nach BSI und Art. 32 DSGVO		
Gefährdungen, die Schutzziele betreffen	Auswirkungen bei Verlust von Schutzzielen	Maßnahmen gegen Verlust der Schutzziele
Verlust der Verfügbarkeit von Informationen personenbezogener Daten und Zielobjekten		
z. B. Stromausfall	*z.* B. Kunden können ihre Konten nicht aufrufen	*z.* B. Stromausfall durch USV beheben
Verlust der Vertraulichkeit von Informationen personenbezogener Daten auf IT-Systemen		
Verlust der Integrität (Korrektheit von Informationen)		

6. Beantworten Sie folgende Fragen zum IT-Grundschutz in eigenen Worten.

a) Wozu dienen die Standards des BSI, das IT-Grundschutz-Kompendium und die Onlineschulungen auf der Webseite des BSI?

b) Welche Bausteine des BSI-Kompendiums gehören zu den zehn Schichten des IT-Grundschutzes und was bedeuten sie, z. B. ORP, SYS?

c) Welche Schutzziele unterscheidet das BSI und welche Grundwerte passen dazu?

d) Warum soll IT-Sicherheit nach dem PDCA-Zyklus bearbeitet werden?

e) Welcher Paragraf der DSGVO verlangt die Sicherheit der Datenverarbeitung und was sind die wesentlichen Forderungen?

f) In welche vier Schadenskategorien sollen Schäden eingestuft werden?

TAG 3 - Aktuelle Bedrohungen zur IT-Sicherheit von Unternehmen präsentieren

Sie sollen für eine Sensibilisierungskampagne in der Klasse, im IT-Bereich oder der Schule aktuelle Bedrohungen präsentieren und erläutern.

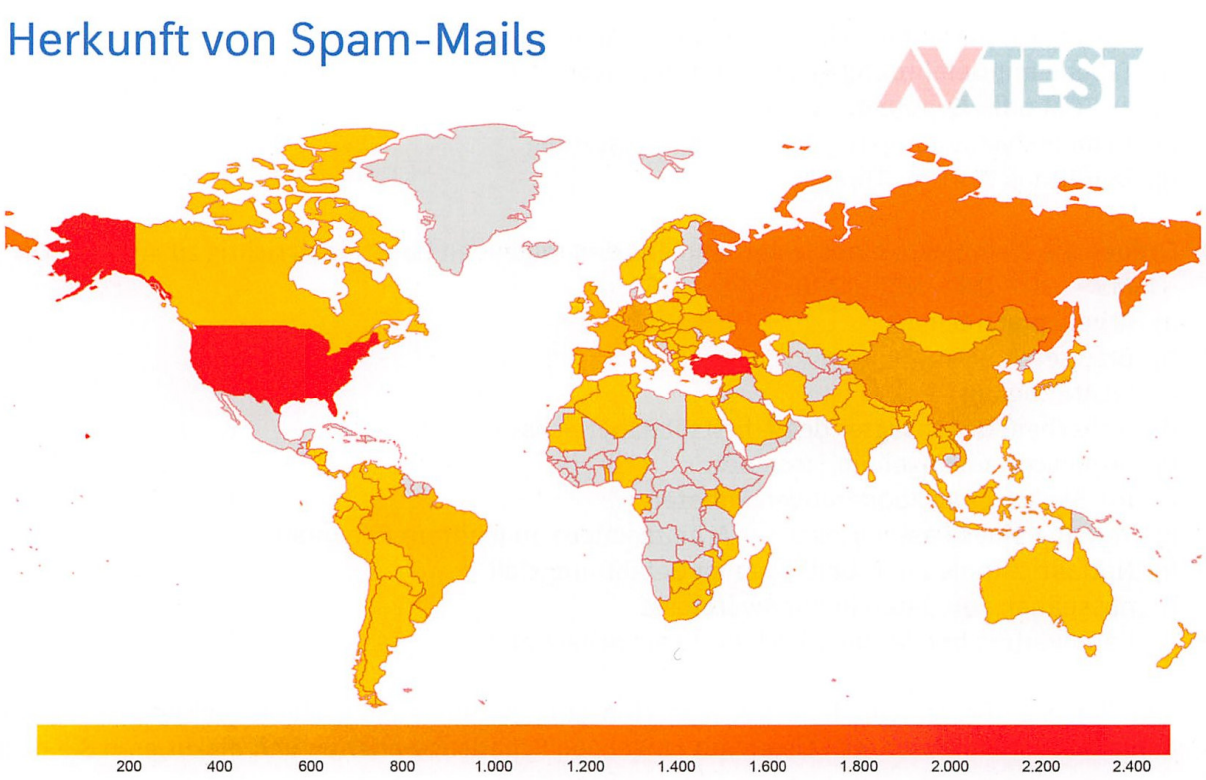
Das BSI versucht, mit seiner Systematik eines IT-Grundschutzsystems Ordnung in die vielfältigen Bedrohungen und Angriffsarten zu bringen. Die Vielfalt und Gewalt der Bedrohungen lässt sich schnell wahrnehmen, wenn Webportale aufgerufen werden, die aktuelle Bedrohungen melden.

LE 1 - Aktuelle Sicherheitsmeldungen in Portalen

Anbieter von Firewalls und Sicherheitstechnik müssen laufend die Gefährdungslagen und Cyberangriffe in Datenbanken festhalten, analysieren und in ihren Produkten umgehend Maßnahmen zur Abwendung dieser Angriffe ergreifen. Diese Unternehmen haben auch Portale aufgesetzt, die laufend über Bedrohungen informieren. Das BSI nimmt ebenfalls Meldungen entgegen. Auch das Angebot des AV-Test-Instituts wird häufig zu Bedrohungslagen aufgerufen.

Beispiele für Sicherheitsmeldungen:

- In Deutschland werden jedes Jahr Schäden in Flöhe von über 43 Milliarden Euro verursacht.
- Die Anzahl der aktuell aktiven Phishing-Webseiten geht in die Hunderttausende.
- Über 50% der berichteten Angriffe sind Malware-Infektionen, von Ransomware-Angriffen ist nahezu jedes zweite Unternehmen schon betroffen gewesen.
- In 90% der Fälle dienen schädliche Anhänge oder Links in E-Mails als Angriffsvektor. Die Hälfte der unterbundenen E-Mail-Angriffe konnten durch technische Maßnahmen verhindert werden, in den übrigen Fällen waren die vorausgegangene Sensibilisierung und Schulung der Beschäftigten die Erfolgsfaktoren.



Quelle: portal.av-atlas.org

Etwa 70% aller Malware-Ausbrüche hatten ihren Ursprung in den Geräten, die Mitarbeiter für die Arbeit einsetzten. PC, Laptops, Mobiltelefone und Tablets dienen Angreifern als Zielobjekte der Unternehmen. Wenn Unternehmensdaten und die Produktivität der Mitarbeiter effektiv geschützt werden sollen, ist ein Fokus auf diese Endpoints unumgänglich.

In aktuellen Sicherheitsmeldungen finden sich häufig martialische Begriffe wie Angriffsarten, Angriffsvektoren oder Angriffsziele. Auch ist häufig die Rede davon, dass sich Staaten, Organisationen und Unternehmen in einem „Cyberkrieg“ mit Cyberkriminellen befinden. Die Kriminalpolizei auf Bundes- und Landesebene haben eigene Cybercrime-Dienststellen eingerichtet, um ihrem gesetzlichen Auftrag der Strafverfolgung nachzukommen.

Cyberangriffe	
Angriffsziele	Ablenkung, Behinderung, Belauschung, Datendiebstahl, Diebstahl personenbezogener Daten, Erpressung, Ideendiebstahl, Schädigung im Wettbewerb, Systemüberlastung, Unternehmensdaten, Unternehmensziele oder politische Ziele zulasten anderer erreichen, Verschleierung durchführen, verschlossene Bereiche öffnen
Angriffsvektoren	Als Angriffsvektor wird die Kombination von Angriffsweg und -technik bezeichnet, mit der sich ein Angreifer Zugang zu IT-Systemen verschafft.
Angriffswege/ Angriffsobjekt	Datenkommunikation, Netzwerk, Web, E-Mail, Datenspeicher (Geräte, Chips, Speicher, Karten), Hardware (Netzwerk, Client, Peripherie, IoT, Adapter, USB, industrielle Steuersysteme, Schnittstellen, Leitungen, Übertragungswege), Protokolle, OS, Software, Treiber, Protokolle, Bibliotheken, Menschen, Nutzer, Social Engineering, Täuschung, Machine Learning und KI-basierte Wege und Objekte
Angriffstechnik	Code-Injection-Angriffe, Diebstahl, Network-Angriffe, Schwachstellenausnutzung, Spam, Trojaner, Malware etc.
Angriffsarten	Ausnutzung von Schwachstellen, Informationsdiebstahl, physische Manipulation von Geräten, Man-in-the-middle-Angriffe (Eindringen in die Mitte zwischen Sender und Empfänger), DoS und DDoS (Angriffe durch Botnets), Malware (Schadsoftware wie Trojaner, Backdoors, Ramsomware)



LE 2 - Malware unterscheiden

Cyberkriminelle greifen täglich mit zehntausenden neuer Schadprogramme (Malware) Endgeräte wie Arbeitsplatzrechner, Notebooks, Tablets oder Smartphones an, um Vorteile zu erlangen oder die Zielobjekte zu schädigen. Die Infektion der Geräte erfolgt über das Herunterladen oder das Aufrufen von Schadprogrammen, die insbesondere über Links, Webseiten oder E-Mails angeboten werden. Über die vernetzten Computer verbreiten sich die Schadprogramme in wenigen Minuten über große Netzbereiche und können Unternehmen und Organisationen, aber auch Privatcomputer, in wenigen Sekunden lahmlegen.



Quelle: portal.av-atlas.org

Schadsoftware - Malware

Adware
Adware ist Schadsoftware, die durch Werbung platziert wird.
Credential Stuffing
Dazu werden geleakte oder generierte Kombinationen aus Benutzernamen und Passwörtern automatisiert gegen den Login-Mechanismus von E-Commerce- und Serviceanbietern gerichtet.

Nicknapping
Nicknapping bezeichnet einen Cyber-Angriff, bei dem der Angreifer unter einem bekannten Namen oder Pseudonym auftritt.

Malware
Malware (Malicious Software) sind Schadprogramme, die wie Viren, Würmer oder Trojaner unauffällig IT-Systeme befallen, auch weitere Schadmodule nachladen können oder unbefugten Zugang („Hintertür", Backdoor) zu Systemen ermöglichen. Sie legen Rechner lahm, spionieren Daten aus oder überschwemmen mit Werbung. Es kann so weit gehen, dass Unternehmen den Betrieb einstellen und Mitarbeiter entlassen müssen. Täglich werden Zehntausende neuer Schadprogramme entwickelt, die darauf ausgelegt sind, Virenschutz-Programme zu umgehen und Sicherheitslücken auszunutzen.

Scareware
Angstsoftware, die versucht den Nutzer dazu zu bringen, auf seinem System schädliche Software zu installieren, indem es System- und Warnmeldungen „vortäuscht".

Schadsoftware - Malware

Viren
Ein Virus ist ungewollt, richtet Schaden an, indem ersieh in den Bootbereich eines Datenträgers einträgt (Boot-Sektor-Virus) oder in andere Dateien einbettet (Dateivirus), wird so auch weiterverteilt.

Würmer
Unterklasse des Virus, kann sich im Gegensatz zum Virus auch von selbst übertragen, indem es die vorhandene Infrastruktur nutzt (z.B. E-Mail-Programm) und sich an alle Adressen verteilt.

Trojaner
Schadprogramm, kein Virus, täuschen echte Anwendungen vor, öffnen in der Regel eine Hintertür im Computersystem, damit andere Schadprogramme daraufzugreifen können, vermehren sich nicht selbstständig.

Verbreitung
Die Verbreitung von Schadsoftware erfolgt durch

- **Herunterladen infizierter Anhänge**, die meist als Bestandteil Interesse weckender E-Mails übermittelt werden;
- **Drive-by-Infection**: cyberkriminelle Webseiten im Internet sind so präpariert, dass Schadsoftware bei Aufruf der präparierten Webseite automatisch heruntergeladen wird;
- **Soziale Netzwerke**, in denen infizierte Anhänge und entsprechende Links geteilt werden;
- **Spear-Infection**: Cyberkriminelle nehmen mittels persönlich adressierter Phishing- oder Infektionsmails gezielt zu bestimmten Personen Kontakt auf, um auf diesem Wege an Daten zu gelangen bzw. den Rechner des Opfers zu infizieren.

PUA (Potentially Unwanted Application)
Es wird im Internet und insbesondere auf Softwareportalen besonders gesuchte Software, z. B. als Freeware, angeboten, die dann aber nicht die gewünschten Leistungen bringt. Die darin integrierte Malware wird nicht sofort erkannt. Sie wird vom Anwender mit der heruntergeladenen Software installiert. Auch beim Löschen des geladenen Programms auf dem Rechner verbleibt die Malware häufig auf dem Rechner und wird bei einem bestimmten Ereignis aktiviert.

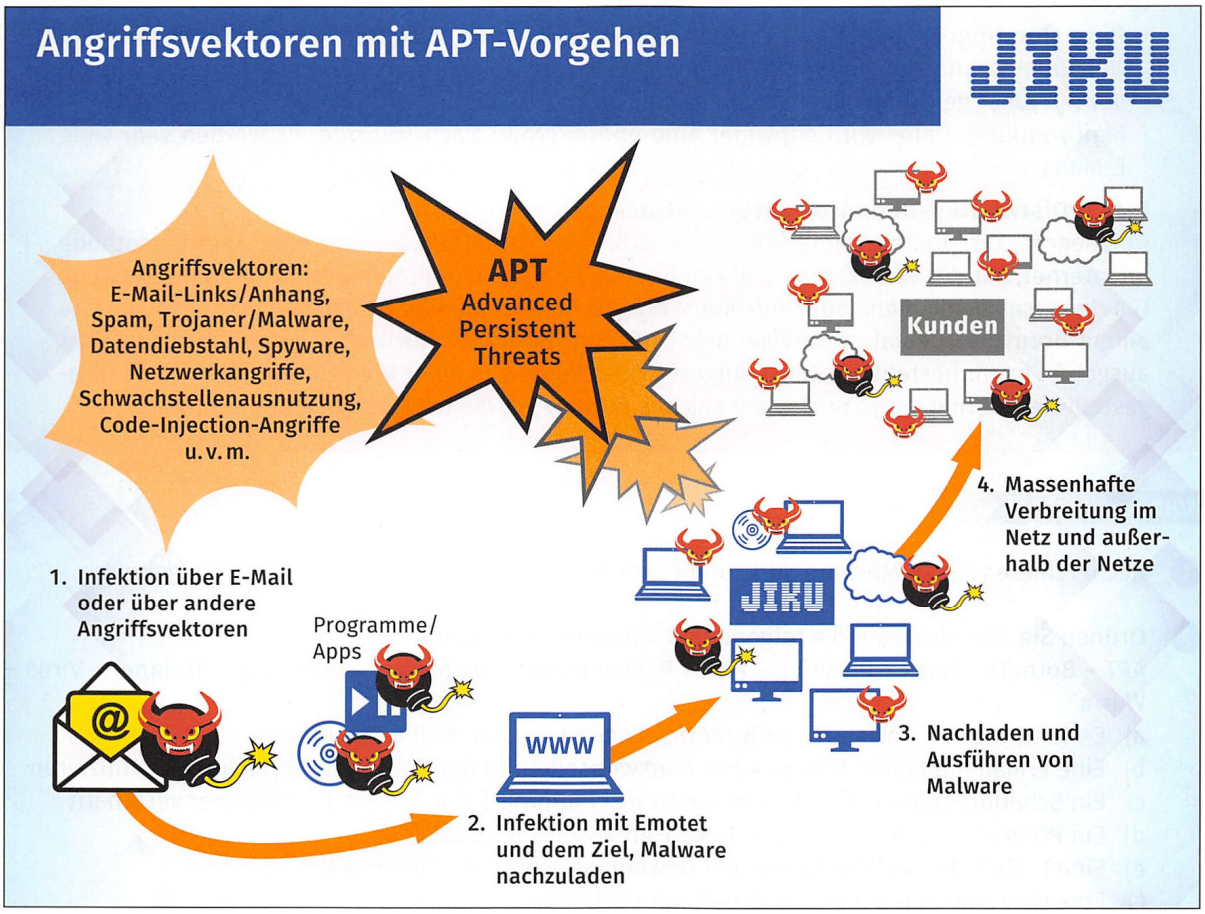
Ramsomware
Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern (Verschlüsselungstrojaner) und diese Ressourcen nur gegen Zahlung eines Lösegeldes (Ransom) wiederfreigeben. Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung.

Spam
Unter Spam versteht man unerwünschte Nachrichten, die massenhaft und ungezielt per E-Mail oder über andere Kommunikationsdienste versendet werden. In der harmlosen Variante enthalten Spam-Nachrichten meist unerwünschte Werbung. Häufig enthält Spam jedoch auch Schadprogramme im Anhang, Links zu verseuchten Webseiten oder wird für Phishing-Angriffe genutzt, sog. Malware-Spam.
Als Spam oder Junk-Mail (Müllpost) bezeichnet man im Internet den Massenversand nicht angeforderter Werbe-E-Mails, Werbebeiträge in Newsgroups, die nichts mit dem Thema der Gruppe zu tun haben, sowie Kettenbriefe. Nach deutschem Recht ist es verboten, fremden Personen unaufgefordert Werbung per E-Mail zuzusenden. Je nach Inhalt lassen sich Spam-Mails in die Bereiche Phishing (vertrauliche Daten wie Passwörter abfischen), Spearing oder Spear- Phishing (gezielt mit beschafften persönlichen Daten nach weiteren Gewinnmöglichkeiten wie mit einem Speer jagen, engl, spear), Hoaxes (Falsch- und Scherzmeldungen einsetzen) und Skimming (Mails mit Gewinnversprechen) unterteilen.

LE 3 - APT, Botnetze und DDoS-Angriffe

Botnet ist ein zusammengesetztes Wort aus den englischen Begriffen „robot" und „network“ und bedeutet so viel wie „massenhafte Fernsteuerung über ein Netzwerk aus Robotern". Häufig werden mehrere tausend Rechnersysteme mit einem Schadcode infiziert und per Command-and-Control-Server (C&C- Server, Fernsteuerung) vernetzt, um dann von Cyberkriminellen zur Durchführung bestimmter Aktionen genutzt zu werden. Botnetze werden oftmals zu gezielten Angriffen auf die Verfügbarkeit von bestimmten Webseiten, sog. Distributed-Denial-of-Service-Angriffe (DDoS-Angriffe), oder zum massenhaften Versand von Spam-Nachrichten eingesetzt.

Relativ einfach und für wenig Einsatz können über das Darknet Cyberkriminelle Botnetze mieten und so Cyberangriffe erfolgreich durchführen. Sie können Zielsysteme ausspähen, diese mit Fake News überschütten und damit die Meinung beeinflussen oder Menschen zu sonst nicht beabsichtigten Käufen oder Taten veranlassen. Das Risiko, Teil einer Botnetz-Attacke zu werden, vor allem bei mobilen Endgeräten, ist hoch. DDoS-Angriffe haben nicht selten Bandbreiten von 150 Gbit/s bis 300 Gbit/s. Die Attacken laufen rasend schnell. Die längsten Attacken dauern häufig nicht einmal zwei Minuten. Mit Malware wie „Emotet" werden Computer infiziert. Sie nutzt komplexe Techniken, die bisher nur bei Advanced PersistensThreats (APT) festgestellt wurden (siehe folgendes Schaubild).



Große Cyber-Attacken

Advanced Persistent Threats (APT)
APT sind Cyber-Angriffe, die gezielt auf Unternehmen/Organisationen gerichtet sind. Cyberkri- minelle versuchen, dauerhaft (persistent) Zugriff auf ein Netzwerk zu erlangen. Hoher Ressourceneinsatz und besondere Kenntnisse der Angreifer (kriminelle Energie) sind dazu notwendig.

Bot/Botnetze
Als Botnetz (Botnet von engl, robotnet = Roboternetz) wird ein Verbund von Rechnern, Smart- phones u.Ä. (Systemen) bezeichnet, die von einem fernsteuerbaren Schadprogramm befallen sind. Die betroffenen Systeme werden vom Botnetz-Betreiber mittels eines Command-and- Control-Servers (C&C-Server) zentral kontrolliert und gesteuert. Die Betreiber bieten damit schädigende Attacken als Dienste an oder betreiben die automatisierten Schadsysteme eigennützig, z. B. für erpresserische Zwecke (vgl. www.botfrei.de).

DoS (Denial of Service)
Denial of Service (DoS) bedeutet „Dienstverweigerung" so viel wie etwas unzugänglich machen oder außer Betrieb setzen. Gekaperte Computer sind nicht mehr zu verwenden, verweigern ihre Dienste, da beispielsweise Webserver durch Massenanfragen zusammengebrochen sind. Formen von DoS sind beispielsweise:

- **Syn Flooding**: Bei einem Syn-Flooding-Angriff werden an ein Computersystem sog. Syn- Pakete geschickt, die anstatt der eigenen Absenderadresse eine gefälschte im Internet erreichbare IP-Adresse tragen, sodass Systemanfragen ins Leere laufen.
- **Ping Flooding**: Hier wird das Programm Ping ausgenutzt, das prüft, ob andere Rechner im Netz überhaupt erreichbar sind. Beim Ping Flooding bombardiert der Angreifer den Zielrechner mit einer gewaltigen Menge von sog. Pings.
- **Mailbombing**: Dabei wird entweder eine enorm große Nachricht oder es werden sehr viele E-Mails an die Zieladresse geschickt und damit der Mail-Server belastet.

DDoS (Distributed-Denial-of-Service-Attacken)
Der Begriff „Distributed-Denial-of-Service-Attacken" (DDoS) bezeichnet eine Angriffsmethode im Internet, mit der versucht wird, ein Zielsystem und seine Internetservices durch Überlastung für den User nicht mehr oder nur stark eingeschränkt nutzbar zu machen. Im Gegensatz zu einem normalen Denial-of-Service-Angriff (DoS-Angriff), der auch von einem einzelnen Host ausgehen kann, besteht ein DDoS-Angriff in der Regel aus einer Vielzahl Anfragen eines ferngesteuerten Botnetzes. Je größer ein solches Botnetz ist, desto wirksamer ist der Angriff.

Lernzielkontrolle TAG 3

1. Ordnen Sie den Aussagen die folgenden Stichwörter richtig zu:

APT - Botnetz - Hoax - Phishing - PUA - Ramsomware - Scareware - Skimming - Trojaner - Virus - Wurm

a) E-Mails, die den Anwender auffordern, etwas zu tun, um sich zu schützen

b) Eine E-Mail mit einem Link zu einer Bankwebseite und der Aufforderung, sich zu identifizieren

c) Ein Schadprogramm, dass einem anderen Schadprogramm Zugang zum Rechner verschafft

d) Ein Programm, dass sich an alle E-Mail-Adressen versendet

e) Eine E-Mail, die den Empfänger mit Gewinnaussichten verführen will

f) Freeware zum Spielen mit eingebettetem Schadprogramm

g) Programm, das den Rechner herunterfährt und nicht mehr starten lässt

h) Malware, die sich im Boot-Sektor einnistet

i) Falschmeldung in einer E-Mail, die zur Eingabe eines Passwortes verleitet

j) Cyberkriminelle versuchen andauernd, Zugriff auf das Netzwerk zu bekommen

k) Netz von vielen infizierten Rechnern legt das Unternehmensnetz lahm

TAG 4 - Identitätsdiebstahl und Social Engineering begegnen

Sie sollen in der Sensibilisierungskampagne Identitätsdiebstahl und Social Engineering stärker herausstellen.

Das BSI stellt die Gefahren durch Social Engineering besonders heraus. Hierbei steht der Mensch als Sicherheitsschwachstelle in der IT im Fokus und die zwischenmenschliche Ausnutzung von IT-Berechtigungen.



Cyberkriminelle unterwandern über Smartphones, Tablets und Apps bei Verbindungen über unsichere Netze die klassische Sicherheitsarchitektur vieler Unternehmen, die auf die Abschirmung des Unternehmensnetzwerks durch Firewalls setzen. Auch Verlust- und Diebstahlrisiken, der Einsatz privater Geräte („Bring your own device") und die Möglichkeit zur Ortung machen mobile Geräte bevorzugt zu Angriffszielen. Neue mobile Arbeitskonzepte bedürfen einer stärkeren Sensibilisierung und Schulung der Mitarbeiter. Mit den Bausteinen ORP.3 (Sensibilisierung und Schulung, GSKS. 121 und der Schwachstelle Social Engineering, GSKS. 123) sowie ORP.4 (Identitäts- und Berechtigungsmanagement, GSKS. 127) gibt das BSI Hilfestellungen, Schwachstellen und Bedrohungen zu schließen.

Social Engineering

Begriff
Über Social Engineering versuchen Cyberkriminelle, Opfer dazu zu bewegen, ihre Daten preiszugeben, um Schutzmaßnahmen umgehen zu können, Daten zu erspähen, zu Falschhandlungen zu animieren oder Schadprogramme installieren zu können. Mit dem Begriff werden Attacken auf Informationen oder Zugänge von IT-Systemen bezeichnet, die durch „Aushorchen von Mitarbeitern" erlangt werden. Dazu baut ein Angreifer häufig einen direkten Kontakt zu einem Opfer auf, z.B. per Telefon, E-Mail oder auch über soziale Netzwerke. Angriffe laufen häufig mehrstufig. Zum Beispiel gibt der Angreifer zunächst Insiderwissen vor und appelliert gleichzeitig an die Hilfsbereitschaft, ihm zu helfen oder verdeckt unzulässig zu handeln. So werden z. B. interne Informationen weitergegeben, womit man IT-Systeme mit Schadsoftware infizieren kann oder es wird über Geschäftskonten Geld an angebliche Geschäftspartner überwiesen (CEO-Fraud, siehe unten). Sowohl im Bereich der Cyberkriminalität als auch bei der Spionage gehen die Täter geschickt vor, um vermeintliche menschliche Schwächen wie Neugier oder Angst auszunutzen und so Zugriff auf sensible Daten und Informationen zu erhalten.

Angler-Phishing
Der Begriff „Angler-Phishing" ist vom Anglerfisch abgeleitet, der mit einem leuchtenden Köder die Beute seiner Opfer imitiert. Bei der Social-Engineering-Variante schalten sich Betrügerin die Kommunikation zwischen dem Kunden und einer Marke ein. Sie geben sich als Kundenservice aus und leiten die Konversation auf einen Fake-Account in einem sozialen Netzwerk oder einer gefälschten Web-Präsenz um.

CEO-Fraud
„Cheftrick“-Methode der Angreifer, „Chefmails" an Mitarbeiter, insbesondere des Rechnungswesens, zu senden, um damit Betrügereien zu unternehmen.

Combosquatting
Combosquatting ist die Nennung eines bekannten Anbieternamens zur Täuschung in der Domain, erweitert mit unüblichen Zusätzen wie Zahlen, für Phishing-E-Mails.

Drive-by-Download/Drive-by-Exploits
Sie bezeichnen die automatisierte Ausnutzung von Sicherheitslücken auf einem Endpoint-Gerät. Dabei werden beim Betrachten einer Webseite ohne weitere Nutzerinteraktion Schwachstellen im Webbrowser, in Zusatzprogrammen des Browsers (z. B. Plug-ins) oder im Betriebssystem ausgenutzt, um Schadsoftware unbemerkt auf dem PC zu installieren.

Doxing
Doxing bezeichnet das vorsätzliche Bloßstellen und Schädigen von Individuen oder Organisationen durch die Verbreitung und Veröffentlichung von Dokumenten, die zusammengetragene personenbezogene Daten enthalten.
E-Mail-Angriffe
E-Mail-Angriffe mit infizierten Office-Dokumenten, die überwiegend über Phishing oder als Spam verbreitet werden, damit Empfänger die Mail-Anhänge oder Links mit Malware anklicken oder über Anmeldeaufforderungen Passwörtern mitteilen.

Identitätsdiebstahl
Rechtswidrige Aneignung von Identifikations- und Authentisierungsdaten, z. B. Benutzername und Passwort, aber auch sonstiger privater Daten, z. B. durch Phishing, Schadsoftware oder computergesteuertes Datensammeln in Social-Media-Portalen und wenig geschützten Online- Clouds.

Keylogging
Beim Keylogging wird Hard- oder Software zum Mitschneiden von Tastatureingaben eingesetzt.

Jailbreak und Rooting
Jailbreak (engl, für Gefängnisausbruch) bezeichnet das benutzergesteuerte Beschaffen von Zugriffsrechten. Dies geschieht, wenn Nutzer Nutzungsbeschränkungen deaktivieren, besonders für Smartphones (Jailbreak mit iOS-Betriebssystem, Rooting bei Android), um vom Hersteller nicht erwünschte Anwendungen zu installieren oder zusätzliche Funktionen freizuschalten. Mit Updates werden i.d. R. Jailbreaks wieder verhindert.

Man-in-the-Middle-Angriffe
Cyber-Angriffe aller Art, bei denen sich jemand in eine Kommunikation einmischt, z. B. zwischen Benutzer und Online-Banking-Portal oder in die Kommunikation zweier Mitarbeiter oder Geschäftspartner, und zu schädigenden Handlungen auffordert, Weitergabe einer App oder Überweisung eines Betrages.

Anforderungen bzw. Maßnahmen
- Passwortregeln und Kennwortrichtlinien beachten
- Geräte am Arbeitsplatz besser vor Diebstahl und Nutzung schützen
- Apps auf Endgeräten nur mit Sicherheitsupdates installieren
- Aufmerksam verfolgen, ob Daten über Apps ausgelesen werden, die für die Funktion der App nicht benötigt werden
- Bildschirmsperre per PIN oder Mustersperre aktivieren
- Einstellungen zum Orten und Fernlöschen anpassen
- Sicherheitsapp installieren
- WLAN-Funknetz und Bluetooth zunächst deaktivieren
- Keine sensiblen Daten auf mobilen Endgeräten speichern
- Vorsicht bei der Nutzung öffentlicher WLAN-Hotspots, nur per WPA2-Standard-Verschlüsse- lung
- Dateien auf den Geräten verschlüsseln, Backups anlegen
- Tools installieren, die gefährliche E-Mails erkennen, z. B. TOrPeDO als Erweiterung des E-Mail- Programms Thunderbird; es warnt User vor Phishing-Mails
- QR-Code-Scanner installieren, die vor Aufruf die Adresse anzeigen

Um Angriffe mit Social Engineering zu unterbinden, sollten Negativlisten mit Malware oder Positivlisten vertrauenswürdiger Webseiten und sichere Passwörter eingesetzt werden.

Höhere Sicherheit durch Blacklisting und Whitelisting

Blacklisting
Blacklisting ist das Führen einer schwarzen Liste mit Dingen, die man ausschließen möchte. Suchmaschinen und Infoportale haben eine Blacklist mit unerwünschten Beiträgen oder Adressaten. In der Suchmaschinenoptimierung (SEO) gibt es Blacklists mit Internetadressen, die gegen Jugendschutz oder unlauteren Wettbewerb verstoßen. Einige Staaten führen Blacklists, um politische Kritik auszuschließen. Google durchsucht proaktiv das Netz nach Malware und setzt Seiten mit Malware auf einen Index, sperrt sie damit für die Suche und warnt User, die die Seiten besuchen (vgl. dazu auch Proxy, S. 368).

Whitelisting
Whitelisting bezeichnet die Zusammenstellung vertrauenswürdiger Quellen und Applikationen in der digitalen Kommunikation und der IT-Sicherheit in einer Positivliste. Als clientseitiges Whitelisting bieten viele E-Mail-Programme solche Funktionalitäten und Filtermöglichkeiten an. Als Application-Whitelisting bezeichnet man Apps oder Plugins, die diese Funktion unterstützen, z. B. Werbeblocker. Serverseitig werden ebenfalls Whitelists geführt, wenn Provider über eine Liste nur vertrauenswürdigen Quellen den Zugang gewähren.

Regelung des Passwortgebrauchs (siehe ORP.4.A8, GSK S. 129)

Sichere Passwörter
Ein sicheres Passwort besteht aus einer (zumindest scheinbar) zufälligen Kombination von mindestens acht Buchstaben, Ziffern und Sonderzeichen. Um sich das gut zu merken, sollte man sich einen bekannten Satz mit mindestens sechs Wörtern aussuchen und dazu die Anfangsbuchstaben verwenden. So wird z. B. aus „Auch ein blindes Huhn findet mal ein Korn“ das Passwort „AebHfmeK"), ergänzt durch Lieblingsziffern (z. B. 007) und Sonderzeichen (z. B. #, ? oder!) ergänzt, Passwort z. B. AebHfmeK007#?.

Passwortgebrauch und Kennwortrichtlinien
Jedes Unternehmen muss für den IT-Grundschutz den Passwortgebrauch verbindlich regeln (siehe ORP.4.A22 Regelung zur Passwortqualität und ORPA.A23 Regelung für passwort-verarbeitende Anwendungen und IT-Systeme). Danach muss das Passwort geheim und sicher aufbewahrt werden und für jede Anwendung anders sein, es darf nur unbeobachtet eingegeben werden. Für einen guten Grundschutz sollten Kennwortrichtlinien in jedem Unternehmen vorhanden sein und strikt angewendet werden.

Zwei- oder Multi-Faktor-Authentifizierung (ZFA/MFA) und Single Sign-on (SSO)
Die Sicherheit von Anmeldeverfahren lässt sich durch ZFA/MFA und SSO oder die Kombination von MFA und SSO deutlich erhöhen. Der Identitätsdiebstahl wird erschwert.

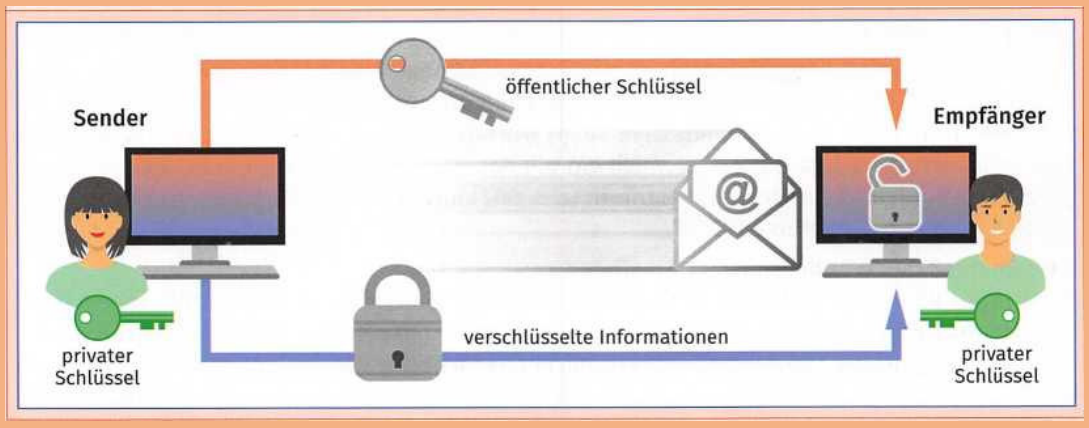
- **Zwei- oder Multi-Faktor-Authentifizierung** (ZFA/MFA): Hierbei handelt es sich um ein Authentifizierungsverfahren, das zwei oder mehr Berechtigungsnachweise (Faktoren) kombiniert. Die verwendeten Faktoren basieren auf biometrischen Merkmalen, speziellem Wissen oder einem mitgeführten Gegenstand und sind voneinander unabhängig. Häufig wird nach der Passworteingabe eine Bestätigung über das Smartphone (Codeeingabe) notwendig.
- **Single Sign-on** (SSO oder „Einmalanmeldung“): Sie ermöglicht über ein SSO-System, dass der Arbeitsplatznutzer sich nur einmal anmelden muss und Zugriff auf alle Dienste und sonstige Ressourcen hat, die er im SSO-System hinterlegt hat. Er muss sich somit für die einzelnen Programme oder Dienste nicht extra anmelden.

Elektronische Siegel und Vertrauensdienste

Qualifizierte Signatur
Um elektronische Signaturen bzw. Siegel (digitale Unterschriften) per E-Mail oder als elektronische Einschreiben zu ermöglichen, wurden die gesetzlichen Grundlagen für elektronische Vertrauensdienste europaweit geschaffen.
Damit E-Mails eine rechtsverbindliche Unterschrift erhalten, können sie mit einer sog. qualifizierten Signatur (als elektronische Unterschrift, Siegel) versehen werden. Das 2017 in Kraft getretene Vertrauensdienstegesetz schafft EU-weit einheitliche Rechtsgrundlagen für elektronische Signaturen sowie neu definierte elektronische „Vertrauensdienste".
Als neuen Dienst führt die eIDAS-Verordnung die elektronischen Siegel ein. Technisch sind diese vergleichbar mit den elektronischen Signaturen. Zur sicheren Speicherung der für die Signa- tur-/Siegelerstellung notwendigen kryptographischen Schlüssel sind qualifizierte Signatur-/ Siegelerstellungseinheiten zuständig, kurz QSEEs.
Aufwww.bundesnetzagentur.de wird eine Anbieterliste der Vertrauensdienste geführt.

Erzeugung und Überprüfung
Zur Erzeugung und Überprüfung einer elektronischen qualifizierten Signatur benötigt man immer ein Schlüsselpaar aus einem privaten (geheimen) und einem passenden öffentlichen Schlüssel (mathematische Schlüssel, die einander zugeordnet sind). Hierdurch werden eine sichere Authentifizierung für Sender und Empfänger sowie Vertraulichkeit und Integrität der übermittelten Daten sichergestellt. Beide Schlüssel sind einer natürlichen Person fest zugeordnet. Der private Schlüssel darf Unbefugten nicht zugänglich gemacht werden, wird bei der Entschlüsselung eingesetzt.

Elektronische Siegel und Vertrauensdienste



E-Mail-Verschlüsselung und Verschlüsselung per PGP und S/MIME

Verfahren
Um die Vertraulichkeit von E-Mails sicherzustellen, wird von einer wachsenden Anzahl von Unternehmen flächendeckend E-Mail-Verschlüsselung eingesetzt. Diese galt bislang, insbesondere aufgrund der hierfür notwendigen Schlüsselverwaltung und der unter Umständen zusätzlich benötigten Client-Software, als aufwendig. Mittlerweile gibt es Verfahren, die die Verschlüsselung über Gateways und Plugins integrativ ermöglichen.

Transportverschlüsselung TLS
Bei der TLS-Verschlüsselung handelt es sich im Gegensatz zu den anderen hier beschriebenen Verschlüsselungsverfahren nicht um eine inhaltliche Verschlüsselung, sondern lediglich um eine Transportverschlüsselung. Die Transportverschlüsselung sichert die E-Mail nach dem Verlassen des Computers bis zum eigenen Mailserver ab. Da diese Transportverschlüsselung am nächsten angesprochenen E-Mail-Server endet, dieser aber nicht zwangsläufig der finale E-Mail-Server des Empfängers sein muss, kann mithilfe TLS vom Absender in der Regel keine durchgängige Verschlüsselung bis zum eigentlichen Zielserver gewährleistet werden.

Ende-zu-Ende-Verschlüsselung der E-Mail-Inhalte
Da eine E-Mail auf dem Weg zwischen verschiedenen E-Mail-Servern nur unzureichend vor dem Ausspähen geschützt ist, sollten sensible Daten des Unternehmens nur Ende-zu-Ende-ver- schlüsselt oder alternativ auf dem Postweg versendet werden. SMIME und OpenPGP sind zwei unterschiedliche, nicht kompatible Verfahren, die beide als sichere Verschlüsselung einzuordnen sind.
OpenPGP-Verschlüsselung
OpenPGP ist ein asymmetrisches Verschlüsselungsverfahren für ein- und ausgehende E-Mails auf Basis der RFCs 4880 und 3156. Erfunden wurde diese Technologie 1991 unter dem Namen Pretty Good Privacy (PGP, deutsch „ziemlich gute Privatsphäre") und ist nach wie vor ein verbreitetes Public-Key-Verfahren. Das OpenPGP-Verfahren ist ein sog. asymmetrisches Verschlüsselungssystem. Es basiert auf dem Prinzip, dass jeder Kommunikationsteilnehmer ein Schlüsselpaar besitzt, das aus einem geheimen und einem öffentlichen Schlüssel besteht. Die öffentlichen Schlüssel werden an die jeweils anderen Kommunikationspartner weitergegeben und dienen zum Verschlüsseln einer Nachricht (die öffentlichen Schlüssel werden beispielsweise im Anhang einer E-Mail verschickt, die vom E-Mail-Programm des Empfängers automatisch als Schlüssel erkannt und gespeichert werden. Nur mit dem zweiten, privaten Schlüssel können die Nachrichten dann wieder entschlüsselt werden. PGP unterstützt daneben auch digitale (elektronische) Signaturen. PGP erlaubt den Nutzern, ein eigenes „Web of Trust" (Vertrauensnetz) aufzubauen, ohne dabei auf eine zentrale Authentifizierungs- oder Zertifizierungsstelle (siehe S/MIME) angewiesen zu sein.

E-Mail-Verschlüsselung und Verschlüsselung per PGP und S/MIME

S/**MIME-Verschlüsselung:**
S/MIME steht für „Sichere/Multizweckmäßige Internet E-Mail Erweiterung" (engl. Secure/Multi- purpose Internet Mail Extension) und ist auch ein asymmetrisches Verschlüsselungsverfahren, das auf einem öffentlichen und privaten Schlüssel basiert. Der Hauptunterschied ist, dass die Schlüsselpaare vergleichbar wie bei der Transportverschlüsselung von einer Zertifizierungsstelle beglaubigt werden. Der öffentliche Schlüssel wird zu der Zertifizierungsstelle hochgeladen, die auf dessen Basis dann ein Zertifikat erstellt, das dann wiederum im Browser oder in E-Mail- Programmen gespeichert wird. S/MIME hat dadurch zwar gegenüber PGP den Nachteil, dass dem Unternehmen Kosten durch die Zertifizierungsstelle entstehen, dafür wird die S/MIME-Verschlüsselung von den meisten E-Mail-Programmen ohne zusätzliche Software unterstützt.

Domain-Verschlüsselung
Dies ist die nutzertransparente asymmetrische Verschlüsselung von Maschine zu Maschine. Diese wird durch den einfachen Austausch des öffentlichen Maschinenschlüssels beider Kommunikationspartner bewerkstelligt. So wird der gesamte E-Mail-Verkehr zwischen zwei Unternehmen oder Geschäftsstellen gesichert.

Managed Domain Service
Als Sonderform der Domainverschlüsselung erfolgt die Verschlüsselung automatisch über einen lokalisierten Schlüsselserver, der die öffentlichen Schlüssel publiziert.

Open-Source-Tools zur Verschlüsselung
VeraCrypt, der Nachfolger von TrueCrypt gehört zu den bekanntesten Tools, wenn es darum geht, Dateien zu verstecken oder zu verschlüsseln. Das Open-Source-Tool ermöglicht das Verschlüsseln einzelner Bereiche oder ganzer Festplatten.

Lernzielkontrolle TAG 4

1. Geben Sie das passende Schlüsselwort an.

a) Sie geben sich als Chef aus und fordern auf, etwas zu tun.

b) Sie tun so, als wären sie Mitarbeiter eines Lieferanten und mischen sich ein.

c) Eine zusätzliche Passwortabsicherung.

d) Unternehmen führen eine Liste mit gefährlichen Webadressen.

e) Es werden personenbezogene Daten von Unternehmen bloßgestellt.

f) Täuschung mit einer Webadresse, in der ein bekannter Name integriert ist.

g) Nutzer schalten die Nutzerbeschränkung ab, um zusätzliche Apps zu installieren.

h) Das Aufzeichnen von Tastatureingaben.

i) Bekanntes Verschlüsselungsprogramm ohne Notwendigkeit einer Zertifizierungsstelle.

2. Kreuzen Sie an, was richtig und was falsch ist

IT-Grundschutz	richtig	falsch
1. BSI steht für Bundesamt für Sicherheit in der Informationstechnik.		
2. Der ISB ist an oberster Stelle verantwortlich für IT-Sicherheit.		
3. DSGVO bedeutet Datenschutz-Grundverordnung.		
4. Als Gesetze sind das BDSG und das IT-Sicherheitsgesetz zu beachten.		
5. Als Standards für IT-Sicherheit sind BSI-Standards und die ISO 27001 zu beachten.		
6. Das BDSG ist seit der EU-DSGVO nicht mehr anzuwenden.		
7. Die DSGVO betrifft nur Unternehmen, die keine personenbezogenen Daten verarbeiten.		
8. Das IT-Grundschutz-Kompendium des BSI enthält Umsetzungshinweise als Bausteine.		
9. Ein ISMS ist das gleichberechtigte Team aus ISB, DSB und QMB.		
10. Neben dem Bundesdatenschutzgesetz gibt es auch Landesdatenschutzgesetze.		
11. Geistiges Eigentum in Software wird durch das UrhG geschützt.		
12. Die IT-Grundschutzbausteine des BSI sind in zwei Ebenen angeordnet.		
13. Das IT-Sicherheitssystem soll im PDCA-Prozess laufend verbessert werden.		
14. Die Schutzziele der DSGVO sind Verantwortung, Integrität und Verlässlichkeit.		
15. Die Schutzziele der DSGVO sind Verfügbarkeit, Integrität und Vertraulichkeit.		
16. Der Grundwert „Authenticity“ ist nach BSI Teil des Schutzzieles Integrität.		
17. Zielobjekte von IT-Grundschutz sind Kunden.		

IT-Grundschutz	richtig	falsch
18. Das BSI unterstützt den IT-Grundschutz entsprechend dem BSI-Gesetz.		
19. Das BSI überarbeitet alle drei Jahre das IT-Grundschutz-Kompendium.		
20. TOM sind technische und organisatorische Maßnahmen entsprechend BDSG.		
21. IT-Sicherheitsschäden werden in fünf Schadenskategorien von niedrig bis hoch eingeteilt.		
22. Das BSI hat fast fünfzig elementare Gefährdungen in seinem Grundschutz-Kompendium herausgestellt.		
23. Mit Kreuzreferenztabellen hat das BSI für Bausteine Gefährdungen und Anforderungen in Zusammenhang gebracht.		

3. Unterscheiden Sie Schadsoftware und kreuzen Sie an, was richtig und was falsch ist.

Schadsoftware	richtig	falsch
1. Malware ist eine allgemeine Bezeichnung für Schadprogramme.		
2. Ein Wurm-Schadprogramm kann sich nicht selbst weiter verteilen.		
3. Ein Trojaner täuscht eine Anwendung vor und ermöglicht den Zugriff von Malware.		
4. Ransomware hat zum Ziel, Lösegeld zu erpressen.		
5. Scareware hat zum Ziel, den Anwender mit Werbung zu erfreuen.		
6. Hoaxes sind Mails mit Gewinnversprechen, Skimming sind Scherzmeldungen.		
7. APT sind starke, andauernde Cyberangriffe mit hohem Mitteleinsatz.		
8. Botnetze greifen den Botbereich der CPU an und unterbinden die Vernetzung.		
9. Durch DoS-Angriffe verweigern infizierte Rechner ihren Dienst.		
10. Bei DDos-Angriffen erfolgen Angriffe von einer Vielzahl von Rechnern.		
11. In einer Blacklist werden alle zuverlässigen Webseiten gelistet.		
12. 1Man-in-the-Middle-Angriffe nutzen für Benutzer zuverlässige Adressen.		

4. Ordnen Sie folgende Schutzmaßnahmen gegen Social Engineering den Anforderungen richtig zu.

Schutzmaßnahmen	
(A) Passwortrichtlinien erstellen und Umsetzung fordern	(D) Präventive Schulung der Mitarbeiter
(B) Mehrfaktor-Authentifizierung	(E) Bildschirmsichtschutz einsetzen
(C) Verschlüsselung	

Anforderungen	
1. Trotz bester Funktion technischer und organisatorischer Schutzmaßnahmen kommt es zu Cyberangriffen	
2. Mitarbeiter verwenden als Kennwort vier Zeichen.	
3. Monitore im öffentlichen Bereich können eingesehen werden.	
4. Kennwörter sollen zusätzlich abgesichert werden.	
5. Dateien sollen bei Versendung nicht von Fremden ausgewertet werden.	

TAG 5 - Technisch-organisatorische Maßnahmen und Beiträge zum Sicherheitskonzept erstellen

Sie sollen in unterschiedlichen Teams Beiträge für ein Sicherheitskonzept präsentieren.

Die gesetzlichen Grundlagen für technisch-organisatorische Maßnahmen (TOM) zur Gewährleistung von IT-Sicherheit bei der Verarbeitung personenbezogener Daten wurden im TAG 2 bereits dargelegt.



Bezogen auf Netzwerksicherheit werden in Modul C die Grundlagen gelegt, z. B. Backupstrategien und der Einstieg in Firewalls. Firewalls schützen heutzutage vor vielen Arten von Malware im Rechenzentrum, im Netzwerk oder in der Cloud. Next-Generation-Firewalls (NGFW) gehen noch einen Schritt weiter, indem sie die Möglichkeit bieten, Malware nicht nur zu identifizieren, sondern auch vollständig zu blockieren und zu bekämpfen, bevor sie in das Netzwerk eindringen können.

Anbieter von IT-Sicherheitslösungen sind entsprechend dem Bedarf für Unternehmen und Privatanwender sehr zahlreich bei Webrecherchen zu finden (siehe auch Linkliste im Arbeitsbuch). Viele Anbieter haben ihre Sicherheitsprodukte und Leistungen in den Angebotsschwerpunkten der E-Mail-Security, Endpoint-Security, Firewall- und Cloud-Security gebündelt. Unter diesen Stichworten lassen sich auch eine große Anzahl Lösungsanbieter und Portale recherchieren.

Bei JIKU IT-Solutions soll ein **Sicherheitskonzept** nach BSI-Standard vorbereitet werden. Um die Sicherheitsziele zu erreichen, müssen entsprechend dem Grundschutzkonzept des BSI in einem Konzept geeignete **technisch-organisatorische Maßnahmen (TOM)** festgelegt werden. Dies sind beispielsweise:

- Maßnahmen zur physischen Absicherung von Gebäuden und Räumlichkeiten,
- technische Vorkehrungen zur Absicherung der Schnittstellen eines Netzes und seiner Segmente,
- Regelungen zum Umgang mit klassifizierten Informationen,
- ein geeignetes Identitäts- und Berechtigungsmanagement,
- die Anwendung kryptografischer Maßnahmen,
- ausreichende Datensicherungsverfahren,
- Verfahren zur Erkennung und Abwehr von Schadsoftware.

Die Erstellung eines Sicherheitskonzeptes, wie es im vorangegangenen Kapitel bereits behandelt wurde, ist der nächste Schritt im Sicherheitsprozess (siehe auch IT-Grundschutz-Schulung des BSI. Die folgende Übersicht zeigt eine Liste von Stichworten, die entsprechend den geforderten technisch-organisatorischen Maßnahmen (TOM) Lösungsansätze sind.

Stichworte von möglichen TOM zur Vorbereitung einer Checklistenerstellung

1. **Zutrittskontrolle (Gebäude, Räume):**
   Besuchsregelung, Gebäude und Räume verschließbar, schriftlich Richtlinien zur Zugangsberechtigung, Überwachungseinrichtungen, Regelung Wartungsarbeiten, Regelungen Schutz bei Anwesenheit, Sicherheit bei Home-/Telearbeit durch Sicherheitskonzept, Einbruchmeldeanlage, Videoüberwachung etc.
2. **Zugangskontrolle Unbefugter zu IT-Systemen/Peripherie**:
   automatische Systemsperren, passende Firewall, sichere Passwörter, Zwei- oder Mehrfaktor-Authentifizierung, Sperrung der Geräteanschlüsse (z. B. USB, Laufwerke) Virenschutzprogramme
3. **Zugriffskontrolle vor Zugriff nicht Berechtigter**:
   Berechtigungskonzepte, Datenträgerverwaltung einrichten (Fernzugriff, Handhabung, Kopieren, Pseudonymisierung, d.h. mit Pseudonym, neutral mit einer Nummer oder Ähnlichem versehen werden), Verschlüsselung, Entsorgung etc., elektronische Signaturen/Siegel bzw. Verschlüsselung von Datenträgern, gesicherte Schnittstellen (USB, Netzwerke etc.), Protokollierung von Zugriffen
4. **Weitergabe-/Transportkontrolle von personenbezogenen Daten**:
   Firewall, Protokolle, Richtlinien zum Transport von Datenträgern und zur Übertragung von Daten, Sicherung der elektronischen Übertragung, Übermittlung und beim Transport, Verschlüsselung, VPN
5. **Eingabekontrolle des Zugriffs auf personenbezogene Daten**:
   Protokollierung Log-Daten
6. **Auftragskontrolle, dass personenbezogene Daten detailliert nur entsprechend Auftrag verarbeitet werden**:
   Richtlinien zur eingeschränkten Verarbeitung, Verpflichtung per Vertrag oder Weisung, Kontrollen, Einsatz unabhängiger Instanzen (z. B. Wirtschaftsprüfer, DSB, Auditoren)
7. **Verfügbarkeitskontrolle, IT-Systemnutzung technisch zu jeder Zeit**:
   Brandschutz, Raumüberwachung, Backup-Konzept, Notfallpläne, Patch-Management, USV, Virenschutz/Firewall
8. **Trennungskontrolle bei unterschiedlichen Aufträgen/Zwecken**:
   Benutzerrechteverwaltung, Funktionstrennung, logische und/oder physikalische Trennung der Datenbestände, Unterweisung der Mitarbeiter zur Trennungskontrolle

9. **Organisationskontrolle als innerbetriebliche Regelung der Verantwortlichkeiten**: Informationssicherheitskonzept vorhanden
10. **Überprüfung der Wirksamkeit der Maßnahmen (TOM):** Audit, Prüfung, Evaluierung, Folgeabschätzung, Schwachstellenidentifikation, Zertifizierung nach ISO 27001
11. **Informationspflichten bzgl. Verarbeitung personenbezogener Daten betroffener Personen:**
    Aufsteller im Unternehmen, Informationsblätter, Hinweise auf Angebote und Rechnungen und andere Geschäftsunterlagen, ggf. mit Link auf eine Internetseite
12. **Verpflichtung der Beschäftigten zur Vertraulichkeit nach Art. 28 und 32 DSGVO**: Schulung, Sensibilisierungsmaßnahmen, Verpflichtungserklärung
13. **Verzeichnisse der Verarbeitungstätigkeiten führen**: z. B. Listen der Betroffenen und der Tätigkeiten

In den Grundschutz-Bausteinen werden jeweils Sicherheitsmaßnahmen vorgeschlagen, die typischerweise für diese Komponenten geeignet und angemessen sind. Für die Erstellung eines Sicherheitskonzeptes sollten die einzelnen Maßnahmen auf Eignung geprüft werden. Es kann notwendig sein, Maßnahmen aufgrund der anzupassenden Dimensionierung und der technischen Entwicklung weiter zu konkretisieren, eventuell andere Maßnahmen zu streichen. Bei der Auswahl und Anpassung der Maßnahmen empfiehlt das BSI eine angemessene Auswahl der Maßnahmen.

Angemessene Auswahl der Maßnahmen von TOM nach DSGVO und BSI

DSGVO Art. 32 (Ausschnitt): Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; ...

Angemessene Auswahl nach BSI: Wirksamkeit, Eignung, Praktikabilität, Akzeptanz, Wirtschaftlichkeit.

Lernzielkontrolle TAG 5

1. Recherchieren Sie in Partnerarbeit zu folgenden Schwerpunktbereichen der IT-Sicherheit.
   Erläutern Sie in Stichworten, was unter den Bereichen zu verstehen ist und warum diese besonders im Fokus der Datenschutz- und IT-Sicherheitsbeauftragten stehen.

Bereiche	Kurzerläuterung
E-Mail-Security	
Endpoint-Security	
Mobile-Security	
Cloud-Security	
Next Gen Firewall	
VPN	

2. Sie sollen für eine Sitzung zum Sicherheitskonzept in Teams Kurzeinführungen geben.

Es sollen Möglichkeiten der Verbesserung der Datensicherung diskutiert werden. Erstellen Sie eine Fragen oder Checkliste mit Präsentationsfolien und verwenden Sie dazu das folgende Material.

Informationsmaterial zur Datensicherung der JIKU IT-Solutions

Datensicherungskonzept: enthält Angaben über Fachverantwortliche, Spezifikation der zu sichernden Daten, Datenvolumen, gesetzliche Auflagen, Vertraulichkeitsbedarf, Integritätsbedarf, Festlegung der Verfügbarkeitsanforderungen und maximale Ausfallzeiten, Rekonstruktionsaufwand der Daten

Verfahrensweise der Datensicherung: Arten (siehe folgend), Häufigkeit, Anzahl Generationen, Speichermedien, Aufbewahrungsorte und -regelungen, Transportregelungen etc.

Datensicherungsarten

Volldatensicherung: Sämtliche zu sichernden Dateien werden zu einem bestimmten Zeitpunkt auf einen zusätzlichen Datenträger gespeichert (Rücksicherung einfach, viel Speicherplatz nötig, eventuell viel Nacherfassungsaufwand).

Inkrementelle Datensicherung: Nur die Dateien werden gesichert, die sich gegenüber der letzten Volldatensicherung oder inkrementellen Sicherung geändert haben (geringerer Speicherplatz, kürzere Datensicherungszeit als Volldatensicherung, kurze Datensicherungszeit, bei Restaurierung eventuell mehr Aufwand und Zeit als bei differenzieller Datensicherung notwendig, da eventuell mehrere Datensicherungen rückgesichert werden müssen).

Differenzielle Datensicherung: Die Dateien werden gesichert, die sich gegenüber der letzten Volldatensicherung geändert haben (mehr Speicherplatz als bei inkrementeller Datensicherung, Dateien lassen sich aber einfacher und schneller restaurieren).

Spiegelung: Eine exakte Kopie der Daten wird laufend in einem anderen Verzeichnis oder Medium erstellt, z. B. als HSM- oder RAID-System. Allerdings werden inkonsistente, mit Malware verseuchte oder verschlüsselte Daten auch gespiegelt, sodass dies kein Ersatz für Datensicherung ist.

Hierarchisches Speicher-Management (HSM): Dateien werden je nach Zugriffshäufigkeit in schnellen Datenspeichern, automatischen Datenträgerwechselsystemen oder Offline-Speichern wie Magnetbändern gehalten bzw. archiviert. Damit werden Speicher möglichst wirtschaftlich eingesetzt.

Redundante Datenspeicherung (RAID/Redundant Array of Inexpensive Disks): Dateien werden auf mehreren Festplatten unter dem Kommando eines sog. Array-Controllers gespeichert. Dabei werden unterschiedliche RAID-Level unterschieden (Level 1: Datenspiegelung). RAID-Systeme ersetzen (z. B. bei Malware, Brand, Diebstahl) keine Datensicherung und besondere Speicherorte.

3-2-1-Datensicherung: Es sollten mindestens drei Kopien der Daten vorhanden sein und Kopien auf zwei unterschiedlichen Medien gespeichert werden. Eine Backup-Kopie soll an einem externen Speicherort gespeichert sein.

Generationenprinzip der Datensicherung (Drei-Generationen-Prinzip): Mehrere Datensicherungen sollten in verschiedenen zeitlichen Abstufungen (als Großvater-, Vater-, Sohn-Sicherung) angelegt werden, um eine Datensicherung wirtschaftlicher (historisch aus der früheren Bandsicherung entstanden) zu ermöglichen, z. B. als Sohn-Sicherung laufende Tagessicherungen einer Woche auf einem Medium, Ende der Woche für vier Wochen zusätzlich eine Vater-Sicherung und Ende des Monats für ein Jahr eine Großvater-Sicherung. Damit können Datenrücksicherungen (bis) zu einem Jahr erstellt werden.

Minimaldatensicherungskonzept nach Empfehlung des BSI

- Software: Vollsicherung einmalig
- Systemdaten: mindestens einmal monatlich mit einer Generation
- Anwendungsdaten: mindestens wöchentlich als Vollsicherung (Drei-Generationen-Prinzip)
- Protokolldaten: mindestens einmal monatlich als Vollsicherung (Drei-Generationen-Prinzip)

Vertrauliche Daten sollten vor der Sicherung möglichst verschlüsselt werden.

3. In einer Sitzung zum Sicherheitskonzept sollen Sie zu folgenden Themen kurz einen Beitrag leisten. Erstellen Sie dazu Informationsfolien, prüfen Sie eine arbeitsteilige Vorgehensweise.

Auszug aus dem Glossar der JIKU IT-Solutions
Datenschutzbeauftragte/-r: Im § 38 BDSG ist festgelegt, dass Unternehmen dann zur Benennung einer/ eines Datenschutzbeauftragten verpflichtet sind, wenn mindestens **20 Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Ergänzend gelten weitere Bedingungen, die unabhängig davon zu einer verpflichtenden Bestellung eines Datenschutzbeauftragten führen können.
Wiederherstellbarkeitsservice (Datenrecovery): Datenrettungssoftware oder Dienstleistung, um durch elektronische oder mechanische Fehler gelöschte oder verloren gegangene Daten wiederherzustellen, Daten auf Datenträgern wieder lesbar zu machen.
Penetrationstest: IT-Sicherheitsexperten führen systematisch Sicherheitstests mit real möglichen Angriffsszenarien auf zu untersuchende Einrichtungen, Personen, Systeme, Anwendungen und Netze durch, protokollieren Vorgehen und Ereignisse, stellen Schwachstellen und Gefährdungspotenziale fest. Unterschiedliche Perspektiven (Innen-/Außentäter), Positionen und Zielobjekte (Räume, Systeme, Netze, Webapplikationen, Webservices oder Mobile Apps) und besondere Schwachstellen (Denial-of-Service, Wartungszugänge, Social Engineering), Gefährdungen eines potenziellen Angreifers werden durch unterschiedliche Testabläufe geprüft.
Digitale Forensik/IT-Forensik: Nach BSI eine nach strengen Maßstäben methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Sicherheitsvorfällen. Sie geschieht im Auftrag der Anlagenbetreiber eines IT-Systems oder zur Klärung oder Vermeidung gerichtlicher Auseinandersetzungen. Das BSI bettet die IT-Forensik in die Prozesse des IT-Betriebs ein und bezeichnet damit die Vorbereitung und die Aufklärung von Vorfällen. Fragen: Was ist geschehen? Wann ist es geschehen? Wie ist es geschehen? Zur digitalen Forensik gehört die gerichtsfeste und verifizierbare Beweissicherung und -auswertung.
Incident-Response-Management (Vorfall-Reaktionsplan): Nach Art. 32 DSGVO ist die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten. Präventiv sollten Sicherheitsvorfälle frühzeitig erkannt und entsprechend Verantwortlichkeiten, Verfahren zur rechtzeitigen Erkennung von Vorfällen und wirksame Maßnahmen zur schnellen Abwendung und Minimierung von Schadensfällen vorgehalten werden.

4. Geben Sie zu folgenden Themen einen kurzen Einblick.

a) Verschlüsselungsverfahren

b) Passwortregeln und Multifaktorauthentifizierung

c) Kriterien für die Auswahl der TOM nach Art. 32 DSGVO und BSI-Standard 100-2 (von 2008)

TAG 6 - Schutzbedarfsfeststellungen anhand eines Beispielunternehmens des BSI vorbereiten

Sie sollen vorbereitende Arbeiten und Elemente zu Schutzbedarfsfeststellungen präsentieren.

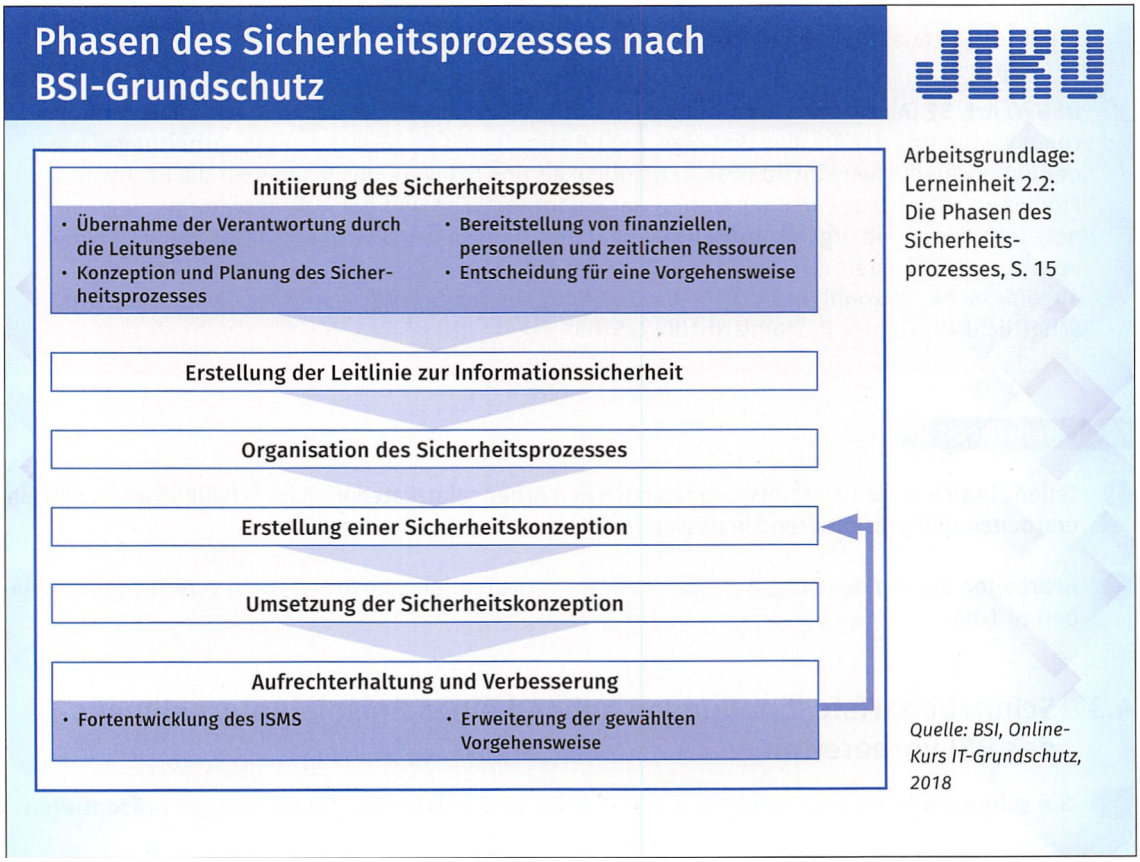
An diesem Tag wird ein Überblick über die Elemente der Schutzbedarfsanalyse gegeben. Weitere Details lassen sich den angegebenen Quellen, insbesondere dem IT-Grundschutzkurs des Bundesamtes für Sicherheit in der Informationstechnik (BSI), entnehmen. Da es in diesem Modul um die Feststellung der Schutzbedarfe in den Arbeitsbereichen der Auszubildenden geht, werden auszugsweise die Bausteine und Zielobjekte des BSI berücksichtigt.

Als Ergänzung zum Online-IT-Grundschutzkurs hat das BSI zur Veranschaulichung ein Modellunternehmen mit dem Namen RECPLAST GmbH entworfen, das auch im BSI-Standard 200.2., S. 82 ff. Verwendung findet. Daher sind in diesem Kapitel ebenfalls Beispiele dieses Modellunternehmens aufgeführt.

LE 1 - Phasen des Sicherheitsprozesses nach dem BSI-Grundschutz beschreiben

Sie sollen Phasen des BSI-Sicherheitsprozesses vorstellen.

Für einen geregelten Sicherheitsprozess empfiehlt das BSI die im Schaubild dargestellte Vorgehensweise. Wichtig ist bei der Initiierung des Sicherheitsprozesses, dass die oberste Leitung nicht nur die Bedeutung und Verantwortung für diesen wichtigen und dauerhaften Prozess herausstellt, sondern ihn auch mit eigener Tatkraft und den notwendigen Ressourcen unterstützt.



Die Erstellung einer Leitlinie zur Informationssicherheit ist daher ein wichtiges Grundsatzdokument der Leitung, um den Stellenwert, die verbindlichen Prinzipien, Ziele, Rahmenbedingungen und das anzustrebende Niveau der Informationssicherheit im Unternehmen herauszustellen. Die Organisation eines Sicherheitsprozesses ist erforderlich, um Verantwortlichkeiten zu schaffen und die erforderlichen Maßnahmen umzusetzen. So müssen beispielsweise neben den Zuständigkeiten die Vorgehensweise, die Art der Kommunikation, der Terminplan, die Protokollierung der Ergebnisse, die Organisation der erstellten Dokumente u.a. festgelegt werden. Die Erstellung eines Sicherheitskonzeptes, wie es im vorangegangenen Tag bereits behandelt wurde, ist der nächste Schritt im Sicherheitsprozess.

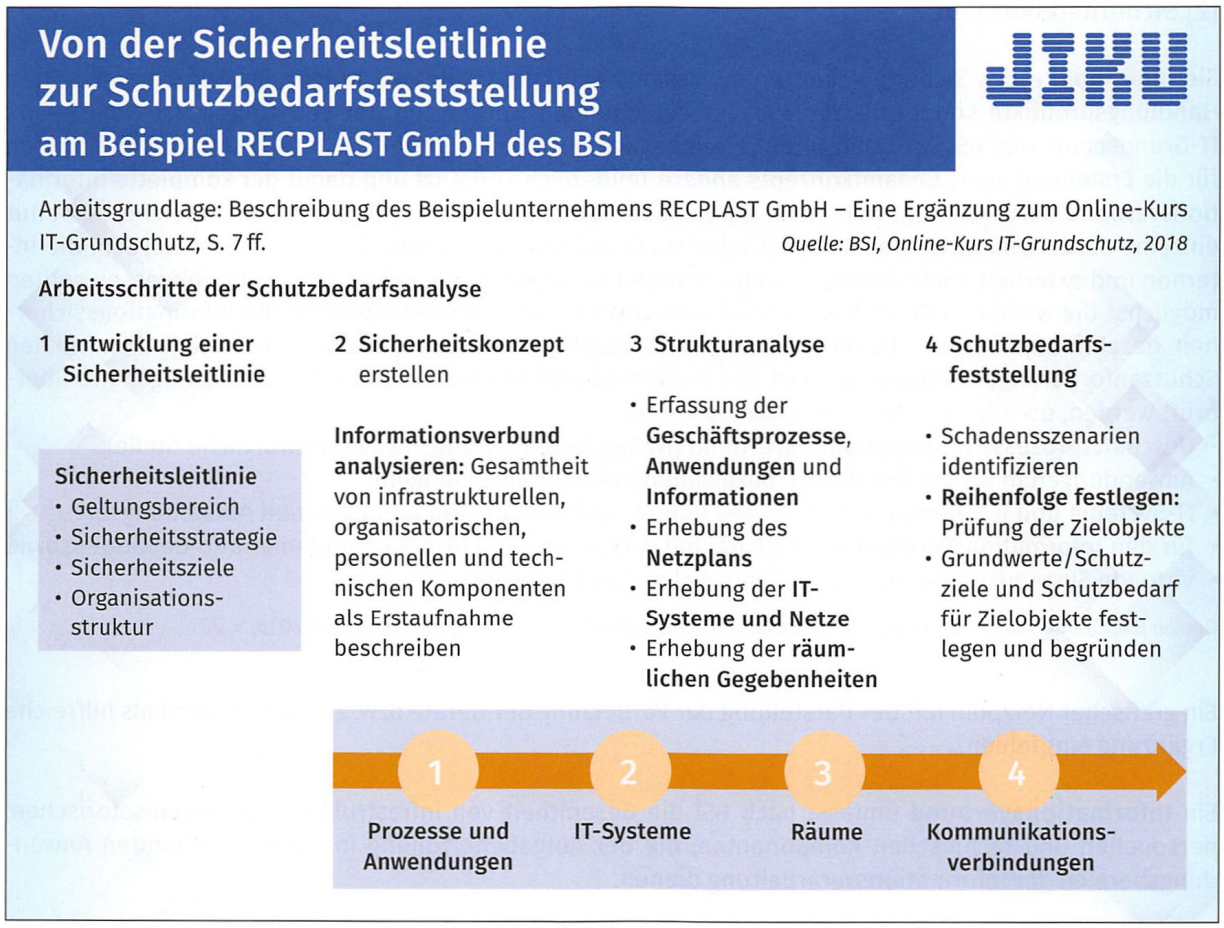
LE 2 - Den Prozess von der Sicherheitsleitlinie zur Schutzbedarfsfeststellung beschreiben

Sie zeigen zunächst Prozessschritte, die der Schutzbedarfsfeststellung vorangehen sollen.

Die Schutzbedarfsfeststellungen sollten auf der Basis einer Sicherheitsleitlinie, eines Sicherheitskonzepts und einer vorangegangenen Strukturanalyse erfolgen.

(1) Entwicklung einer Sicherheitsleitlinie

Eine Sicherheitsleitlinie ist nach BSI ein wichtiges **Grundsatzdokument**, in dem der Stellenwert der Informationssicherheit für die Leitung und die Mitarbeiter, die verbindlichen Prinzipien, das anzustrebende Niveau und die gesetzten Ziele sowie der organisatorische Rahmen formuliert sind. Auch sollte klar geregelt sein, welche Folgen Zuwiderhandlungen haben.



Eine eingesetzte Projektgruppe erarbeitet idealerweise in zwei halbtägigen Sitzungen in enger Kooperation mit der Leitung einen ersten Entwurf für eine Leitlinie. Dieser wird mit der Geschäftsführung abgestimmt und in einer weiteren Sitzung den Abteilungsleitungen und dem Betriebsrat vorgestellt. Nach einer Diskussionsrunde werden eventuell Änderungen vorgenommen, der zustimmende Beschluss der Beteiligten erlangt, die Leitlinie von der Geschäftsleitung unterschrieben und auf einer Betriebsversammlung vorgestellt. Jeder Mitarbeiter sollte eine schriftliche Ausfertigung des Dokuments erhalten bzw. diese im Intranet aufrufen können. Schulungen und Sensibilisierungsaktionen schließen sich an.

Inhalte der Leitlinie zur Informationssicherheit

- Der Geltungsbereich wird konkretisiert.
- Die Bedeutung, die Informationssicherheit für eine Institution hat, wird hervorgehoben [...].
- Die Verantwortung der Leitung wird betont, sowohl im Hinblick auf die Initiierung des Sicherheitsprozesses als auch auf dessen kontinuierliche Verbesserung.
- Es wird auf einschlägige Gesetze und Regulierungsauflagen hingewiesen und die Mitarbeiter werden verpflichtet, diese zu beachten.
- Es werden für die Informationssicherheit besonders wichtige Geschäftsprozesse genannt [...] und auf die strikte Einhaltung von Sicherheitsregeln hingewiesen.
- Die Organisationsstruktur für Informationssicherheit und die Aufgaben der verschiedenen Sicherheitsverantwortlichen werden vorgestellt.
- Sinnvoll ist auch der Hinweis auf Sicherheitsschulungen und Sensibilisierungsmaßnahmen.

Quelle: BSI, Online-Kurs IT-Grundschutz. Druckversion, Lerneinheit 2.7: Die Sicherheitsleitlinien, 2018, S. 20 und BSI-Standard 200.2, S. 32 ff.

(2) Sicherheitskonzept

Ziel und Inhalte des Sicherheitskonzepts wurden bereits in Kapitel 4.2 aufgezeigt. Die dort erstellten Handlungsprodukte können in den Prozess eingebunden werden. (In der Lerneinheit 2.8 Online-Kurs IT-Grundschutz des BSI wird darauf näher eingegangen.) Falls Teilbereiche untersucht wurden, müssen für die Erstellung eines Gesamtkonzepts andere Teilbereiche ergänzt und damit der komplette Informationsverbund berücksichtigt werden. Es sollten aber mindestens immer Organisationsbereiche, nicht nur einzelne Stellen, im Sicherheitskonzept untersucht werden. Auch sollte darauf geachtet werden, die internen und externen Kommunikationsschnittstellen zu beschreiben. Bei den Geschäftsprozessen sollten möglichst die wichtigen Geschäftsprozesse hinsichtlich ihrer Anforderungen für die Informationssicherheit beschrieben werden. Dabei ist anzugeben, welche sehr hohen, hohen oder lediglich normalen Schutzanforderungen anzusetzen sind. Die Zusammenstellung aus Kapitel 4.2 sollte dahingehend überprüft werden, ob folgende Angaben enthalten sind:

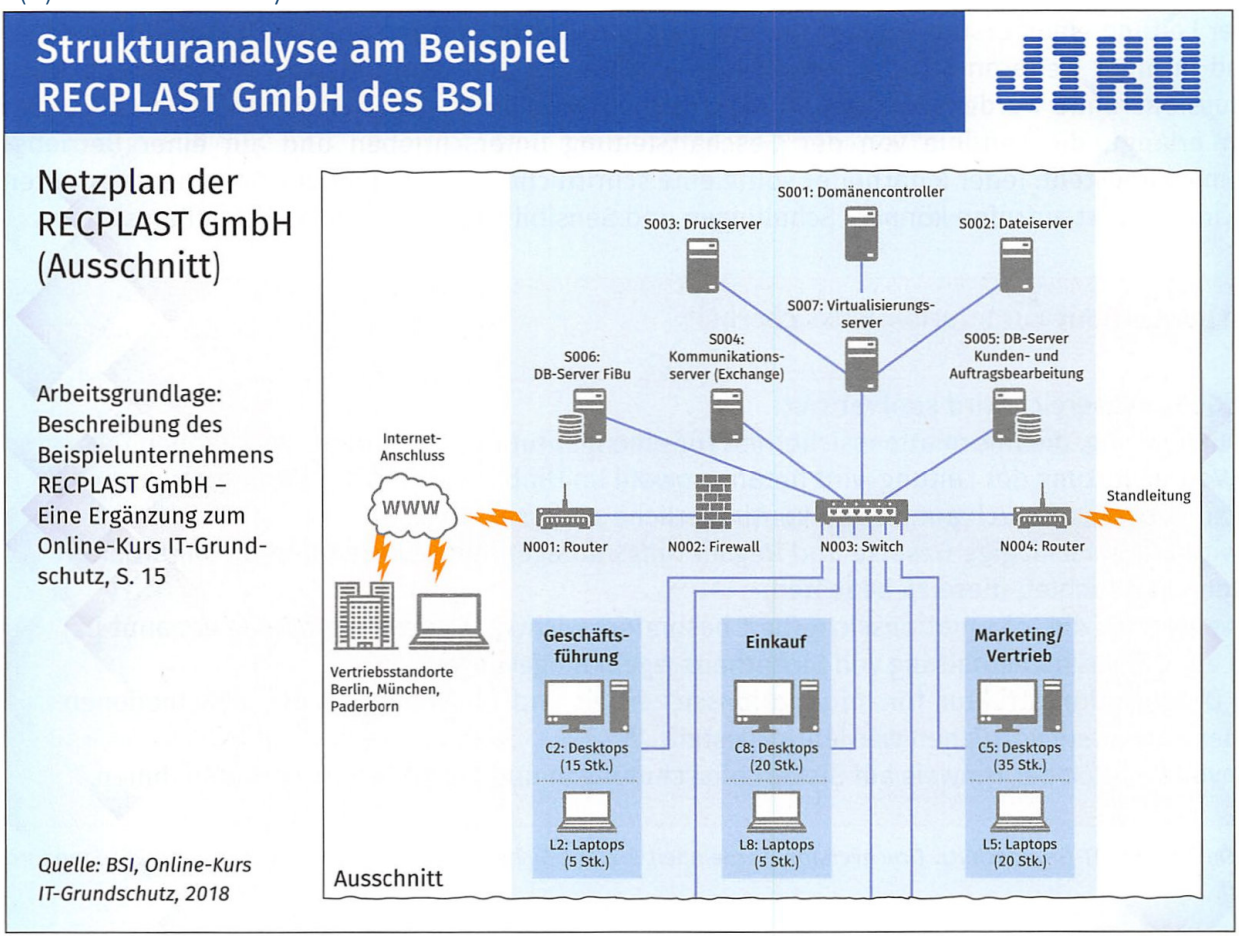
- Geschäftsprozesse im Informationsverbund (Name, Beschreibung, fachverantwortliche Stelle),
- Anwendungen in diesen Prozessen (Bezeichnung und Beschreibungen),
- IT-Systeme und ICS-Komponenten (Bezeichnung, Systemplattform und eventuell Aufstellungsort),
- für den Informationsverbund wichtige Räume wie Serverraum (Art, Raumnummer und Gebäude) sowie
- virtuelle Systeme (entsprechend gekennzeichnet und benannt).

Quelle: BSI, Online-Kurs IT-Grundschutz. Druckversion, Lerneinheit 2.8: Das Sicherheitskonzept, 2018, S. 22

Ein grafischer Netzplan mit der Darstellung der Vernetzung der Geräte bzw. Zielobjekte wird als hilfreiche Ergänzung empfohlen.

Ein **Informationsverbund** umfasst nach BSI die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen.

(3) Strukturanalyse



Ziel der Strukturanalyse ist es, die bisher gesammelten Informationen, insbesondere aus dem Sicherheitskonzept, systematisch aufzubereiten. In der Strukturanalyse werden die Ergebnisse der zuvor durchgeführten Erstaufnahme der Prozesse, Anwendungen und IT-Systeme vervollständigt.

Am Beispiel der RECPLAST GmbH wird aufgezeigt, mit welchen Netzplänen und Tabellen dies erfolgen kann. Im Schaubild sind die vernetzten Komponenten dargestellt. Im vollständigen Schaubild ist auch die Vernetzung zu weiteren Bereichen und zu externen Netzbereichen dargestellt.

Strukturanalyse am Beispiel RECPLAST GmbH des BSI

Erhebung der Systeme und Zuordnung zu Anwendungen

Nr.	Beschreibung	Plattform	Standort	Anzahl	Benutzer/Administrator
C5	Desktops Marketing & Vertrieb	Windows 10	BG, R. 2.03–2.09	35	Marketing und Vertrieb/ IT-Administration
C6	Desktops von Fertigung und Lager	Windows 10	Beuel, R. 2.10–2.13	10	Mitarbeiter Fertigung und Lager/IT-Administration
C7	Desktops der Entwicklungsabteilung	Windows 10	Beuel, R. 2.14–2.20	60	Entwicklung/ IT-Administration
C8	Desktops der Einkaufsabteilung	Windows 10	BG, R. 2.13–2.17	20	Mitarbeiter des Einkaufs/ IT-Administration
C9	Laptops in den Vertriebsbüros	Windows 10	Vertriebsbüros (Be Mü	9	Mitarbeiter in den
L1	Laptops der Finanzbuchhaltung	Windows 10	BG, R. 2		

Ausschnitte

Nr.	Beschreibung	C1	C2	C3	C4	C5	C6	C7	C8	C9
A001	Office-Anwendungen	X	X	X	X	X	X	X	X	X
A002	E-Mail und Terminkalender	X	X	X	X	X	X	X	X	X
A003	Internet-Recherche	X	X	X	X	X			X	X
A004	Prozessleitsystem						X	X		
A005	Entwicklungssystem						X	X		
A006	Personaldatenverarbeitung		X	X						

Arbeitsgrundlage: Beschreibung des Beispielunternehmens RECPLAST GmbH – Eine Ergänzung zum Online-Kurs IT-Grundschutz, S. 18

Quelle: BSI, Online-Kurs IT-Grundschutz, 2018

Die Tabellen zeigen die Liste der Kategorie von Systemen und Anwendungen ausschnittsweise an. Bei den Systemen werden die Standorte und Benutzer angegeben. Weiterhin wurde nach Betriebssystemen und Kategorien von Gerätenutzungen unterschieden. Die Systemkategorien wurden in der Tabelle der Anwendungen den Systemen zugeordnet.

(4) Schutzbedarfsfeststellung

Als Ziel der Schutzbedarfsfeststellung ist zu klären, wie viel Schutz Informationen, Anwendungen und die zugehörigen technischen Systeme und Infrastrukturkomponenten benötigen. Dabei ist zu prüfen und zu begründen, welche Komponenten mehr Sicherheit benötigen und wann elementare Schutzmaßnahmen genügen.

Im Beispiel wurde entschieden, bei den Prozessen und Anwendungen zu beginnen, danach die IT-Systeme, Räume und Kommunikationsverbindungen zu untersuchen.

LE 3 - Elemente der Schutzbedarfsfeststellungen im Beispielunternehmen präsentieren

Sie sollen Elemente zu Schutzbedarfsfeststellungen am Beispiel zeigen.

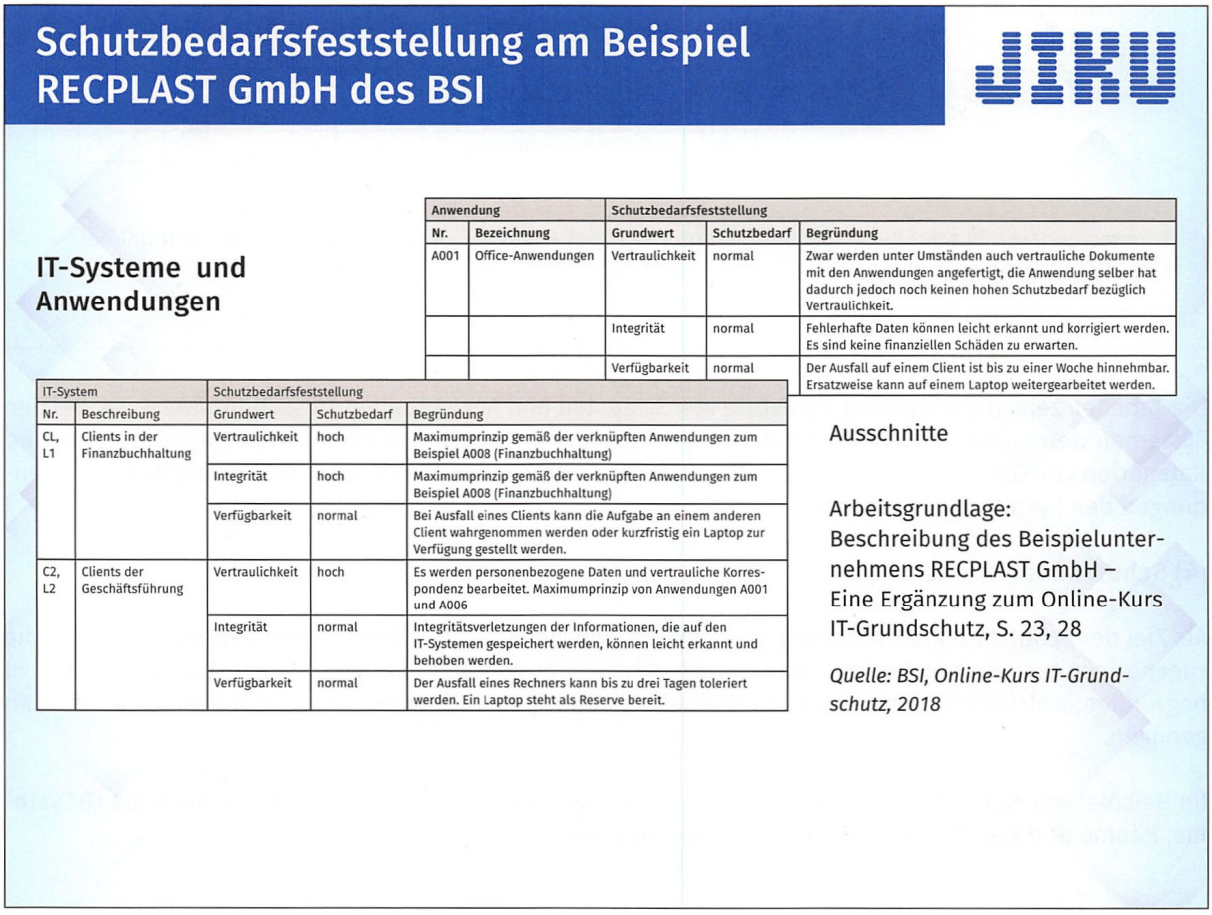
Um den Schutzbedarf festzustellen, sind folgende Aufgaben zu bearbeiten:

Aufgaben bei der Schutzbedarfsfeststellung laut BSI

- Mithilfe von Schadensszenarien sind die Schutzbedarfskategorien für Zielobjekte zu definieren, z. B. Arbeitsrechner Standard.
- Es wird die Reihenfolge im Schutzbedarf für die verschiedenen Zielobjekt-Typen eines Informationsverbundes festgestellt, z. B. mit den Anwendungen begonnen.
- Es werden Abhängigkeiten zwischen den Zielobjekten auf die Ergebnisse der Schutzbedarfsfeststellung aufgezeigt, z. B. welche Anwendungen auf welchen Rechnern.
- Es werden Schlussfolgerungen aus den Ergebnissen der Schutzbedarfsfeststellung gezogen, welche Zielobjekte und deren Schutzziele einen sehr hohen, hohen oder normalen Schutzbedarf haben.

Quelle: Vgl. BSI, Online-Kurs IT-Grundschutz. Druckversion, Lektion 4: Schutzbedarfsfeststellung, 2018, S. 39

Im folgenden Schaubild sind Ausschnitte aus den Schutzbedarfsfeststellungen in der RECPLAST GmbH dargestellt, und zwar für die Zielobjekte „IT-Systeme" und „Anwendungen".



Schutzbedarfsfeststellung am Beispiel RECPLAST GmbH des BSI

JKU

IT-Systeme und Anwendungen

Anwendung		Schutzbedarfsfeststellung		
Nr.	Bezeichnung	Grundwert	Schutzbedarf	Begründung
A001	Office-Anwendungen	Vertraulichkeit	normal	Zwar werden unter Umständen auch vertrauliche Dokumente mit den Anwendungen angefertigt, die Anwendung selber hat dadurch jedoch noch keinen hohen Schutzbedarf bezüglich Vertraulichkeit.
		Integrität	normal	Fehlerhafte Daten können leicht erkannt und korrigiert werden. Es sind keine finanziellen Schäden zu erwarten.
		Verfügbarkeit	normal	Der Ausfall auf einem Client ist bis zu einer Woche hinnehmbar. Ersatzweise kann auf einem Laptop weitergearbeitet werden.

IT-System		Schutzbedarfsfeststellung		
Nr.	Beschreibung	Grundwert	Schutzbedarf	Begründung
CL, L1	Clients in der Finanzbuchhaltung	Vertraulichkeit	hoch	Maximumprinzip gemäß der verknüpften Anwendungen zum Beispiel A008 (Finanzbuchhaltung)
		Integrität	hoch	Maximumprinzip gemäß der verknüpften Anwendungen zum Beispiel A008 (Finanzbuchhaltung)
		Verfügbarkeit	normal	Bei Ausfall eines Clients kann die Aufgabe an einem anderen Client wahrgenommen werden oder kurzfristig ein Laptop zur Verfügung gestellt werden.
C2, L2	Clients der Geschäftsführung	Vertraulichkeit	hoch	Es werden personenbezogene Daten und vertrauliche Korrespondenz bearbeitet. Maximumprinzip von Anwendungen A001 und A006
		Integrität	normal	Integritätsverletzungen der Informationen, die auf den IT-Systemen gespeichert werden, können leicht erkannt und behoben werden.
		Verfügbarkeit	normal	Der Ausfall eines Rechners kann bis zu drei Tagen toleriert werden. Ein Laptop steht als Reserve bereit.

Ausschnitte

Arbeitsgrundlage:
Beschreibung des Beispielunternehmens RECPLAST GmbH – Eine Ergänzung zum Online-Kurs IT-Grundschutz, S. 23, 28

Quelle: BSI, Online-Kurs IT-Grundschutz, 2018

Hier werden den Zielobjekttypen die Schutzziele (Grundwerte) zugeordnet und jeweils angegeben, wie hoch der Schutzbedarf ist. Das Maximumprinzip wird angezeigt, wenn maximaler Schutzbedarf gefordert wird (Schutzziele „Vertraulichkeit - Integrität - Verfügbarkeit", siehe TAG 2 – LE 1.

Schutzbedarfskategorien nach BSI-Standard 200-2	
Kategorie	**Erläuterung**
Sehr hoch	**Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.** Der Ausfall der IT oder wesentlicher Geschäftsprozesse oder die Offenlegung bzw. Manipulation von kritischen Informationen führt zum Zusammenbruch der Institution oder hat schwerwiegende Folgen für breite gesellschaftliche oder wirtschaftliche Bereiche.
Hoch	**Die Schadensauswirkungen können beträchtlich sein.** Insgesamt gilt: Im Schadensfall tritt Handlungsunfähigkeit zentraler Bereiche der Institution ein. Schäden haben erhebliche Beeinträchtigungen der Institution selbst oder betroffener Dritter zur Folge.
Normal	**Die Schadensauswirkungen sind begrenzt und überschaubar.** Insgesamt gilt: Schäden haben Beeinträchtigungen der Institution zur Folge.

Schutzbedarfsfeststellung bei virtualisierten Infrastrukturen	
Kumulationseffekt beim Schutzziel „Vertraulichkeit“	Es sollte geprüft werden, ob durch die Kumulation mehrerer (z. B. kleinerer) Schäden auf dem Virtualisierungsserver ein insgesamt höherer Gesamtschaden entstehen kann. Dann erhöht sich der Schutzbedarf des Virtualisierungsservers entsprechend von „normal“ auf „hoch"
Verteilungseffekt beim Schutzziel „Verfügbarkeit“	Der Schutzbedarf kann sinken, wenn auf den Servern ein Lastausgleich möglich ist (vgl. BSI-Standard 200.2, S. 118)
Maximumprinzip	Es wird in der Begründung (siehe Tabelle oben) als erster Begriff der maximale Schutzbedarf angezeigt und gefordert, durch die systemkritische Bedeutung durch Kumulation und Verknüpfung mit anderen Anwendungen oder Komponenten bedingt.

Als weiteres Element des Schutzbedarfs sollen die Tabellen der Gebäude und Räume sowie der Kommunikationsverbindungen dargestellt werden.

Schutzbedarfsfeststellung am Beispiel RECPLAST GmbH des BSI

Gebäude/Raum				IT/ Informationen	Schutzbedarf		
Kürzel	Bezeichnung	Art	Lokation	IT-Systeme	Vertraulich-keit	Integrität	Verfügbarkeit
R4	Büros Personal-abteilung (BG, R. 1.07–1.09)	Büroräume	GB1	C3, L3	hoch	normal	normal
R12	Büros Entwick-lungsabteilung (Beuel, R. 2.14–2.20)	Büroräume	GB2	C7, L7	sehr hoch	normal	normal
R13	Vertriebsbüros	Häuslicher Arbeitsplatz	Berlin, Hamburg, München	C9, L9, T2	hoch	hoch	normal
R14	Außendienst	Mobiler Arbeitsplatz	Alle Standorte	L1 bis L9	hoch	hoch	normal

Kommunikationsverbindungen		Schutzbedarfsfeststellung		
Nr.	Beschreibung	Grundwert	Schutzbedarf	Begründung
K001	Internetanschluss Bad Godesberg	Vertraulichkeit	**hoch**	Abgefangene E-Mails könnten an den Wettbewerb gelangen.
		Integrität	**hoch**	Ein Großteil der Kommunikation erfolgt über das Internet. Gefälschte Informationen können z. B. den Ruf schädigen.
		Verfügbarkeit	**hoch**	Ohne diese Außenverbindung kann keine Kommunikation mehr stattfinden.

Ausschnitte

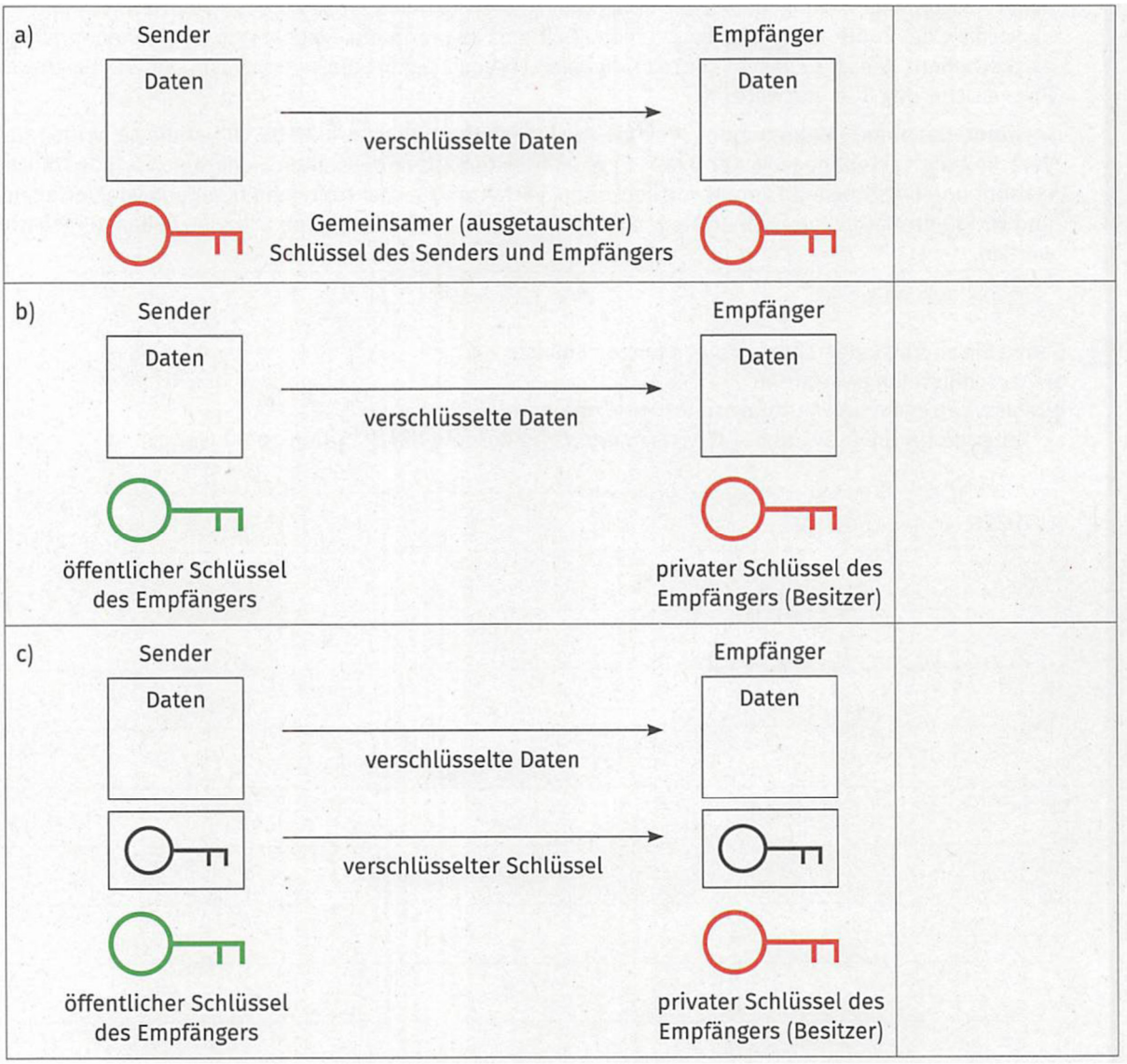
Arbeitsgrundlage: Beschreibung des Beispielunternehmens RECPLAST GmbH - Eine Ergänzung zum Online-Kurs IT-Grundschutz, S. 341 ff.

Quelle: Quelle: BSI, Online-Kurs IT-Grundschutz, 2018

Es werden nur die für IT-Sicherheit notwendigen Informationen erfasst und die zugehörigen IT-Systeme- Kategorien ergänzt. Diese Darstellung dient dem BSI als Muster. Sie enthält den Hinweis, dass die Tabellen individuell nach Bedarf auch anders gestaltet werden können. Wichtig ist, passend zu dem jeweiligen Raumtyp den Schutzbedarf festzulegen. Einzelne Räume sollten nur dann aufgeführt werden, wenn sich Räume nicht zu Raumtypen verallgemeinern lassen bzw. der Schutzbedarf speziell auf einen Raum festgestellt werden soll.

Lernzielkontrolle TAG 6

1. Geben Sie an, um welches Verschlüsselungsverfahren es sich jeweils handelt:



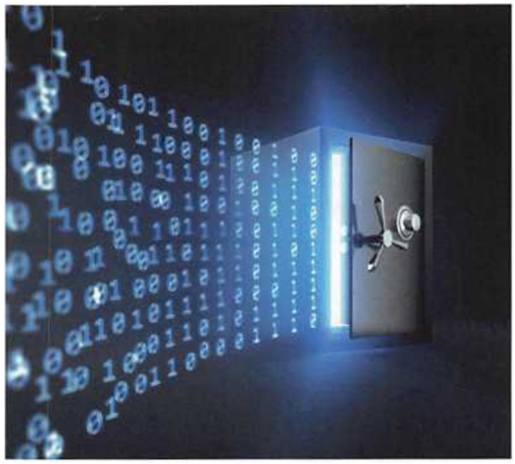
TAG 7 und 8 - Schutzbedarfsfeststellung in Arbeitsbereichen von JIKU IT-Solutions durchführen

Sie wollen den Schutzbedarf für Ihren Arbeitsbereich feststellen, mögliche Gefährdungen erkennen und geeignete Schutzmaßnahmen auswählen.

Nachdem die Grundlagen für den IT-Grundschutz in den vorhergehenden Abschnitten behandelt wurden, werden nun exemplarisch auf Grundlage des BSI-Kompendiums der Schutzbedarf eines Arbeitsbereiches festgestellt, mögliche Bedrohungen ermittelt und geeignete Schutzmaßnahmen empfohlen. Dabei wird zunächst auf die Software und die dazugehörigen Daten eingegangen. Der Schutzbedarf von diesen bildet die Grundlage für den Schutzbedarf der IT-Systeme, auf denen die Software installiert ist und wo die Daten verarbeitet werden. Zum Schluss wird noch die Verwendung von mobilen IT-Geräten und Datenträgern näher betrachtet.

LE 1 - Den Schutzbedarf bezüglich der Arbeitsplatzsoftware feststellen

Sie sollen in unterschiedlichen Teams die Gefährdungen, den Schutzbedarf und entsprechende Schutzmaßnahmen bezüglich der Software in Ihrem Arbeitsbereich ermitteln.

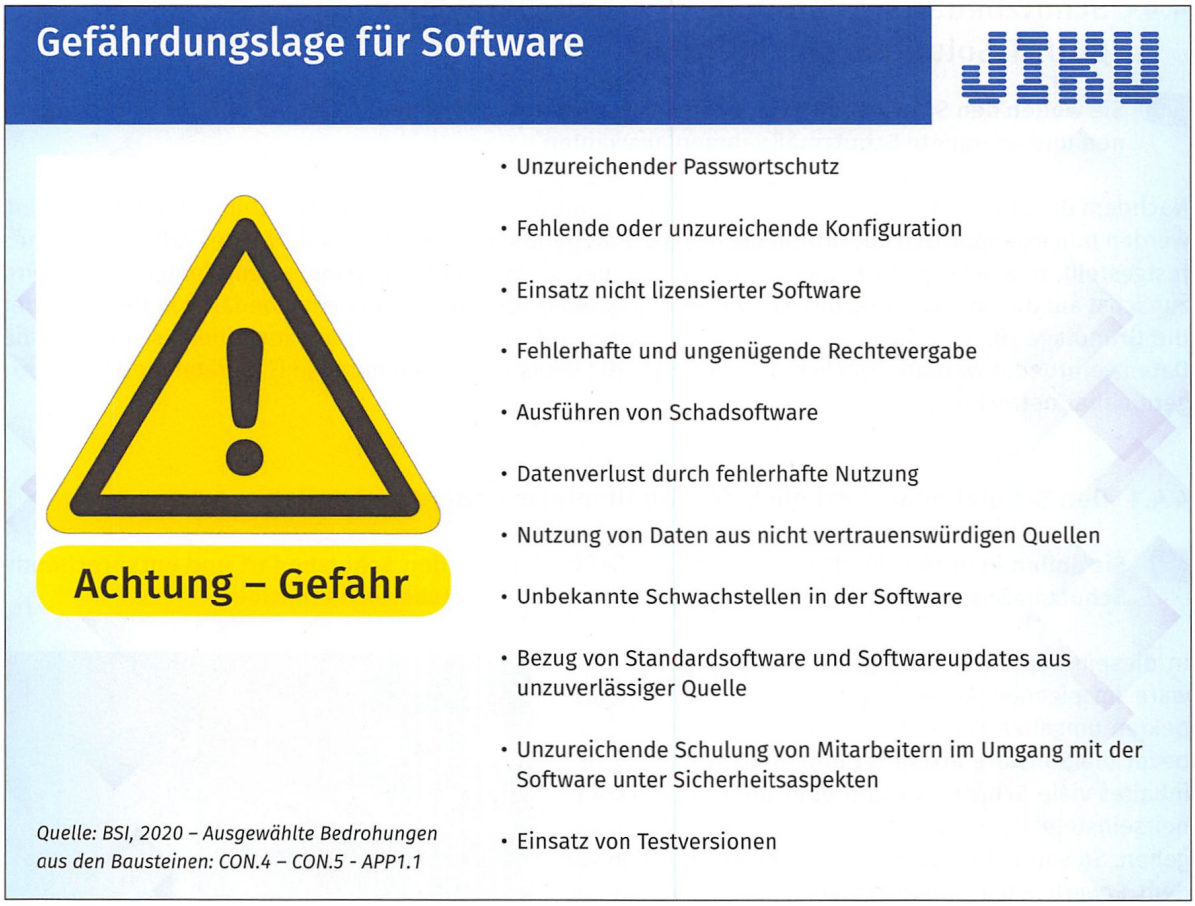


In diesem Kapitel wird dargestellt, wie man mit Software im eigenen Arbeitsbereich unter Sicherheitsaspekten umgehen sollte. Dieser Prozess beginnt schon, bevor die Software installiert und benutzt wird. Er beinhaltet viele Schritte, welche über die reinen Sicherheitseinstellungen innerhalb der Software hinausgehen. So sollte die Software beispielsweise schon vor dem Erwerb nach einem festen Anforderungskatalog ausgewählt werden. Der Installationsprozess ist ebenso zu betrachten wie eine geeignete Verwaltung der Lizenzen. Auch spielt die sichere Deinstallation der Software in diesem Zusammenhang eine Rolle. Dabei werden alle Anwendungen des Arbeitsbereiches betrachtet, welche zuvor bei der Strukturanalyse (siehe TAG 6 LE 1) ermittelt wurden.

(1) Gefährdungslage

In diesem Abschnitt wird die allgemeine Gefährdungslage für Software untersucht. Besonders gefährdet sind dabei Anwendungen, welche sehr verbreitet und auf vielen Rechnern zu finden sind.

Hier handelt es sich in den meisten Fällen um Standardsoftware und deren Schwachstellen sind in der Regel hinreichend bekannt. So gehören beispielsweise Office-Produkte zur Standardausrüstung eines jeden Rechnern. Mithilfe von Makros in Office-Dokumenten lässt sich Schadsoftware teilweise problemlos verbreiten, wenn nicht entsprechende Maßnahmen getroffen werden. Eine weitere Anwendung, welche auf den meisten Rechnern zu finden ist, ist ein Web-Browser. Web-Browser dienen dem Abruf und der Darstellung von Daten aus dem Internet. Bei Nutzung eines Web-Browsers werden die Daten in der Regel auch aus nicht vertrauenswürdigen Quellen geladen. Diese Daten können schädlichen Code enthalten, z. B. Viren, Trojaner, Spyware (siehe TAG 3 LE 3), und den Arbeitsplatzrechner unbemerkt infizieren. Des Weiteren wird manchmal eine Standardsoftware durch Customizing an die Bedürfnisse des Unternehmens angepasst. Insbesondere in diesem Fall müssen auch die Auswirkungen auf die Sicherheit der Software berücksichtigt werden.



(2) Schutzbedarf

Hierbei ist vor allem zu klären, welchen Schutzbedarf die Daten und Prozesse besitzen, welche beim Einsatz der entsprechenden Software bearbeitet werden. Nachfolgend ist ein Beispiel für eine Schutzbedarfsfeststellung für Software bei JIKU IT-Solutions aufgeführt. Dieses Protokoll baut auf dem Beispiel des Modellunternehmens RECPLAST GmbH (siehe TAG 6 LE 3) des BSI auf und wurde für eine Schutzbedarfserststellung eines Arbeitsbereiches entworfen. Die Software, welche bewertet wird, ist in einer vorhergehenden Strukturanalyse ermittelt worden.

Schutzbedarfsfeststellung

IT-Solutions

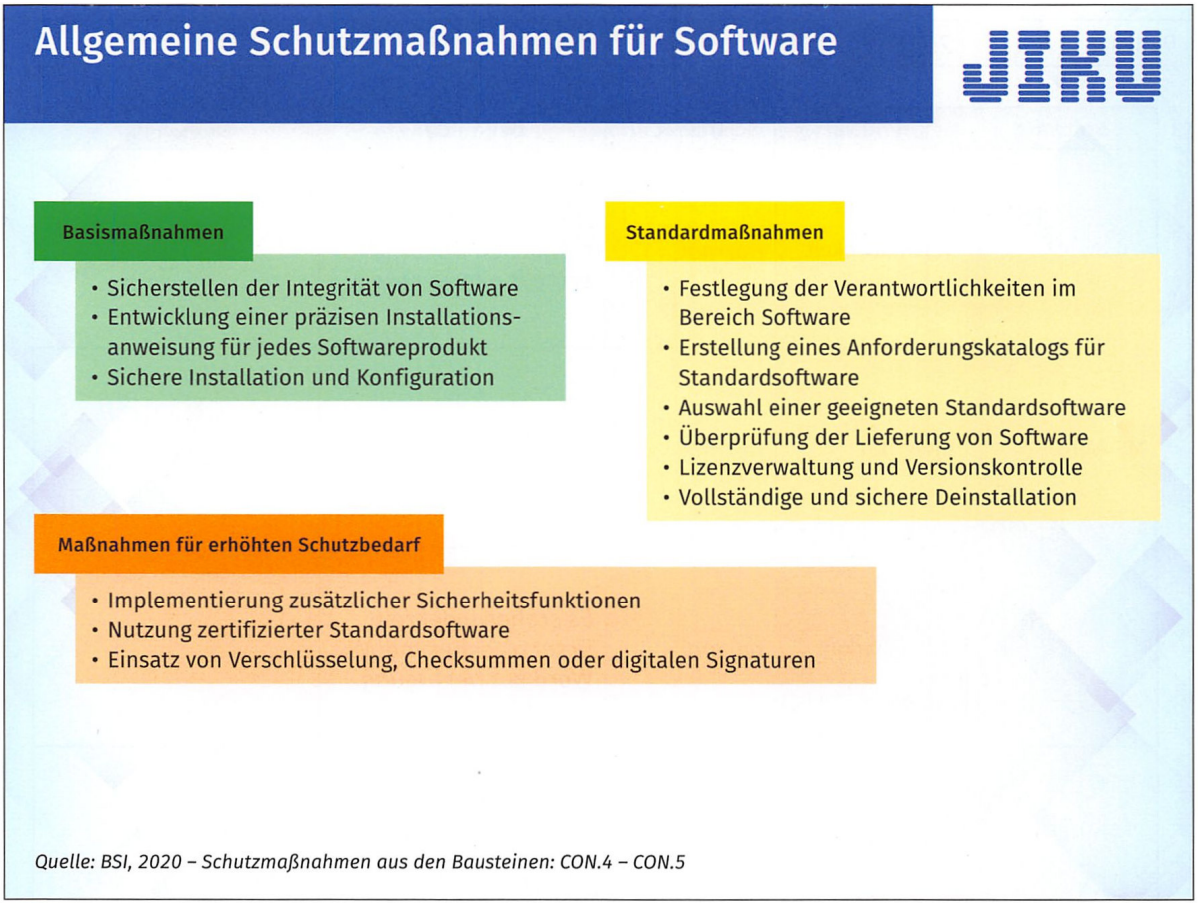
Arbeitsbereich:	PC-Arbeitsplätze in der Marketingabteilung		
Thema:	Schutzbedarf „Software"		
Datum:	25.03.20..	Ersteller:	Levi Kramer

Software	Grundwert	Schutzbedarf	Begründung	Maßnahmen
MS Word	Vertraulichkeit	normal	Hier werden keine vertraulichen Dokumente erstellt oder gelesen.	
	Integrität	normal	Fehler werden leicht erkannt und behoben.	
	Verfügbarkeit	normal	Es stehen jederzeit Ersatzrechner mit MS Word zur Verfügung.	
CMU – Branchensoftware für die Erstellung von Marketingunterlagen	Vertraulichkeit	normal	Hier werden keine vertraulichen oder personenbezogenen Daten verarbeitet.	
	Integrität	hoch	Die Integrität der Marketingunterlagen muss gewährleistet sein.	
	Verfügbarkeit	hoch	Manchmal schnelle Änderungen an Marketingunterlagen notwendig; Software ist, lizenzbedingt, nur auf diesem und einem anderen Rechner installiert.	
...				

Unterschrift: L. Kramer

(3) Generelle Schutzmaßnahmen

Auf Grundlage der Schutzbedarfsfeststellung können nun entsprechende Maßnahmen vorgeschlagen werden. Diese werden dann den entsprechenden Punkten zugeordnet.



Die auf der Folie aufgeführten Maßnahmen gelten für alle Arten von Software. Nähere Erläuterungen von einigen Basis- und Standardmaßnahmen sind in der fogenden Auflistung zu finden. Ausgewählte Schutzmaßnahmen für Betriebssysteme und Office-Produkte werden in den nächsten Abschnitten behandelt.

Beschreibung von Schutzmaßnahmen für Software

Sicherstellen der Integrität von Software
Software sollte nur von Originaldatenträgern oder von geprüften identischen Kopien installiert werden. So sollen Veränderungen an der Software beispielsweise durch Malware, Bit-Fehler oder manipulierte Konfigurationsdateien vermieden werden.

Erstellung eines Anforderungskatalogs für Standardsoftware
Für viele Anwendungsgebiete stehen meistens mehrere Softwareprodukte zur Auswahl. Deswegen sollte ein Anforderungskatalog für die Auswahl einer geeigneten Standardsoftware erstellt werden, in dem neben Aspekten der Funktonalität usw. auch sicherheitsrelevante Anforderungen eine Rolle spielen.

Überprüfung der Lieferung von Standardsoftware
Eine Lieferung von Software ist anhand von vorhandenen Unterlagen zu überprüfen. Es sollte u.a. festgestellt werden, ob die Lieferung bestellt wurde, für wen sie bestimmt ist, ob Transportschäden zu erkennen sind und ob sie vollständig ist.

Beschreibung von Schutzmaßnahmen für Software

Vollständige und sichere Deinstallation von Software
Bei der Deinstallation von Software müssen alle Dateien entfernt werden, die für den Betrieb der Software auf dem IT-System angelegt worden sind. Dieses betrifft auch alle Einträge in die Systemdateien. Um alle Veränderungen, welche durch die Installation der Software vorgenommen wurden, wieder rückgängig zu machen, sollte diese schon beim Installationsprozess hinreichend dokumentiert werden.

(4) Beispielhafte Schutzmaßnahmen für Betriebssysteme

In diesem Abschnitt werden Schutzmaßnahmen betrachtet, mit deren Hilfe die Anzahl der Angriffspunkte auf ein Betriebssystem minimiert werden können. Eine besondere Aufmerksamkeit sollte dabei vor allem Betriebssystemen geschenkt werden, welche auf sicherheitskritischen Servern installiert sind. Allerdings werden die dafür notwendigen Schutzmaßnahmen erst im zweiten und dritten Lehrjahr genauer behandelt. An dieser Stelle gibt es nur einige grundlegende Hinweise.

Auswahl grundlegender Schutzmaßnahmen für Betriebssysteme

Sicherstellen eines minimalen Systems
Es sollten nur alle unbedingt notwendigen Programme installiert sein. Alle weiteren Programme stellen ein zusätzliches Gefahrenpotenzial dar.

Korrekte Konfiguration
Eine Standardinstallation ist für sicherheitskritische Systeme nicht zu empfehlen, weil dabei u.a. nicht benötigte Systemprogramme und Funktionalität installiert werden. In diesen Fällen ist eine individuelle Installation zu bevorzugen.

Ports sperren
Alle nicht benötigen Ports sollten gesperrt werden.

Benutzerkonten
Es sollten nur Benutzer angelegt werden, welche wirklich benötigt werden. Dabei ist darauf zu achten, dass die Benutzer nur die für sie notwendigen Rechte erhalten.

Betriebssystem aktuell halten
Unter Sicherheitsaspekten ist es vor allem wichtig, dass Sicherheitsupdates umgehend nach der Veröffentlichung eingespielt werden.

Regelmäßige Sicherheitschecks mithilfe von Log-Dateien
Mithilfe von Log-Dateien können Angriffe und Angriffsversuche aufgedeckt werden. Dazu sollten die Log-Dateien des Betriebssystems regelmäßig überprüft werden.

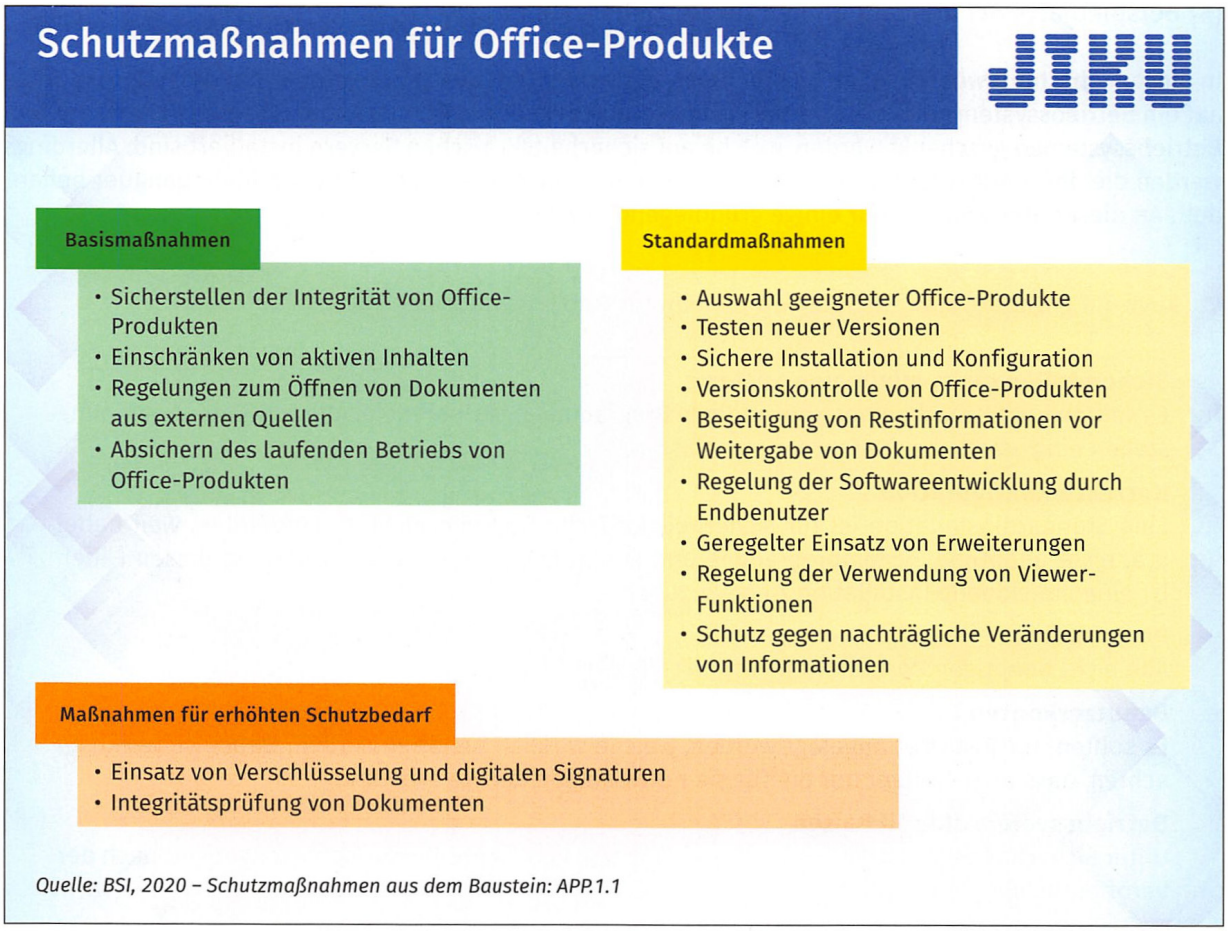
Verwendung von sichereren Passwörtern
Eine der Basisanforderungen ist die Verwendung von sicheren Passwörtern (siehe TAG 4)

Regelmäßig Daten sichern
Bei der Mehrfachnutzung von Rechnern ist das Risiko besonders groß, dass durch Bedienungsfehler oder Vireninfektionen Systeme abstürzen und Daten verloren gehen. Deshalb sollten regelmäßige Backups von den Daten gemacht werden.

(5) Schutzmaßnahmen für Office-Produkte

Office-Produkte wie Microsoft Word, Microsoft Excel, aber auch Libre-Office sind in der heutigen IT-Welt nicht mehr wegzudenken. Sie werden benötigt, um Dokumente, Kalkulationen oder Präsentationen zu erstellen. Somit gehören sie zur Grundausstattung der meisten PCs und sind weitverbreitet. Hierin liegt gleichzeitig die Gefahr dieser Softwareprodukte. Sind erst einmal Schwachstellen in der Software ausgemacht, dann lassen sich sehr viele Systeme angreifen. Office-Produkte sind einer der Hauptangriffswege, um u.a. Schadsoftware zu verbreiten. Aus diesem Grund sollte jedes Unternehmen geeignete Maßnahmen zum Schutz und sicheren Einsatz von Office-Produkten umsetzen.

Die nachstehend aufgeführten Schutzmaßnahmen sind dem Baustein APP.1.1 des BSI Grundschutzkompendiums entlehnt und werden nur auszugsweise erläutert. Für weitere Vertiefung der Kenntnisse, besonders in Bezug auf MS Office und Libre-Office, wird auf diesen Baustein verwiesen.



Einige der ausgewählten Maßnahmen sind bereits aus den allgemeinen Schutzmaßnahmen für Software bekannt und hier speziell auf Office-Produkte ausgelegt. So bedeutet auch in diesem Kontext, dass beim „Sicherstellen der Integrität von Office-Produkten" die Installation nur von Originaldatenträgern zu erfolgen hat. Des Weiteren sollte sichergestellt sein, dass auf allen Arbeitsplätzen der Institution eine möglichst einheitliche Installation und Konfiguration der Office-Produkte erfolgt. Dies ermöglicht beispielsweise eine saubere Deinstallation des Produktes. Auch sollten alle Mitarbeiter in den sicheren Umgang mit Office-Produkten eingewiesen werden und die Regelungen des Unternehmens dazu kennen. Dieses betrifft beispielsweise Regelungen zur Softwareentwicklung durch den Endbenutzer, in denen festgelegt wird, inwieweit der Endbenutzer die Funktionalität des Offices-Produktes durch Makros erweitern darf. In der nachstehenden Auflistung werden einige der Basis- und Standardmaßnahmen näher erläutert.

Schutzmaßnahmen für Office-Produkte

Einschränken von aktiven Inhalten
Aktive Inhalte von Office-Produkten sind beispielsweise Makros, mit denen Berechnungen durchgeführt werden, oder Aktive-X-Steuerelemente, mit denen in Office-Dokumenten umfangreiche Formulare eingebettet werden können. Allerdings können auf diese Weise auch Schadprogramme ausgeführt und verbreitet werden. Deswegen sollte zumindest das automatische Ausführen solcher Inhalte unterbunden werden.

Regelungen zum Öffnen von Dokumenten aus externen Quellen
Das Öffnen von Dokumenten aus unbekannten externen Quellen sollte unbedingt vermieden werden. Solche Dateien sollten bis zu einer vollständigen Sicherheitsüberprüfung als „ausführbare Programme" angesehen werden.

Versionskontrolle
Es sollte dokumentiert werden, welche Versionen von einem Office-Produkt auf welchen Rechnern installiert sind und wie diese konfiguriert wurden. Um Inkompatibilitäten zwischen den einzelnen Versionen zu umgehen, ist anzustreben, dass auf allen Rechnern möglichst die gleiche Version mit einer einheitlichen Konfiguration installiert ist.

Beseitigung von Restinformationen vor der Weitergabe von Dokumenten
Office-Dokumente können eine Vielzahl an Meta-Informationen enthalten. Solche Informationen sind beispielsweise Angaben zum Autor, zur letzten Freigabe oder zur Version des Dokuments. Einige dieser Informationen können auch schützenswert sein. Deshalb sollte genau überlegt werden, welche Meta-Daten ein Dokument enthalten darf und welche nicht. Alle überflüssigen Informationen sind zu entfernen.

Regelung der Verwendung von Viewer-Funktionen
Office-Dokumente können immer Schadcode enthalten, welcher beim Öffnen der Dokumente ausgeführt wird. Dies können Makros sein oder Code, welcher Schwachstellen derSoftware ausnutzt. Viewer dienen nur dem Anzeigen des Dokumentes. Durch die Benutzung von Viewern wird die Gefahr eines Angriffs verringert.

Schutz gegen nachträgliche Veränderungen von Informationen
Die meisten Office-Produkte bieten Funktionen an, mit denen der weitere Umgang mit erstellten Dokumenten eingeschränkt wird. Damit kann beispielsweise ein nachträgliches Bearbeiten des Dokumentes unterbunden werden.

(6) Gefährdungslage und Schutzmaßnahmen beim Einsatz von (Software-)Containern



Aufgrund der zunehmenden Konfigurationen, Tools und Sicherheitsauflagen gestaltet es sich immer schwieriger, Anwendungen in einen anderen Kontext zu portieren. (Software)-Container sind eine Virtualisierungstechnik, bei der ein Wirtssystem mehrere Anwendungen parallel in separierten Umgebungen ausführt. Im Gegensatz zu einer virtuellen Maschine beinhalten Container kein eigenes Betriebssystem, sondern verwenden das des Systems, auf dem sie installiert sind. Ihr eigentliches Potenzial entfalten (Software)- Container aber erst im massenweisen Einsatz, was wiederum ein mögliches Gefahrenpotenzial darstellt. In diesem Kapitel wird kurz betrachtet, welchen Gefahren die Daten, welche in einem Container verarbeitet werden, ausgesetzt sind und welche Maßnahmen zu ihrem Schutz getroffen werden können. Zur Vertiefung des Wissens wird auf den Baustein SYS.1.6 im IT-Grundschutz-Kompendium des BSI verwiesen.

Gefährdungen beim Einsatz von Containern (Baustein SYS.1.6)	
• Schwachstellen in Images • Ausbruch aus dem Container • Administrative Zugänge ohne Absicherung • Datenverlust, z. B. durch Löschung von Containern (fehlende Persistenz)	• Tool-basierte Verwaltung beim Einsatz mehrerer Container ohne Absicherung • Sorglose Verwendung von Zugangsdaten

In vielen Fällen werden Container auf der Basis von vorgefertigten Images erstellt, welche nur noch um eigene Software ergänzt werden. Das spart Arbeit, birgt aber auch die Gefahr in sich, dass die bereits vorhandene Software des Images Schwachstellen enthält und damit das gesamte System angreifbar macht. Diese Schwachstellen sind in der Regel nicht bekannt und auch schwer zu erfassen. Auf der anderen Seite kann die Software zur Verwaltung von mehreren Containern selbst auch Schwachstellen besitzen, welche zur Gefahr werden können. Weiterhin sind die Zugangsdaten sowohl zum Verwalten der Container als auch für die Software innerhalb des Containers gefährdet. Mechanismen zur Authentisierung und Verschlüsselung der administrativen Zugänge sind häufig nicht standardmäßig aktiviert und die Aktivierung wird später auch nicht vorgenommen. Zugangsdaten für die Software innerhalb des Containers sind oftmals ungeschützt im Image zu finden. Auf diese Weise sind nicht nur die Daten selbst gefährdet. Wenn der Angreifer erst einmal in der Lage ist, eigene Programme im Container zu platzieren und auszuführen, dann könnte es ihm auch möglich sein, das Host-System anzugreifen. Eine andere Form der Gefährdung der Daten besteht darin, dass diese nur innerhalb des Containers abgelegt werden. Wird dieser ohne Sicherung der Daten beendet und entfernt, gehen auch alle Daten des entsprechenden Containers verloren. Auf Grundlage einer Schutzbedarfsfeststellung können nun entsprechende Maßnahmen für den Einsatz von Containern vorgeschlagen werden.

Ausgewählte Schutzmaßnahmen beim Einsatz von Containern (Baustein SYS.1.6)	
Basismaßnahmen	**Standardmaßnahmen**
• Planung des Container-Einsatzes • Planung der Anwendungen in Containern • Planung der Verwaltung der Container • Sicherung des Host-Systems • Separierung der Container • Verwendung sicherer Images • Anwendung von Schutzmaßnahmen für die Containersoftware • Sicherung der Zugangsdaten • Speicherung von wichtigen Daten außerhalb des Containers	• Erstellen einer Richtlinie für den Betrieb von Containern • Erstellen einer Richtlinie für die Images von Containern • Nur eine Anwendung bzw. Dienst pro Container • Sicherstellung der Unveränderlichkeit von Containern • Limitierung der Ressourcen pro Container • Erstellung von Richtlinien für das Einbinden von Datenträgern in Containern • Regelmäßige Überwachung von Containern
Maßnahmen für erhöhten Schutzbedarf	
• Automatisierte Auditierung von Containern, eigene Trusted Registry für Container • Erstellung erweiterter Richtlinien für Container, Host Based Intrusion Detection für Container • Mikro-Segmentierung von Containern, Hochverfügbarkeit von Container • Verschlüsselte Datenhaltung bei Containern, Verschlüsselung der Netzkommunikation zwischen Containern	

LE 2 - Den Schutzbedarf bezüglich der Clients eines Arbeitsplatzes feststellen

Sie sollen in unterschiedlichen Teams die Gefährdungen, den Schutzbedarf und entsprechende Schutzmaßnahmen bezüglich der Clients in Ihrem Arbeitsbereich ermitteln.



Der Schutzbedarf eines IT-Systems generell hängt im Wesentlichen von dem Schutzbedarf der Software und den dazugehörigen Daten ab, welche mit diesem IT-System verarbeitet werden sollen. Deswegen ist der Schutzbedarf des IT-Systems mindestens ebenso hoch anzusetzen. Hier gilt das **Maximumprinzip**.

Auf der anderen Seite kann natürlich der Schutzbedarf eines IT-Systems auch höher sein als der Schutzbedarf seiner Software und seiner Daten, z.B. wenn dieses System in einem Verbund mit anderen IT-Systemen steht. In diesem Fall spricht man auch vom **Kumulationseffekt**.

In diesem Kapitel werden von den IT-Systemen speziell die Clients (siehe Modul C) betrachtet. Ein Client ist mit einem Betriebssystem ausgestattet und in der Regel mit anderen Clients und Servern vernetzt (siehe Modul C). Außerdem besitzen Clients meistens Laufwerke und Schnittstellen für den Datenaustausch mithilfe von mobilen Datenträgern (siehe Modul B).

(1) Gefährdungslage

Clients sind auf unterschiedlichste Art und Weise gefährdet. Auf der einen Seite sind die Gefährdungen zu betrachten, welche im Zusammenhang mit der Hardware stehen. Auf der anderen Seite sollte der Blick auf Gefährdungen im Zusammenhang mit dem Betriebssystem und den Softwarekomponenten gerichtet werden. Als dritter, nicht zu unterschätzender Punkt kommen noch die Gefährdungen durch Fehlbedienung durch den Benutzer hinzu.

Gefährdungslage von Clients

- Schadprogramme
- Datenverlust durch lokale Datenhaltung
- Datenverlust durch Hardwaredefekte
- Softwareschwachstellen oder Fehler
- Unberechtigte Benutzung
- Installation nicht benötigter Betriebssystemkomponenten und Applikationen
- Abhören von Räumen mittels Mikrofon und Kamera
- Fehlerhafte Administration oder Nutzung von Geräten und Systemen



Achtung – Gefahr

Quelle: BSI, 2020 – Ausgewählte Bedrohungen aus dem Baustein: SYS.2.1

Dieses macht Clients besonders anfällig für Schadprogramme jeglicher Art. Dabei sind die Einfallstore sehr vielfältig und reichen vom Öffnen von E-Mails mit schädlichem Inhalt bis zum Anschließen von mobilen Datenträgern, welche Schadsoftware enthalten. Dadurch, dass die Clients in der Regel vernetzt sind, können sich die Schadprogramme danach im schlechtesten Fall im ganzen Unternehmen verteilen. Eine weitere große Gefahr besteht in dem Verlust von (wichtigen) Daten, wenn diese nur lokal gespeichert werden und auf diese, durch defekte Hardware oder Bedienungsfehler, nicht mehr zugegriffen werden kann. Auch die Gefahr des Informations- und Datendiebstahls ist nicht zu unterschätzen. Dieses kann beispielsweise direkt über die unberechtigte Benutzung des Clients oder indirekt durch das Abhören von Räumen mittels des Clientmikrofons geschehen.

(2) Schutzbedarfsfeststellung

Auch bei der Schutzbedarfsfeststellung für Clients werden die drei Grundwerte „Vertraulichkeit - Integrität - Verfügbarkeit" betrachtet. Nachfolgend ist ein Beispiel für eine Schutzbedarfsfeststellung für Clients bei JIKU IT-Solutions aufgeführt. Dieses Protokoll baut erneut auf dem Beispielunternehmen RECPLAST GmbH des BSI (siehe TAG 6 LE 3) auf und wurde für eine Schutzbedarfserststellung eines Arbeitsbereiches entworfen. Die Clients, welche bewertet werden sollen, sind vorher in einer Strukturanalyse zu ermitteln, In dem abgebildeten Beispiel geht es um Clients in der Personalabteilung. Es ist davon auszugehen, dass dort noch mehr Clients vorhanden sind. Hier wurden nur exemplarisch zwei Clients ausgewählt.

Schutzbedarfsfeststellung

ITKU IT-Solutions

Arbeitsbereich:	PC-Arbeitsplätze in der Personalabteilung		
Thema:	Schutzbedarf „Clients"		
Datum:	12.08.20..	Ersteller:	Peter Dager

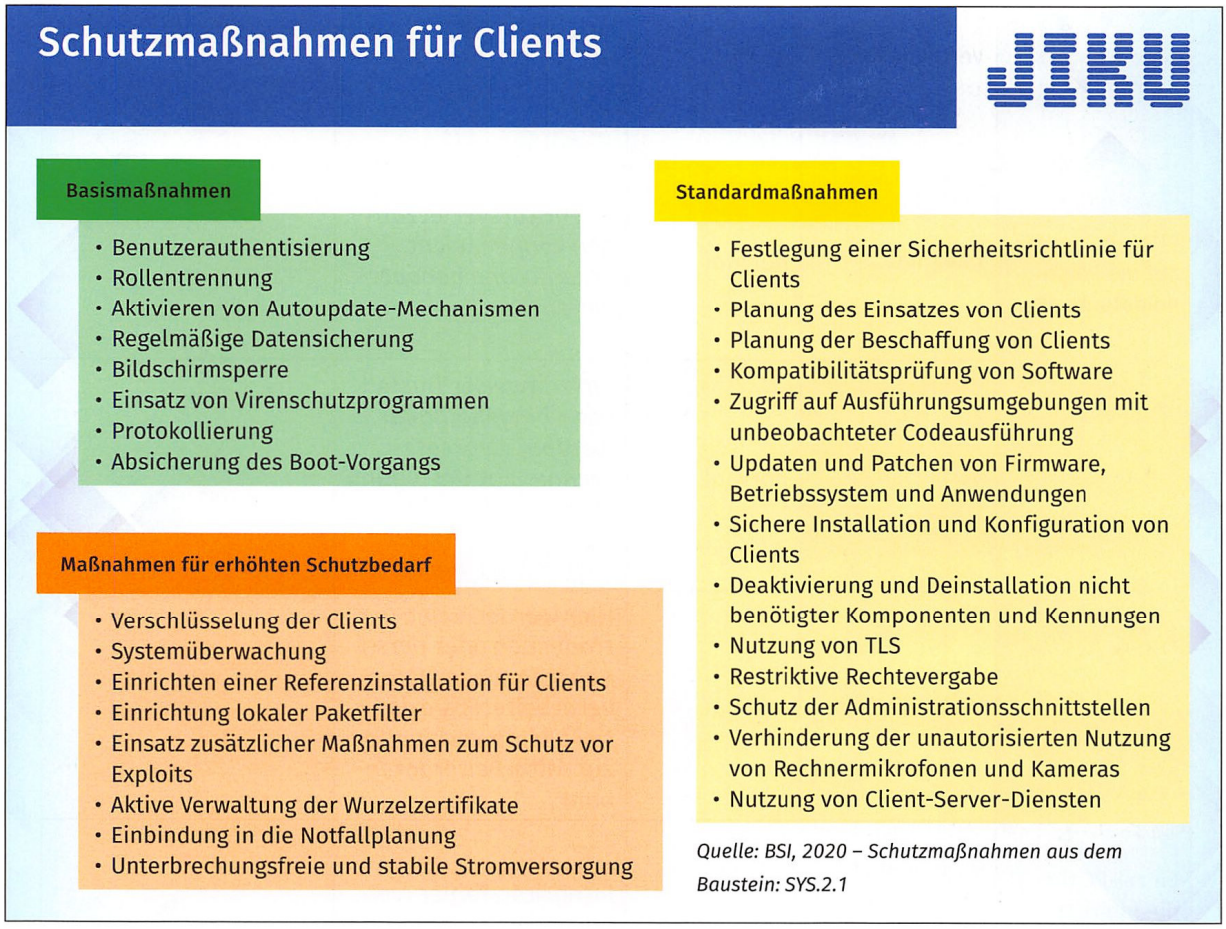
Client	Grundwert	Schutzbedarf	Begründung	Maßnahmen
PCs mit Zugriff auf die Personaldatenbank	Vertraulichkeit	hoch	Hierbei handelt es sich um personenbezogene Daten.	
	Integrität	normal	Integritätsverletzungen können leicht erkannt und behoben werden.	
	Verfügbarkeit	normal	Ein zeitweiser Ausfall kann hingenommen werden, da Ersatzrechner zur Verfügung stehen und die Personaldaten nicht lokal gespeichert werden.	
Einzel-PC für die Internetrecherche	Vertraulichkeit	normal	Hier werden keine vertraulichen oder personenbezogenen Daten verarbeitet. Es existiert keine Verbindung zur Mitarbeiterdatenbank.	
	Integrität	normal	Integritätsfehler werden leicht erkannt und behoben.	
	Verfügbarkeit	normal	Bei Ausfall steht übergangsweise ein Laptop zur Verfügung.	
...				

Unterschrift: P. Dager

(3) Schutzmaßnahmen

Basierend auf der Schutzbedarfsfeststellung und den Gefährdungen können nun entsprechende Schutzmaßnahmen angewandt werden. Eine der wichtigsten Sicherheitsmaßnahmen beim Betrieb heutiger Client-Systeme sind der Einsatz eines Virenscanners und eine regelmäßige Datensicherung.

Auf der nachfolgenden Folie sind einige wichtige Schutzmaßnahmen aufgeführt. Diese sind nur ein Auszug aus dem Baustein SYS.2.1 des IT-Grundschutz-Kompendiums des BSI, da dieser Baustein sehr umfangreich ist. Es werden dort weitere Schutzmaßnahmen aufgeführt und detailliert erläutert. Viele dieser erweiterten Inhalte werden späteren Modulen intensiver behandelt.



Viele der hier aufgeführten Maßnahmen, z.B. eine regelmäßige Datensicherung oder der Einsatz von Virenschutzprogrammen, sind selbsterklärend und werden deshalb nicht weiter erläutert. Weitere Basis- und Standardmaßnahmen sind in der anschließenden Auflistung mit einer kurzen Erläuterung versehen. Für den Rest und umfangreichere Erläuterungen wird auf das entsprechende Kapitel im BSI-Schutzkonzept verwiesen.

Einige grundlegende Schutzmaßnahmen für Clients näher betrachtet

Absicherung des Boot-Vorganges
Wenn beispielsweise von Wechselmedien gebootet wird, können Sicherheitsvorkehrungen umgangen und das System angegriffen werden. Außerdem muss verhindert werden, dass eventuelle Schadprogramme auf dem Client direkt in den Boot-Vorgang eingreifen.

Zugriff auf Ausführungsumgebungen mit unbeobachteter Codeausführung
Die Nutzung von Ausführungsumgebungen mit unbeobachteter Codeausführung, z. B. Intel Software Guard Extensions (SGX), sollte in der Firmware des Clients deaktiviert werden. Diese befinden sich meistens in den Sicherheitseinstellungen des BIOS.

Rollentrennung
Grundsätzlich kann zwischen den Rollen „Benutzer" und „Administrator" unterschieden werden. Administratoren müssen alle Rechte bekommen, um das IT-System verwalten zu können. Alle anderen Benutzer dürfen keine Administrationsrechte besitzen. Sie sollten nur so viele Rechte erhalten, damit sie ihre Aufgaben am Client ausführen können.

Protokollierung
Es sollten alle sicherheitsrelevanten Ereignisse, z. B. Versuche von unberechtigten Zugriffen, am Client protokolliert werden. Dazu ist die Protokollierung zu aktivieren und die Protokolle sind regelmäßig zu überprüfen.

Nutzung von TLS
Bei der Web-Nutzung sollte das Sicherheitsprotokoll SSL/TLS verwendet werden. Mit SSL/TLS können Verbindungen u.a. durch Verschlüsselung der Verbindungsinhalte, durch Überprüfung der Vollständigkeit und Korrektheit der übertragenen Daten oder durch Prüfung der Identität des Servers abgesichert werden.

Deaktivierung und Deinstallation von nicht benötigten Komponenten und Kennungen
Oft wird im Rahmen der Standardinstallation eines Betriebssystems eine größere Anzahl von Benutzerkennungen, Programmen, Diensten und sonstigen Komponenten eingerichtet, die für den Betrieb des Clients nicht notwendig sind. Es sollte deshalb geprüft werden, welche von diesen Komponenten wirklich benötigt werden. Der Rest ist zu deinstallieren oder zumindest zu deaktivieren.

Benutzerauthentisierung
Benutzer müssen eindeutig identifiziert und authentisiert werden können und die Interaktion zwischen dem Benutzer und dem IT-System darf nur bei erfolgreicher Authentisierung erfolgen. Zu den Authentisierungstechniken gehören u.a. PIN, Passwörter, Zugangskarten oder die Biometrie.

Nutzung von Client-Server-Diensten
Bei gleichberechtigten IT-Systemen kann jedes System Dienste anbieten oder nutzen. Damit werden die typischen Funktionen eines Servers und eines Clients auf einem IT-System vereint und es können sich mehrere IT-Systeme Ressourcen dezentral untereinander teilen, z.B. die Nutzung von einem Drucker, welcher lokal an einem IT-System angeschlossen ist.

LE 3 - Den Schutzbedarf bezüglich des Austausches von Daten mithilfe von mobilen Datenträgern feststellen

Sie sollen in unterschiedlichen Teams die Gefährdungen, den Schutzbedarf und entsprechende Schutzmaßnahmen bezüglich des Austausches von Daten mithilfe von mobilen Datenträgern ermitteln.

Mobile Datenträger finden vielfache Verwendung.

Sie werden vor allem für die Speicherung und den Transport von Daten eingesetzt. Je nach Art der Daten müssen verschiedene sicherheitstechnische Betrachtungen durchgeführt werden. Es wird aufgezeigt, wie die auf mobilen Datenträgern gespeicherten Daten sicher genutzt werden können, und andererseits, wie einer unbefugten Weitergabe von Daten über mobile Datenträger vorgebeugt werden kann. Dazu werden zunächst die Gefährdungslage und der Schutzbedarf analysiert und im Anschluss entsprechende Maßnahmen festgelegt.

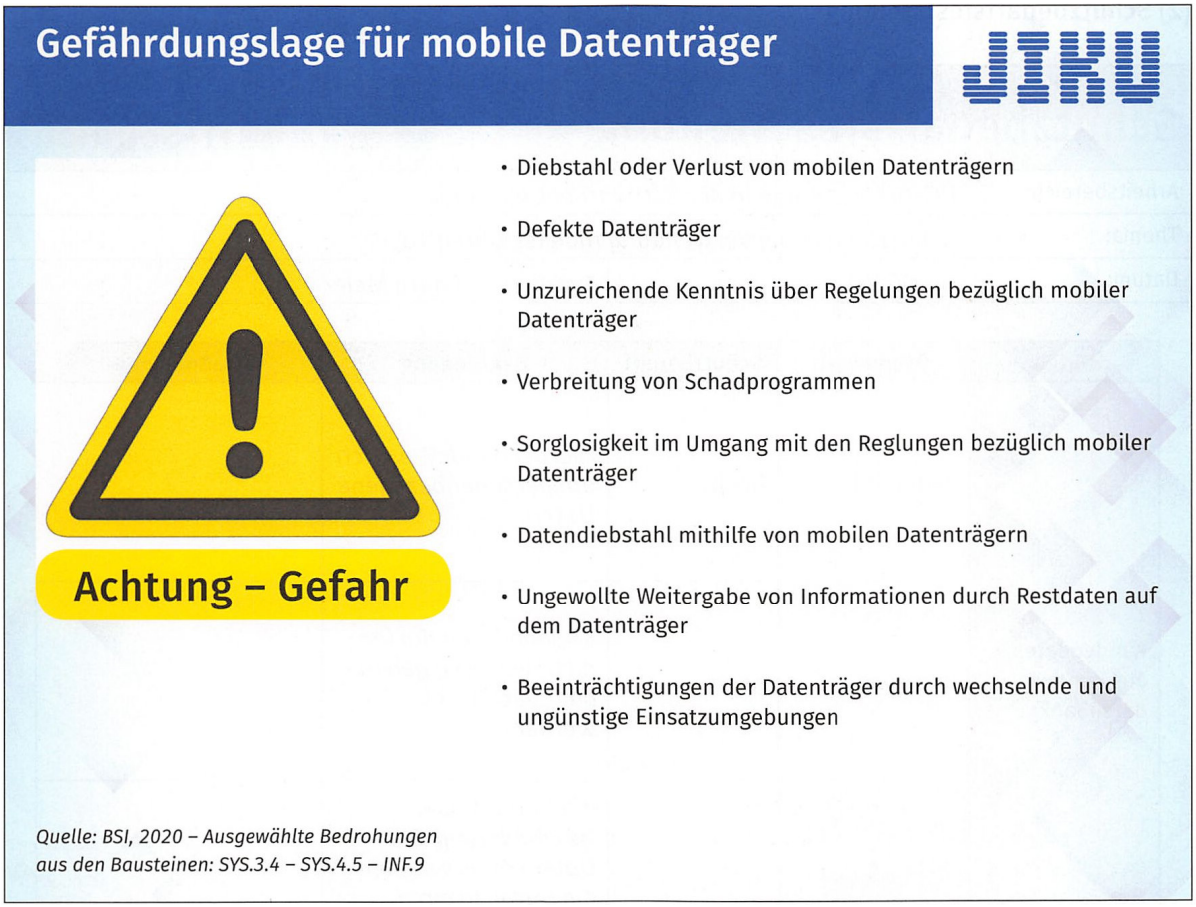


Mobile Datenträger	
Auswechselbare Datenträger (Wechseldatenträger)	Wechseldatenträger werden zum Datenaustausch in Laufwerke eingelegt. Beispiele hierfür sind CD-ROM, DVD, Blu-ray Disc, Magnetbänder und Speicherkarten.
Externe Datenträger	Externe Datenträger werden zum Datenaustausch direkt an das IT-Gerät angeschlossen. Beispiele hierfür sind USB-Sticks und externe Festplatten.
Datenträger, welche in mobile IT-Geräte integriert sind	Datenträger, welche in mobile IT-Geräte integriert sind, werden zum Datenaustausch indirekt über das mobile Gerät mit einem anderen IT-Gerät verbunden. Beispiele hierfür sind Speicherkomponenten in Smartphones, Tablets und Digitalkameras.

USB-Sticks stellen dabei heutzutage den weitaus größten Anteil an mobilen Datenträgern. Fast jeder hat einen in der Tasche, um auf die Schnelle Daten zu kopieren oder auszutauschen. Sie sind klein, in der Regel gut zu handhaben und relativ preiswert, sodass ein Verlust aus finanzieller Sicht nicht allzu schmerzhaft ist. Und in diesen positiven Eigenschaften liegen gleichzeitig die Gefahren im Umgang mit ihnen begründet.

(1) Gefährdungslage

In diesem Abschnitt werden kurz die Gefährdungen betrachtet, welche beim Austausch von Daten mittels mobiler Datenträger vorhanden sind. Auf der Folie sind die wesentlichen Gefährdungen aufgeführt. Grundlage dafür bieten die Bausteine SYS.3.4, SYS.4.5 und INF.9 des Grundschutzkompendiums des BSI.



Für die Gefahren für die IT-Sicherheit, welche vom Datenaustausch mittels mobiler Datenträger ausgehen, sind viele Unternehmen bereits sensibilisiert. Um diesen zu begegnen, wurden bereits eigene Regelungen dafür aufgestellt. Allerdings sind diese nicht immer allen Mitarbeitern bekannt oder es wird sehr sorglos mit ihnen umgegangen, was wiederum eine der Hauptgefahrenquellen darstellt, weil so die besten Maßnahmen ausgehebelt werden. Am Rechner vergessene oder auf Reisen verlorene USB-Sticks sind dafür nur ein Beispiel.

Aufgrund der Größe und ihres Materials sind viele mobile Datenträger zudem sehr anfällig für Beschädigungen und Ausfälle. Gründe dafür können u.a. wechselnde und ungünstige Einsatzumgebungen wie Staub, Dreck, Wasserdampf, hohe und niedrige Temperaturen sein. Aber auch leichte mechanische Einwirkungen können schon zu Beschädigungen führen. Auch beim Versand von mobilen Datenträgern ist daher mit Transportschäden oder sogar dem Verlust zu rechnen. Eine weitere große Gefahr besteht darin, dass mobile Datenträger oftmals recht sorglos an fremde IT-Systeme angeschlossen werden oder Fremde ihre mobilen Datenträger mit dem eigenen IT-Arbeitsplatz verbinden. Auf diese Weise kann man sich schnell Schadprogramme einfangen und diese auf das eigene System übertragen und so überall im Unternehmen verbreiten. Außerdem besteht immer die Gefahr, dass über mobile Datenträger größere Datenmengen unbefugt kopiert werden.

Festzuhalten ist: Je wichtiger und schutzbedürftiger die entsprechenden Daten sind, umso umfangreicher müssen auch die Schutzmaßnahmen sein. Um dieses festzustellen, wird zunächst wieder eine Schutzbedarfsfeststellung durchgeführt.

(2) Schutzbedarfsfeststellung

Schutzbedarfsfeststellung

JKU IT-Solutions

Arbeitsbereich:	*PC-Arbeitsplätze in der Softwareentwicklung*		
Thema:	*Schutzbedarf bei Verwendung mobiler Datenträger*		
Datum:	*04.06.20*	Ersteller:	*Laura Meier*

Daten	Grundwert	Schutzbedarf	Begründung	Maßnahmen
Kundendaten aus Kunden-datenbank	Vertraulichkeit	*hoch*	*Hierbei handelt es sich um personenbezogene Daten.*	
	Integrität	*hoch*	*Kundendaten dürfen nicht verloren gehen oder verfälscht werden.*	
	Verfügbarkeit	*normal*	*Bei Verlust oder Beschädigung des Datenträgers stehen die Daten in einer Datenbank weiterhin zur Verfügung.*	
Quellcode, Testergebnisse	Vertraulichkeit	*sehr hoch*	*Neben der Erstellung von Kundensoftware werden hier auch moderne und besondere Algorithmen entwickelt.*	
	Integrität	*sehr hoch*	*Der Quellcode und die Entwicklungspläne dürfen nicht verfälscht werden oder in dritte Hände gelangen.*	
	Verfügbarkeit	*normal*	*Die Daten werden zentral verwaltet und stehen jederzeit zur Verfügung.*	
...				

Unterschrift: *L. Meier*

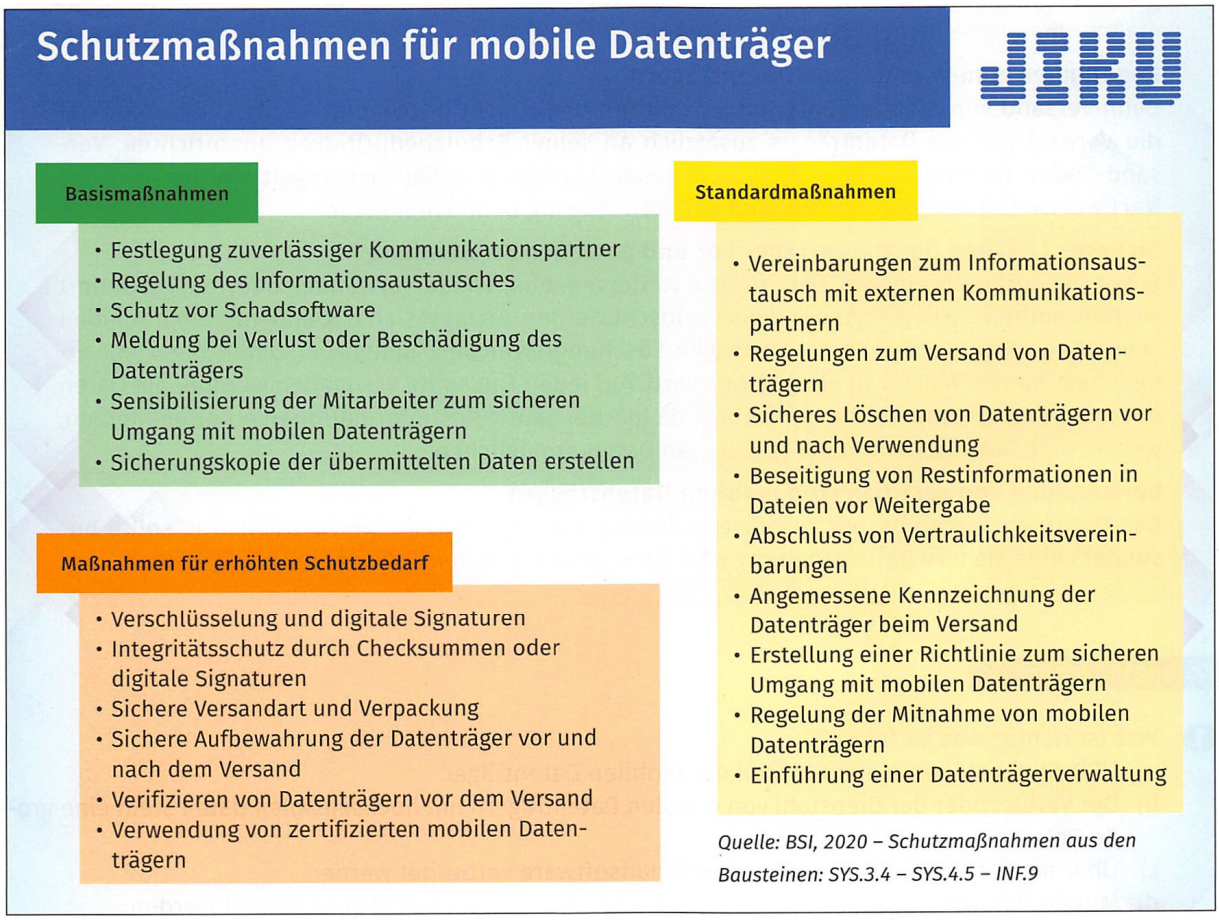
Bei der Schutzbedarfsfeststellung für den Datenaustausch mithilfe mobiler Datenträger ist vor allem zu klären, um welche Art von Daten es sich handelt. Daten von einem Arbeitsplatz, an dem keine vertraulichen oder sensiblen Daten verarbeitet werden, haben einen anderen Schutzbedarf als streng vertrauliche Daten. Eine Rolle spielt auch, in welcher Art und Weise das IT-System, über das der Austausch der Daten mit dem mobilen Datenträger erfolgen soll, in das Gesamtnetz eingebunden ist. Bei wichtigen IT-Systemen sollte ein möglicher Anschluss von mobilen Datenträgern völlig unterbunden werden. Ziel der Schutzbedarfsfeststellung ist es, auch hier den Prozess der Auswahl geeigneter Sicherheitsmaßnahmen zu unterstützen.

Nachfolgend ist ein Beispiel für eine Schutzbedarfsfeststellung für mobile Datenträger bei JIKU IT-Solutions aufgeführt. Dieses Protokoll baut wieder auf dem Beispiel des Modellunternehmens RECPLAST GmbH des BSI auf und wurde für eine Schutzbedarfsfeststellung eines Arbeitsbereiches entworfen.

(3) Schutzmaßnahmen

Ausgehend von den Ergebnissen der Schutzbedarfsfeststellung werden nun entsprechende Maßnahmen für den Umgang mit mobilen Datenträgern vorgeschlagen. Bevor auf spezielle Maßnahmen eingegangen wird, werden einige allgemeine Maßnahmen erwähnt. Zunächst sollte generell festgelegt werden, welche Arten von mobilen Datenträgern wofür eingesetzt werden. Des Weiteren sind alle Mitarbeiter für den sicheren Umgang mit mobilen Datenträgern zu sensibilisieren und Schnittstellen der IT-Systeme gemäß den Sicherheitsvorgaben zu schützen. Auch sollten die Daten, welche auf den mobilen Datenträger gespeichert werden, als Sicherungskopie vorliegen.

Nachfolgend sind die wichtigsten Basis- und Standardmaßnahmen sowie Maßnahmen für den erhöhten Schutzbedarf aufgeführt. Diese stellen eine Auswahl der in den Bausteinen SYS.3.4, SYS.4.5 und INF.9 aufgeführten Schutzmaßnahmen des Grundschutzkompendiums des BSI dar und können dort nochmals vertiefend nachgelesen werden.



Beim Datenaustausch mittels mobiler Datenträger ist eine Reihe von Maßnahmen zu beachten, wie die Auswahl in der Abbildung zeigt. Dazu gehört der Zugriffs- und Manipulationsschutz durch Verschlüsselung genauso wie eine sichere Aufbewahrung und Verpackung der Datenträger. Des Weiteren kann eine eindeutige Kennzeichnung die Verwechslungsgefahr verringern und die Daten sollten vor und nach dem Austausch auf Viren überprüft werden. Die meisten dieser Maßnahmen sind selbsterklärend oder wurden schon in einem anderen Abschnitt dieses Kapitels erläutert, z. B. die Verschlüsselung (siehe S. 45 und 46) Deswegen werden nachfolgend nur einige der aufgeführten Maßnahmen näher betrachtet.

Beschreibung ausgewählter Maßnahmen für den sicheren Datenaustausch mittels mobiler Datenträger

Festlegung zuverlässiger Kommunikationspartner
Sollen Daten an einen Kommunikationspartner innerhalb oder außerhalb der eigenen Institution übertragen werden, so muss sichergestellt werden, dass der Empfänger die notwendigen Berechtigungen zum Erhalt und zum Weiterverarbeiten dieser Informationen besitzt. Dazu muss die Identität des Kommunikationspartner vorher überprüft werden.

Verlustmeldung
Der Verlust eines mobilen Datenträgers muss umgehend gemeldet werden. Das gilt auch für private Datenträger, die dienstlich genutzt werden. Nun sollte schnell gehandelt werden, da es hier nicht nur darum geht, die Daten zu übermitteln, sondern auch darum, den potenziellen Missbrauch der betroffenen Informationen zu verhindern. Wenn verlorene Datenträger wieder auftauchen, müssen sie auf jeden Fall auf eventuelle Manipulationen untersucht werden.

Regelung der Mitnahme von mobilen Datenträgern
Mobile Datenträger werden oft außerhalb des Unternehmens eingesetzt. Deswegen muss die Mitnahme solcher Datenträger klar geregelt werden. Dabei sollte festgelegt werden, wer, unter welchen Umständen welchen mobilen Datenträger mitnehmen darf und welche Sicherheitsmaßnahmen dabei beachtet werden müssen.

Regelungen zum Versand von Datenträgern
Beim Versand von mobilen Datenträgern dürfen diese nicht beschädigt werden. Außerdem ist die Verpackung des Datenträgers zusätzlich an seiner Schutzbedürftigkeit auszurichten. Versand- oder Transportarten, z. B. Kuriertransport, müssen genauso geregelt werden wie das Nachweisverfahren über den Versand und den Eingang beim Empfänger.

Sicheres Löschen der Datenträger vor und nach der Verwendung
Bevor wiederbeschreibbare Datenträger weitergegeben, wiederverwendet oder ausgesondert werden, sollten sie in geeigneter weise gelöscht werden. So lässt sich z. B. eine für den normalen Schutzbedarf ausreichende physikalische Löschung erreichen, indem der Datenträger mit einem bestimmten Muster überschrieben wird. Auf jeden Fall sollte vermieden werden, die Daten nur mit einem Löschbefehl zu entfernen, da hierbei häufig Restinformationen erhalten bleiben, welche eine Rekonstruktion der gelöschten Daten ermöglichen.

Verwendung von zertifizierten mobilen Datenträgern
Das Unternehmen sollte nur zertifizierte Datenträger verwenden. Die Zertifizierung sollte besonders eine sichere Datenerhaltung und eine vorhandene Verschlüsselung einschließen.

Lernzielkontrolle TAG 7 und 8

1. Was ist richtig, was ist falsch?

a) Office-Produkte sind weitverbreitet.

b) Container beinhalten kein eigenes Betriebssystem.

c) In der Regel kann man bedenkenlos jede Datei mit einem entsprechenden Programm öffnen.

d) Betaversionen von Software sollten so schnell wie möglich installiert und genutzt werden, weil diese die neuesten Sicherheitsstandards besitzen.

e) Zur Installation von Software sollten Originaldatenträger verwendet werden.

f) In der Regel reicht einfach das Löschen des kompletten Verzeichnisses, in dem die Software ins-

g) talliert ist, um diese sicher vom PC zu entfernen.

h) Wenn möglich sollte immer die gleiche Version eines Office-Produktes mit derselben Konfigura-

i) tion auf allen Rechnern im Unternehmen installiert sein.

j) Die Programmierung und Nutzung von Makros in Office-Produkten sollten einheitlichen Regeln

k) unterworfen sein.

l) Während des produktiven Einsatzes sollte die Software des Containers nicht verändert werden.

2. Was ist richtig, was ist falsch?

a) IT-Systeme besitzen mindestens den gleichen Schutzbedarf wie die darauf gespeicherten Daten.

b) Über vernetzte Clients können sich Schadprogramme schnell auf andere Systeme übertragen.

c) Es sollte Regelungen geben, ob und inwieweit mobile Datenträger mit einzelnen Clients verbunden werden dürfen.

d) In den Clients verbaute Kameras könnten zur Spionage genutzt werden.

e) In der Regel reicht eine Standardinstallation vom Betriebssystem auf dem Client aus.

f) Das Booten sollte immer auch von mobilen Datenträgern aus möglich sein, um so im Notfall schnell agieren zu können.

g) Viren-Schutzprogramme sollten zur Grundausstattung eines Clients gehören.

h) In der Regel findet bei der Schutzbedarfsfeststellung für Clients das Minimumprinzip Anwendung.

i) Der Schutzbedarf ist für alle Clients in einem Arbeitsbereich gleich.

3. Was ist richtig, was ist falsch?

a) USB-Sticks stellen einen Großteil der mobilen Datenträger.

b) Der Verlust oder der Diebstahl von mobilen Datenträgern mit hochsensiblen Daten stellt eine große Gefahr für das Unternehmen dar.

c) Über mobile Datenträger kann keine Schadsoftware verbreitet werden.

d) Mobile Datenträger sollten zum Datenaustausch ausreichend gekennzeichnet werden.

e) Der Versand von vertraulichen Daten sollte per Kurierdienst in einer gesicherten Verpackung erfolgen.

f) In der Regel reicht einfaches Löschen der Daten vom Datenträger, um diesen für den nächsten Gebrauch vorzubereiten.

g) Der Gebrauch von privaten mobilen Datenträgern zu dienstlichen Zwecken ist in jedem Fall zu gestatten.

h) Verschlüsselung ist eine Maßnahme, um die Daten auf mobilen Datenträgern zu schützen.

i) Es sollte immer eine Sicherheitskopie von den Daten, welche ausgetauscht werden sollen, existieren.

TAG 9 – Lernsituationen und Aufgaben bearbeiten

Aufgaben siehe Handout

TAG 10 - Vertiefung des Wissens und Modulprüfung

Einleitung

Der letzte Tag in diesem Modul bietet Ihnen die Möglichkeit der Wiederholung und Vertiefung Ihres Wissens. Sollten es noch offene, nicht vollständig bearbeitete Modul-Inhalte geben, nutzen Sie den heutigen Tag zur Komplettierung.

LE 2 - Modulprüfung

120 Minuten zu denen wir Ihnen recht viel Erfolg wünschen!

Lösungen:

TAG 1

1. a) IT-SiG
   b) DSGV, BDSG
   c) Urhebergesetz

2. Richtig: b, f, g

3. a)
   1. Artikel 15
   2. Artikel 17
   3. Artikel 17
   4. Artikel 18
   5. Artikel 15
   6. Artikel 19
   7. Artikel 16
   8. Artikel 20
   9. Artikel 16
   10. Artikel 15
   11. Artikel 13
   12. Artikel 14
   13. Artikel 13
   14. Artikel 12
   15. Artikel 13
   16. Artikel 12
   17. Artikel 19
   18. Artikel 12

   b) Die DSGVO gilt europaweit bei der Verarbeitung personenbezogener Daten, das BDSG bundesweit neben den LDSG, die DSGVO hat daher Vorrang, BDSG und LDSG sind zusammen mit DSGVO anwendbar. Die Regelungen im BDSG und LDSG werden an die EU-DSGVO angepasst.

4. Individuelle Lösung

5.
   1.
   a) Richtig
   b) Falsch
   c) Falsch
   d) Richtig
   e) Falsch
   f) Falsch
   g) Richtig
   h) Richtig
   i) Falsch
   j) Falsch
   k) Falsch
   l) Falsch

   2.
   a) Richtig
   b) Falsch
   c) Richtig
   d) Falsch

   3.
   a) Falsch
   b) Falsch
   c) Richtig
   d) Richtig
   e) Falsch
   f) Falsch
   g) Falsch
   h) Falsch
   i) Richtig

   4.
   a) Falsch
   b) Falsch
   c) Richtig
   d) Richtig
   e) Richtig

TAG 5

1. Individuelle Lösung; mithilfe der gerade behandelten Kapitel im Schülerbuch und eigener Recherchen

2. a) richtig
   b) falsch
   c) falsch
   d) richtig
   e) richtig
   f) richtig

3. a) V = Verfügbarkeit oder A = Availability und I = Integrität oder I = Integrity und V = Vertraulichkeit oder C = Confidendiality
   b) BSI
   c) Forensik
   d) Kreuztabelle
   e) Zugangskontrolle, Datenträgerkontrolle, Speicherkontrolle, Benutzerkontrolle, Zugriffskontrolle, Übertragungskontrolle, Eingabekontrolle, Transportkontrolle, Wiederherstellbarkeit, Zuverlässigkeit, Datenintegrität, Auftragskontrolle, Verfügbarkeitskontrolle, Trennbarkeit
   f) PDCA
   g) Bedrohungen

4. a) SYS
   b) APPS
   c) NET
   d) ISMS
   e) INF
   f) IND
   g) ORP
   h) DER
   i) OPS
   j) CON

5.

Schutzzielen nach BSI/DSGVO Art. 32		
Gefährdungen, die Schutzziele betreffen	Auswirkungen bei Verlust von Schutzzielen	Maßnahmen gegen Verlust der Schutzzielen
Verlust der Verfügbarkeit von Informationen personenbezogener Daten und Zielobjekten		
• Brand-/Wasserschaden • Stromausfall • Cyberangriffe (DDoS) • Fehlbedienung/ -handlung • Manipulation • Sabotage, Einbruch • Diebstahl	• Kunden können ihre Konten nicht aufrufen • keine Einkäufe tätigen • ihre Arbeit nicht mehr mit der IT verrichten • ihre E-Mails nicht aufrufen • wirtschaftlicher Schaden • Imageschaden etc.	• Stromausfall durch USV beheben • sofort Rücksicherung durchführen und System wieder hochfahren • System erneut starten • Kunden sofort transparent informieren • mobiles Rechenzentrum bestellen oder auf Cloud-System Parallelsystem installieren

Schutzzielen nach BSI/DSGVO Art. 32		
Verlust der Vertraulichkeit von Informationen personenbezogener Daten auf IT-Systemen		
• Cyberangriffe • Datendiebstahl durch Mitarbeiter • Social Engineering • Datenträgerdiebstahl • Datendiebstahl	• Datendiebstahl und Missbrauch • Weiterverkauf der Daten • Erpressung, Nötigung • Manipulation • Betrug • wirtschaftlicher Schaden • Imageschaden	• Passwortschutz verbessern • Multifaktorauthentifizierung • Sicherheitszonen • Sicherheitsregeln • Sicherheitsmanagement • Sicherheitsschulungen • Antivirensoftware und Firewall optimieren • Ständiges Sicherheitsmonitoring • Verschlüsselung der Daten wo möglich und notwendig • Datenschutz bei Entsorgung
Verlust der Integrität (Korrektheit von Informationen)		
• Verfälschung von Daten durch Programmfehler • Mitarbeiterfehler • Fehlbuchungen • Redundanz (Doppelspeicherungen) von Daten und damit verbundene Datenanomalien (z. B. Benutzer mehrfach erfasst) • kriminelle Verfälschung der Identitäten • Cyberangriffe	• hoher wirtschaftlicher Schaden durch schlechte Kundenbetreuung/Kundenbeschwerden, Überprüfungsverfahren • falsche Handlungen/Aktionen durch falsche Daten • Schäden bei Kunden durch falsch oder nicht ausgeführte Kundenaufträge, Regressansprüche, Imageschaden	• Prüfroutinen bei der Erfassung von Daten • intelligente Überprüfung von Daten auf Plausibilität • Revisionsteams

6. a) bis f) Individuelle Lösungen

TAG 3

1. a) Scareware
   b) Phishing
   c) Trojaner
   d) Wurm
   e) Skimming
   f) PUA
   g) Ramsomware
   h) Virus
   i) Hoax
   j) APT
   k) Botnetz

TAG 4

1. a) CEO Fraud
   b) Man-in-the-Middle-Angriffe/Angler-Phishing
   c) Zweifaktor-Authentifizierung
   d) Blacklist
   e) Doxing
   f) Combosquatting
   g) Jailbreak und Rooting
   h) Keylogging
   i) PGP

2. 1. Richtig
   2. Falsch
   3. Richtig
   4. Richtig
   5. Richtig
   6. Falsch
   7. Falsch
   8. Richtig
   9. Richtig
   10. Richtig
   11. Richtig
   12. Falsch
   13. Richtig
   14. Falsch
   15. Richtig
   16. Richtig
   17. Falsch
   18. Richtig
   19. Falsch
   20. Richtig
   21. Falsch
   22. Falsch
   23. Richtig

3. 1. Richtig
   2. Falsch
   3. Richtig
   4. Richtig
   5. Falsch
   6. Falsch
   7. Richtig
   8. Falsch
   9. Richtig
   10. Richtig
   11. Falsch
   12. Richtig

4. 1. (D)
   2. (A)
   3. (E)
   4. (B)
   5. (C)

TAG 5

1. Individuelle Lösung

2. Individuelle Lösung
3. Individuelle Lösung
4. a) bis c) Individuelle Lösung

TAG 6

6. a) Symmetrische Verschlüsselung
   b) Asymmetrische Verschlüsselung
   c) Hybride Verschlüsselung

TAG 7 und 8

1. a) richtig
   b) richtig
   c) falsch
   d) falsch
   e) richtig
   f) falsch
   g) richtig
   h) richtig
   i) richtig

2. a) richtig
   b) richtig
   c) richtig
   d) richtig
   e) falsch
   f) falsch
   g) richtig
   h) falsch
   i) falsch

3. a) richtig
   b) richtig
   c) falsch
   d) richtig
   e) richtig
   f) falsch
   g) falsch
   h) richtig
   i) richtig

TAG 9

Aufgabe 1

1. Richtig: b, c
2. Richtig: a, c
3. Richtig: a, c
4. Richtig: b
5. Richtig: a, b, c
6. Richtig: c, d

Aufgabe 2

Individuelle Lösung

1. Windows ist aufgrund seiner Installationsbasis am wenigsten sicher

Windows ist das am meisten anvisierte Betriebssystem, da es aufgrund der Größe der Installationsbasis am effizientesten angegriffen werden kann. Wenn Sie Malware schreiben, die auf 88 % der Computer ausgeführt werden kann, haben Sie höchstwahrscheinlich den größten Erfolg.

Dies bedeutet jedoch nicht, dass Windows weniger sicher ist als andere Betriebssysteme. Man könnte auch sagen, dass die Popularität von Windows bedeutet, dass Microsoft die meiste Erfahrung im Schutz vor Malware-Angriffen hat. Der eigentliche Punkt ist, dass es mehr Malware gibt, die auf Windows abzielt, und das bedeutet, dass Sie eine gute Sicherheitslösung benötigen. Es sollte jedoch immer eine gute Sicherheitslösung verwendet werden, unabhängig davon, welches Betriebssystem Sie verwenden und wie viel Malware dafür vorhanden ist.

2. Linux ist am sichersten, da es Open Source ist

Viele Leute sagen das die ganze Zeit. Die Sicherheitstheorie, dass ein Quellcode, wenn viele Leute ihn betrachten, automatisch sicherer ist, ist offensichtlich fehlerhaft. Die SentinelOne-Forscherin Dor Dankner hat kürzlich bekannt gegeben, dass Linux eine unerkannte Sicherheitsanfälligkeit bezüglich der Eskalation von Berechtigungen aufweist. Dieses wurde 2004 im Linux-Kernel eingefügt. Obwohl der Code überprüft wurde, wurde nichts unternommen, um ihn zu verbessern. Ebenso enthielt openssl den Heartbleed-Bug über zwei Jahre lang, bevor er schließlich entdeckt wurde.

3. macOS ist am sichersten, weil „Apple“
Apple hat es geschafft, sich in der Öffentlichkeit als „sicherheitsbewusst“ zu positionieren, wegen der geschlossenen Natur der mobilen Plattform und iOS. In Apples Marketing ist viel Sicherheit „eingebaut“, aber die Wahrheit ist, dass Mac-Sicherheitsfunktionen wie Gatekeeper, XProtect und MRT einfach durchzuführen und nicht besonders umfassend sind. Man könnte auch argumentieren, dass Apple weniger Erfahrung in der Abwehr von Malware hat und in der Kunst des Erstellens eines gehärteten Betriebssystems nicht so gut ist wie Microsoft.
4. Linux ist am sichersten, da es hochgradig konfigurierbar ist
Es ist wahr, dass so etwas wie SELinux wahrscheinlich mehr Möglichkeiten hat, das System zu „härten“ als macOS oder Windows. Aber nur sehr wenige Unternehmen werden eine gesperrte SELinux-Installation als Desktop-Betriebssystem verwenden, zumindest nicht, wenn Mitarbeiter nützliche Arbeit leisten sollen. Sicherheit und Benutzerfreundlichkeit gehen Hand in Hand, und Benutzer treffen häufig weniger sichere Entscheidungen, wenn sie gegen das Betriebssystem kämpfen, nur um ihre Arbeit zu erledigen.

Aufgabe 3
1. Individuelle Lösung, z. B.
• Unzureichender Passwortschutz
• Fehlende oder unzureichende Konfiguration
• Fehlerhafte und ungenügende Rechtevergabe
• Ausführen von Schadsoftware
• Datenverlust durch fehlerhafte Nutzung
• Nutzung von Daten aus nicht vertrauenswürdigen Quellen
• Unbekannte Schwachstellen in der Software
• Unzureichende Schulung von Mitarbeitern im Umgang mit der Software unter Sicherheitsaspekten

2.

Grundwert	Schutzbedarf	Begründung	Maßnahmen
Vertraulichkeit	hoch	Hier werden personenbezogen Daten verwaltet. Daneben werden auch sehr vertrauliche Reisedaten verarbeitet.	• Software nur von Originaldatenträger installieren • Benutzerauthentisierung • Rollentrennung • Bildschirmsperre • keine Daten lokal speichern
Integrität	hoch	Die Daten dürfen nicht verloren gehen oder gefälscht werden.	• Aktivieren von Autoupdate-Mechanismen • Benutzerauthentisierung • Rollentrennung • keine Daten lokal speichern
Verfügbarkeit	normal	Bei Verlust der lokalen Daten oder Ausfall der Software stehen die Daten in einer Datenbank weiterhin zur Verfügung. Außerdem ist die Software auf mehreren Rechnern installiert. Eine 24/7 Verfügbarkeit der Daten ist nicht erforderlich.	• Sichere Installation und Konfiguration • Eventuell zusätzlich einen Laptop als Notfallgerät mit dieser Software ausstatten • Original-Installations-CD sicher aufbewahren und Installation und Konfiguration dokumentieren

3. Individuelle Lösung

Aufgabe 4
1. (D), (C)
2. (B)
3. (A)
4. (B), (A)
5. (D)

Aufgabe 5

1. Individuelle Lösung, z. B.
• Schadprogramme
• Datenverlust durch lokale Datenhaltung
• Datenverlust durch Hardwaredefekte
• Softwareschwachstellen oder Fehler
• Unberechtigte Benutzung
• Installation nicht benötigter Betriebssystemkomponenten und Applikationen
• Fehlerhafte Administration oder Nutzung von Geräten und Systemen

2. Individuelle Lösung, z. B.

Grundwert	Schutzbedarf	Begründung	Maßnahmen
Vertraulichkeit	hoch	Hier werden personenbezogen Daten verwaltet. Daneben werden auch vertrauliche Vertriebsdaten verarbeitet.	• Benutzerauthentisierung • Rollentrennung • Bildschirmsperre • Sichere Installation und Konfiguration von Clients • Restriktive Rechtevergabe • Schutz der Administrationsschnittstellen • Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Kameras • Verschlüsselung der Clients
Integrität	hoch	Die Daten dürfen nicht verloren gehen, in falsche Hände gelangen oder gefälscht werden.	• Benutzerauthentisierung • Rollentrennung • Verschlüsselung lokaler Daten • Verschlüsselung der Clients • automatisierter Datenabgleich mit der Datenbank, wenn Verbindung besteht
Verfügbarkeit	hoch	Beim Gespräch mit den Kunden müssen die wichtigsten Daten und die Präsentationssoftware zur Verfügung stehen.	• Einsatz robuster Hardware • mehrere Ersatzlaptops bereitstellen • zentrale Verwaltung der Laptops • Wartung der Laptops vor und nach jedem Einsatz

3. Individuelle Lösung

Aufgabe 6

1.

Art	Beispiele
Auswechselbare Datenträger	DVD, Speicherkarten
Externe Datenträger	USB-Stick, externe Festplatten
Datenträger, welche in mobile IT-Geräte integriert sind	Speicherkomponenten in Smartphone oder Digitalkameras

2. Individuelle Lösung, z. B.

Bedrohung	Schutzmaßnahme
Sorglosigkeit im Umgang mit den Reglungen bezüglich mobiler Datenträger	Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern
Ungewollte Weitergabe von Informationen durch Restdaten auf dem Datenträger	Sicheres Löschen von Datenträgern vor und nach Verwendung
Diebstahl oder Verlust von mobilen Datenträgern	Verschlüsselung und digitale Signaturen

3. Individuelle Lösung, z. B.

Schutzmaßnahme	Beschreibung
Sicheres Löschen der Datenträger vor und nach der Verwendung	Bevor wiederbeschreibbare Datenträger weitergegeben, wiederverwendet oder ausgesondert werden, sollten sie in geeigneter Weise gelöscht werden. So lässt sich z. B. eine für den normalen Schutzbedarf ausreichende physikalische Löschung erreichen, indem der Datenträger mit einem bestimmten Muster überschrieben wird. Auf jeden Fall sollte vermieden werden, die Daten nur mit einem Löschbefehl zu entfernen, da hierbei häufig Restinformationen erhalten bleiben, welche eine Rekonstruktion der gelöschten Daten ermöglichen.
Verlustmeldung	Der Verlust eines mobilen Datenträgers muss umgehend gemeldet werden. Das gilt auch für private Datenträger, die dienstlich genutzt werden. Nun sollte schnell gehandelt werden, da es hier nicht nur darum geht, die Daten zu übermitteln, sondern auch darum, den potenziellen Missbrauch der betroffenen Informationen zu verhindern. Wenn verlorene Datenträger wiederauftauchen, müssen sie auf jeden Fall auf eventuelle Manipulationen untersucht werden.
Einführung einer Datenträgerverwaltung	Mithilfe einer zentralen Datenträgerverwaltung kann sichergestellt werden, dass alle notwendigen Sicherungsmaßnahmen für die Datenträger vorgenommen und diese regelmäßig überprüft werden. Es können Datenträger für verschiedene Einsatzgebiete speziell vorbereitet werden und der Verlust wird schneller bemerkt.

4. Der Datenaustausch ist heutzutage ein wichtiger Bestandteil des Alltags geworden. In vielen Fällen werden hierfür noch USB-Sticks verwendet. Leider bergen USB-Sticks trotz regelmäßiger Sensibilisierungskampagnen mit den wichtigsten Verhaltensregeln immer noch ein erhöhtes Infektionsrisiko für Computer. Der neueste Honeywell-Bericht zeichnet für jeden Cybersicherheitsexperten ein erschreckendes Bild: 40 % der USB-Sticks enthalten mindestens einen potenziell gefährlichen Ordner, und 26 % dieser Risiken können zu Fehlfunktionen des Betriebssystems führen. Aus diesem Grund ist in vielen Unternehmen wie IBM die Verwendung von USB einfach verboten.

Aufgabe 7

1. Individuelle Lösung, z. B.

- Diebstahl oder Verlust von mobilen Datenträgern
- Defekte Datenträger
- Unzureichende Kenntnis über Regelungen bezüglich mobiler Datenträger
- Verbreitung von Schadprogrammen
- Sorglosigkeit im Umgang mit den Reglungen bezüglich mobiler Datenträger
- Datendiebstahl mithilfe von mobilen Datenträgern
- Ungewollte Weitergabe von Informationen durch Restdaten auf dem Datenträger
- Beeinträchtigungen der Datenträger durch wechselnde und ungünstige Einsatzumgebungen

2. Individuelle Lösung, z. B.

Grundwert	Schutzbedarf	Begründung	Maßnahmen
Vertraulichkeit	hoch	Hier werden personenbezogen Daten von Mandanten verwaltet.	• Erstellung einer Richtlinie zum sicheren Umgang mit mobilen Datenträgern • Regelung der Mitnahme von mobilen Datenträgern • Einführung einer Datenträgerverwaltung • Verschlüsselung und digitale Signaturen • Abschluss von Vertraulichkeitsvereinbarungen • Meldung bei Verlust oder Beschädigung des Datenträgers • Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern
Integrität	hoch	Die Daten dürfen nicht verloren gehen, in falsche Hände gelangen oder gefälscht werden.	• Erstellung einer Richtlinie zum sicheren Umgang mit mobilen Datenträgern • Regelung der Mitnahme von mobilen Datenträgern • Einführung einer Datenträgerverwaltung • Verschlüsselung und digitale Signaturen • Abschluss • Sicheres Löschen von Datenträgern vor und nach Verwendung • Beseitigung von Restinformationen in Dateien vor Weitergabe • Meldung bei Verlust oder Beschädigung des Datenträgers • Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern
Verfügbarkeit	normal	Die Daten stehen sowohl in der Datenbank bzw. bei den Kunden weiterhin zur Verfügung und können bei Bedarf neu ermittelt werden.	• Erstellung einer Richtlinie zum sicheren Umgang mit mobilen Datenträgern • Regelung der Mitnahme von mobilen Datenträgern • Einführung einer Datenträgerverwaltung • Meldung bei Verlust oder Beschädigung des Datenträgers • Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern • Sicherungskopie der übermittelten Daten erstellen

3. Individuelle Lösung