



Themengebiet 4: Schutzbedarfsanalyse im eigenen Arbeitsbereich durchführen

IT-Security umfasst die Sicherheit der ganzen IT

IT-Sicherheit reicht vom Schutz einzelner Dateien bis hin zur Absicherung von Rechenzentren und Cloud-Diensten. IT-Security gehört zu jeder Planung und Maßnahme in der IT und ist grundlegend für die Compliance im Unternehmen.

Unter IT-Sicherheit versteht man alle Planungen, Maßnahmen und Kontrollen, die dem Schutz der IT dienen. Der Schutz der IT hat drei klassische Ziele: Die Vertraulichkeit der Informationen, die Integrität der Informationen und Systeme und die Verfügbarkeit der Informationen und Systeme. Der Schutz der IT-Systeme vor Ausfall und die notwendige Belastbarkeit der IT-Systeme ist grundlegend für die Aufrechterhaltung des Geschäftsbetriebs [...].

Im Gegensatz zur Datensicherheit geht es in der IT-Sicherheit nicht nur um personenbezogene Daten, für die der rechtlich geforderte Datenschutz Sicherheitsmaßnahmen verlangt. Es geht vielmehr um alle Arten von Informationen, die es zu schützen gilt. [...]

IT-Security bedeutet Schutz von Informationen und IT-Systemen

Sicherheit denken, da viele Anwendungen und IT-Ressourcen inzwischen als Cloud-Dienst bezogen werden. Mit der Verbindung ins Internet kommen neue Risiken und Gefahren ins Spiel, die bei der Planung und Umsetzung der IT-Sicherheit stark ins Gewicht fallen müssen: die Cyber-Bedrohungen, darunter die Hackerangriffe auf IT-Systeme und Informationen über das Internet.

IT-Sicherheit schützt die Vernetzung bis ins Internet

Die Endgeräte arbeiten heute kaum noch alleine, vielmehr sind die Geräte und Anwendungen in der Regel über Netzwerke miteinander verknüpft. Die Vernetzung kann dabei über das firmeninterne Netzwerk hinausgehen und Verbindungen über das Internet einschließen.

Wenn man die Sicherheit der Vernetzung, die Netzwerksicherheit gewährleisten will, muss man deshalb auch an Internetsicherheit und an Cloud-Sicherheit denken, da viele Anwendungen und IT-Ressourcen inzwischen als Cloud-Dienst bezogen werden.

Mit der Verbindung ins Internet kommen neue Risiken und Gefahren ins Spiel, die bei der Planung und Umsetzung der IT-Sicherheit stark ins Gewicht fallen müssen: die Cyber-Bedrohungen, darunter die Hackerangriffe auf IT-Systeme und Informationen über das Internet.

IT-Security schützt auch den Nutzer

Der Anwender selbst steht ebenfalls im Fokus der IT-Sicherheit. Informationen und IT-Systeme lassen sich nur dann schützen, wenn sichergestellt ist, dass nur legitimierte Nutzer die Informationen und Systeme verwenden und dass die legitimen Anwender nur die für sie freigegebenen Systeme und Informationen nutzen. [...]

IT-Sicherheit muss Schwachstellen verhindern und Compliance gewährleisten

Die IT-Sicherheit ist immer dann bedroht, wenn es eine Schwachstelle gibt, die ein Angreifer ausnutzt oder die zu Fehlern in der IT führt. Mit dem Schwachstellen-Management sollen deshalb Schwachstellen oder Sicherheitslücken aufgespürt und geschlossen werden.

Die gefährlichste Schwachstelle in der IT ist eine lückenhafte IT-Security. Die häufig zu hörende Aussage, dass es keine hundertprozentige Sicherheit gebe, gilt auch in der IT. Trotzdem muss die IT-Sicherheit dem Risiko und Schutzbedarf für Informationen und Systeme entsprechend so umfassend wie möglich ausgelegt sein. [...]

Quelle: <https://www.security-insider.de/it-security-umfasst-die-sicherheit-der-ganzen-it-a-578480/?print>

Arbeitsauftrag

Überlegen Sie, wie und wo IT-Sicherheit in Ihrem Ausbildungsbetrieb umgesetzt wird, und halten Sie Stichwörter hierzu schriftlich fest.

4.1 Zuständigkeiten, Verantwortung und Stellen der Informationssicherheit

Das Thema der IT-Sicherheit ist ein komplexes und vielschichtiges Thema. Dies liegt vor allem daran, dass so viele Bereiche im Betrieb betroffen sind. Dabei verliert man schnell den Überblick und weiß nicht so recht, wo wer für was zuständig ist. Wissen Sie, wen Sie bei bestimmten Fragen zur Informationssicherheit fragen?

Arbeitsauftrag

- a) Diskutieren Sie mit Ihrem Sitznachbarn, wer im Unternehmen für Fragen zur Informationssicherheit verantwortlich ist.
- b) Skizzieren Sie auf Basis Ihrer Erkenntnisse aus der Diskussion eine mögliche Organisationsstruktur.

Geschäftsführung
(obere Führungsebene)

Informatikos-
sicherheits-
beauftragte

Mitarbeiter,
Angestellte,
User

IT-Abteilung,
Admins

- c) Die jeweiligen Verantwortlichen werden nicht allein gelassen. Es gibt mehrere Informationsquellen, bei denen sich Verantwortliche über Informationssicherheit informieren können. Recherchieren Sie im Internet und geben Sie eine Auswahl an möglichen seriösen Informationsquellen.

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
"Cybersicherheits-Behörde" des Bundes
<http://www.bsi.bund.de>
- CERT (Europa)
<https://cert.europa.eu>
- Informationen über schwachstellen und Bugs
CVE: <http://nvd.nist.gov>

4.2 Gesetze und Standards bei der Informationssicherheit

Selbstverständlich ist die Informationssicherheit auch gewissen Gesetzen und Standards unterworfen, welche Rechtssicherheit für alle beteiligten gewährleisten sollen, sowie einheitliche und verbindliche Standards schaffen. Grundsätzliche können 3 Bereiche benannt werden:

- (1) IT-Sicherheit (auch IT-Security),
- (2) Datenschutz und
- (3) Urheberrecht, Copyright, Markenrecht und Lizenzrecht

Arbeitsauftrag

Finden Sie für jeden Bereich durch Recherche entsprechende Gesetze und Standards. Kennzeichnen Sie jeweils, ob es sich um Gesetze (G) oder Standards (S) handelt.

IT-Sicherheit	Datenschutz	Urheberrechte, Copyright, Markenrecht und Lizenzrecht
IT-Sicherheits- gesetz (G) (IT_SIG)	DSGVO (G) BDSG (G)	Patentgesetz (PatG) Markengesetz (MarkenG)
BSI-Gesetz(G) (BSIG)		Urheberrechtsgesetz (UrhG)
IT-Grundschutz kompendium(S)		

4.3 IT-Grundschutz: Schutzziele, Gefährdungen und Schadensszenarien

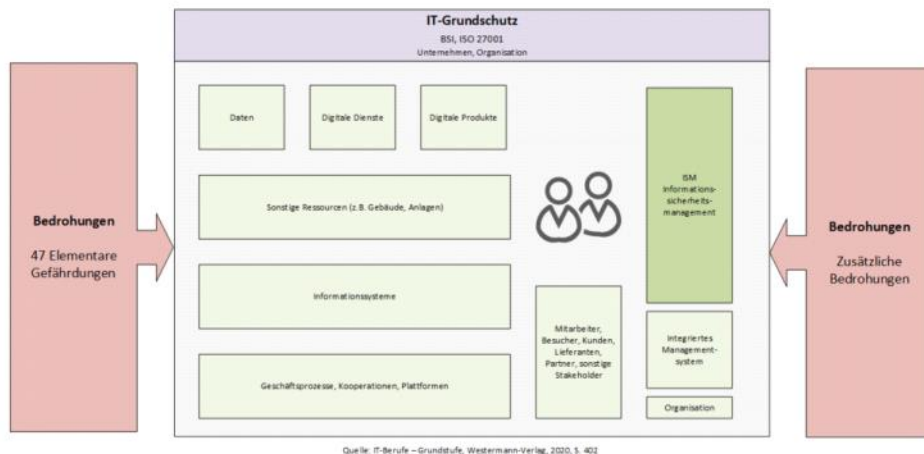
4.3.1 IT-Grundschutz nach dem BSI

Mit dem IT-Grundschutz des BSI soll in Behörden und Unternehmen jeder Größenordnung das Niveau der Informationssicherheit erhöht werden.

Definition

„INFORMATIONSSICHERHEIT HAT DAS ZIEL, INFORMATIONEN JEDLICHER ART UND HERKUNFT ZU SCHÜTZEN. DABEI KÖNNEN INFORMATIONEN AUF PAPIER, IN IT-SYSTEMEN ODER AUCH IN DEN KÖPFEN DER BENUTZER GESPEICHERT SEIN. IT-SICHERHEIT ALS TEILMENGE DER INFORMATIONSSICHERHEIT KONZENTRIERT SICH AUF DEN SCHUTZ ELEKTRONISCH GESPEICHERTER INFORMATIONEN UND DEREN VERARBEITUNG.“¹

Folgende Grafik verdeutlicht die Struktur im Unternehmen und die Herausforderungen bei der Nutzung und dem Angebot digitaler Dienste.

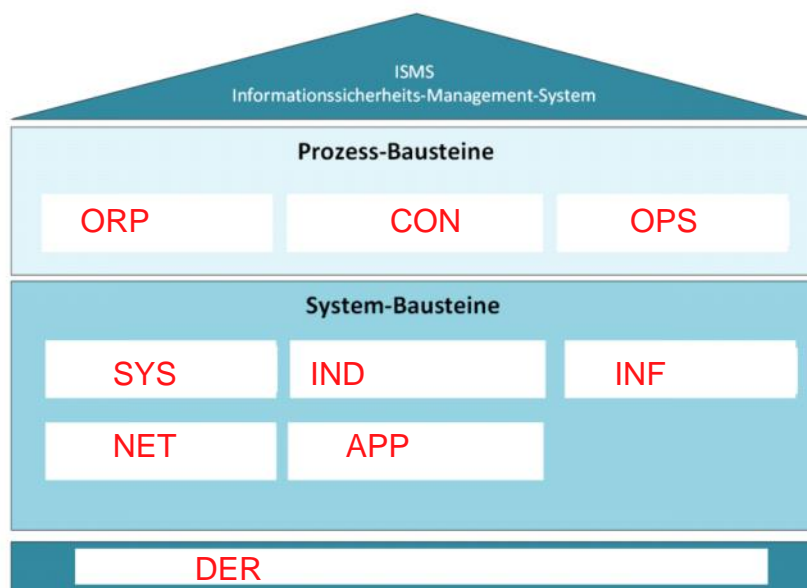


¹ BSI-Standard 200-1 – ISMS, S.8

Arbeitsauftrag

- a) Erklären Sie die obenstehende Abbildung im Gesamtzusammenhang des IT-Grundschutzes.
- b) Das BSI hat die Sicherheitsaspekte in **Bausteinen** zusammengefasst und in Schichten eingeteilt. Ordnen Sie die folgenden Bausteine aus dem BSI IT-Grundschutz-Kompendium den jeweiligen Schichten zu.

Organisation und Personal (ORP)	Anwendungen (APP)	Netze und Kommunikation (NET)
Industrielle IT (IND)	Infrastruktur (INF)	Betrieb (operative, spezielle) (OPS)
Detektion und Reaktion (DER)	Konzepte und Vorgehensweisen (CON)	IT-Systeme (SYS)



Quelle: BSI Schichtenmodell

- c) Beim IT-Grundschutz wird immer wieder von sogenannten **Zielobjekten** gesprochen. Was ist unter Zielobjekt im Sinne des BSI IT-Grundschutzes zu verstehen?

Zielobjekte sind alle Teile des Unternehmens, denen im Rahmen des IT-Grundgesetzes ein oder mehr Bausteine aus dem Kompendium zugeordnet werden

← physische Objekte

- It-Systeme
- Server(-räume)
- Hardware
- etc.

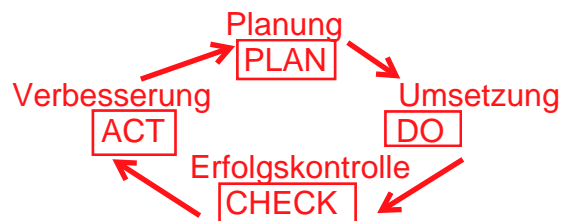
→ logische Objekte

- Organisationseinheiten
- Anwendungen
- etc.

- d) Das BSI spricht bei der Erstellung eines Sicherheitskonzepts davon, dass der gesamte Sicherheitsprozess einem sogenannten **Lebenszyklus** unterliegt.

Informieren Sie sich mittels Recherche über den Lebenszyklus des Sicherheitsprozesses und **skizzieren** Sie diesen.

PDCA - Zyklus



e) Das IT-Grundschutz-Kompendium ist eine Unterstützungsmaßnahme des BSI.

Geben Sie weitere Unterstützungsmaßnahmen (Dokumente) an.

- IT-Grundschutzkompendium
- BSI- Standard 200-1 (Management für Informationssicherheit)
- BSI- Standard 200-2 (IT-Grundschutz Vorgehensweise)
- BSI- Standard 200-3 (Risikoanalyse)
- BSI- Standard 200-4 (Notfallmanagement)

Weitere Hilfsmittel:

- Leitfaden Basisabsicherung
- Online-Kurs vom BSI zum Grundschutz

Hinweis: Für die weitere Bearbeitung im Verlauf des Themas ist es sinnvoll die entsprechenden Unterstützungsmaßnahmen sich lokal zu sichern (Download als PDF).

4.3.2 Schutzziele nach IT-Grundschutz

Die vom BSI festgelegten Schutzziele lassen sich aus der DSGVO (Datenschutz-Grundverordnung) ableiten. Dabei werden diese Schutzziele als Grundwerte der Informationssicherheit festgelegt und verstanden. Diese sind:

- **Verfügbarkeit** (Availability)
- **Integrität** (Integrity)
- **Vertraulichkeit** (Confidentiality)

Das Bundesdatenschutzgesetz (BDSG) 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. Herausgestellt werden hierbei auch die technischen und organisatorischen Maßnahmen (TOM) an den Datenverarbeitungsanlagen (siehe Unterabschnitt Datensicherheit und technisch-organisatorische Maßnahmen).

Vertraulichkeit der Daten: Daten sind für unberechtigte Dritte nicht zugänglich

Integrität der Daten: Daten können nicht verfälscht/unberechtigt verändert werden

Verfügbarkeit der Daten: Zugriff auf Daten ist sicher gestellt, wenn diese benötigt werden

Nicht durcheinander bringen mit den 3 Grundzielen der Verschlüsselung

- Vertraulichkeit
- Integrität
- Authentizität

Arbeitsauftrag

Informieren Sie sich über die **Grundsätze** der Verarbeitung personenbezogener Daten (Art. 5 DSGVO) und **nennen** und **erläutern** Sie diese kurz.

Grundsatz	Erklärung
Rechtmäßigkeit... zweckbindung Datenminimierung	Verarbeitung der personenbezogenen Daten nur, wenn es eine Rechtsgrundlage gibt Personenbezogene Daten dürfen nur für den Zweck verwendet werden, für den sie erasst wurden Daten sollen nur dann erhoben werden, wenn diese für die Dienstleistung / den Zweck notwendig ist. Möglichst "Datensparsam" verhalten.
Richtigkeit	Personenbezogene Daten sollen (möglichst) korrekt (Inhalt) und richtig (Form) Aufbewahrt werden. Fehlerhafte Daten sind zu korrigieren oder zu löschen.
Speicherbegrenzung	Persb. Daten nur so lange wie nötig speichern. (Gesetzliche Vorgaben beachten!)
Integrität und Vertraulichkeit	Persb. Daten müssen sicher (s. Seite vorher) aufbewahrt werden.
Rechenschaftspflicht	Nachweisen und dokumentieren, dass man sich an das Datenschutzrecht hält.

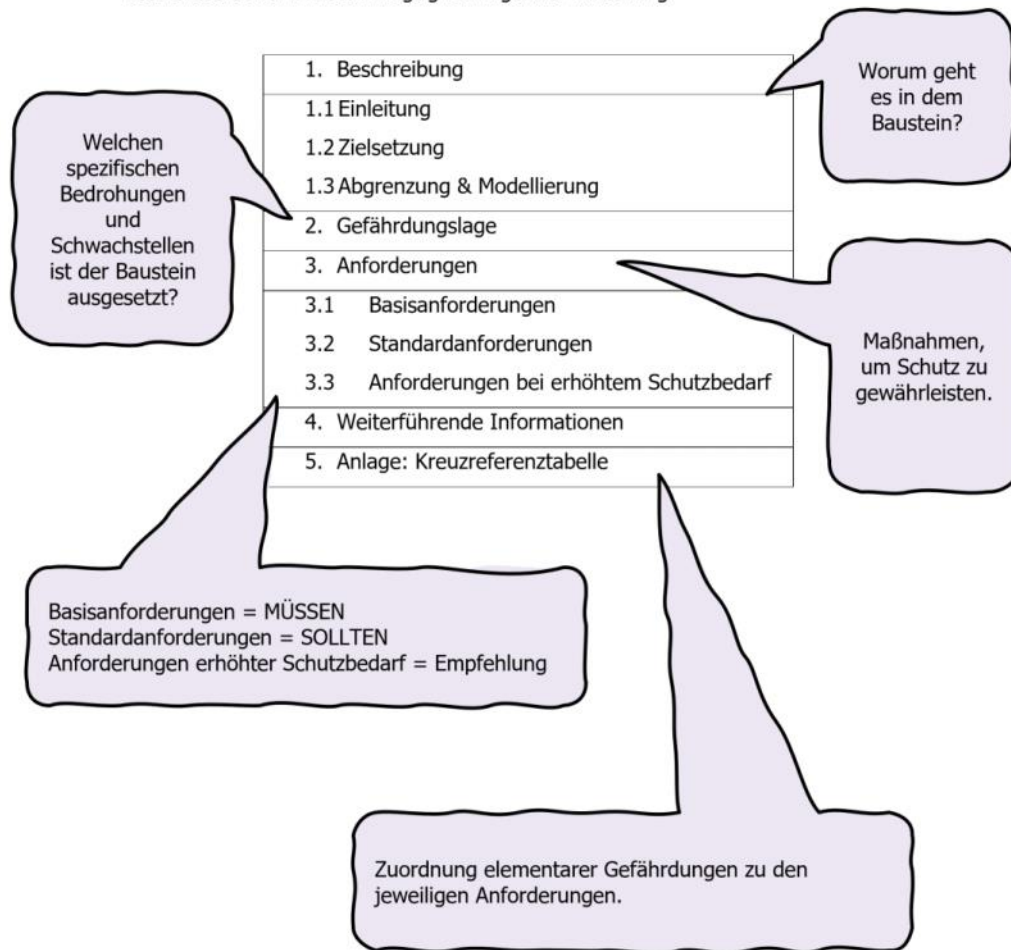
4.3.3 Gefährdungen und Anforderungen

Aufgrund der Grundwerte der Informationssicherheit (Schutzziele) gibt es einen sehr hohen Schutzbedarf bei der Verarbeitung von personenbezogenen Daten. Hierbei hat das BSI eine Systematisierung von Gefährdungen vorgenommen und diese in 47 elementare Gefährdungen abgegrenzt.

Arbeitsauftrag

- a) **Informieren** Sie sich mit Hilfe des **GS-Kompodiums** über die elementaren Gefährdungen.
- b) Finden Sie **5 Elementare Gefährdungen**, welche auch in Ihrem Ausbildungsbetrieb eine große Rolle spielen.
- c) Tauschen Sie sich mit Ihrem Sitznachbarn aus und gleichen Sie die ausgewählten Gefährdungen ab. **Finden Sie Gemeinsamkeiten?**

Im IT-Grundschutz-Kompodium werden die jeweiligen **Bausteine** detailliert betrachtet. Jeder Baustein folgt grob folgender Aufteilung:



- d) Bearbeiten Sie mit Ihrem Sitznachbar den **System-Baustein App.1.2 Web-Browser**. Geben Sie hierzu die **Anforderungen** für einen Schutz (Basis, Standard, erhöhter Schutzbedarf) an.

Stufe	Anforderung
Basis-Anforderung	APP .1.2.A1 Verwendung von grundlegenden Sicherheitsmechanismen(B) APP .1.2.A2 Unterstützung sicherer Verschlüsselungen der Kommunikation(B) APP .1.2.A3 Verwendung von vertrauten Zertifikaten (B) APP .1.2.A6 Kennwortmanagement im Webbrowser (B) APP .1.2.A13 Nutzung von DNS-over-HTTPS (B)
Standard-Anforderung	APP .1.2.A7 Datensparsamkeit in Webbrowsern (S)
Erhöhter Schutzbedarf	APP .1.2.A9 Einsatz einer isolierten Webbrowser-Umgebung (H) APP .1.2.A10 Verwendung des privaten Modus (H) APP.1.2.A11 Überprüfung auf schädliche Inhalte (H) APP.1.2.A12 Zwei-Browser-Strategie (H)

- e) Überprüfen Sie, ob Ihre 5 Gefährdungen aus b) bei diesem Baustein zu finden sind und welche Maßnahmen laut BSI getroffen werden müssen und sollten. Setzt Ihr Betrieb diese um?
- f) Falls Sie schon fertig, dann führen Sie d) nochmals durch anhand eines freiwählbaren Bausteins.

4.3.4 Schadensszenarien und Schadenskategorien

Durch auftretende Sicherheitsvorfälle können Unternehmen beträchtliche Schäden erleiden. Das BSI legt 4 Schadenskategorien und 3 Schutzbedarfskategorien fest.

Schadenskategorien zur Bewertung von Schadensausmaßen	
Bezeichnung	Erläuterung
Niedrig	Ausfall hat eine geringe, kaum spürbare Auswirkung.
Normal	Ausfall hat spürbare Auswirkungen.
Hoch	Ausfall hat erhebliche Auswirkungen.
Sehr hoch	Ausfall oder Beeinträchtigung führen zu existenziell bedrohlichen Auswirkungen.

Schutzbedarfskategorien <ul style="list-style-type: none">• direkte, materielle und finanzielle Schäden• indirekte, immaterielle Schäden	
Bezeichnung	Erläuterung
Normal	Die Schadensauswirkungen sind begrenzt und überschaubar.
Hoch	Die Schadensauswirkungen können beträchtlich sein.
Sehr hoch	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

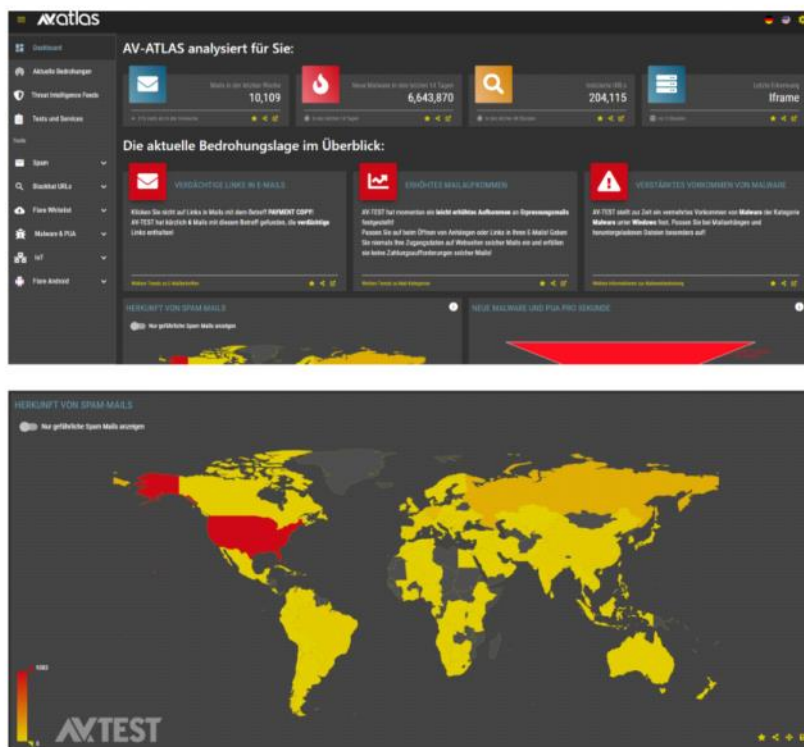
Arbeitsauftrag

Nehmen Sie für den Systembaustein App 1.2 Web-Browser eine Einstufung vor und begründen Sie diese.

	Schadenskategorie		Schutzbedarfskategorien	
	Stufe	Begründung	Stufe	Begründung
App 1.2				

4.3.5 Aktuelle Bedrohungen

Kriminalität macht auch vor dem Internet nicht halt. Täglich gibt es unzählige Angriffe von sogenannten Cyberkriminellen auf Unternehmen, Behörden, Institutionen und private IT-Geräte mittels Schadprogrammen bzw. Schadsoftware (auch Malware genannt). Auf <https://portal.av-atlas.org> finden Sie eine Übersicht der aktuellen Bedrohungslage im Bereich der IT.



Arbeitsauftrag

Besuchen Sie den oben aufgeführten Link und verschaffen Sie sich einen Überblick über die aktuelle Bedrohungslage im Internet / in der IT.

- a) Finden Sie in diesem Zusammenhang die Fachbegriffe für die jeweilige Erklärung.

Begriff	Erklärung
Adware	Hierunter fallen Schadprogramme, die mittels Werbung platziert werden.
Virus	Ein Programm, welches sich unkontrolliert in andere Programme einschleust und sich reproduziert und immensen Schaden anrichten kann.
Wurm	Eine Unterklasse eines Virus, welche sich ebenfalls selbst kopiert, aber autark ausbreitet. Z.B. über Netzwerke oder Wechseldatenträger.
Trojaner	Schadprogramme, die echte Anwendungen vortäuschen. Diese öffnen dann zumeist eine „Hintertür“ im System, damit Schadprogramme eindringen können.
Ransomware	Dieses sind Schadprogramme, die den Zugriff auf Daten und Systeme einschränken.
Scareware	Sogenannte Angstsoftware, die versucht Nutzer dazu zu bringen auf ihrem System schädliche Software zu installieren.
Spam	Hierunter werden unerwünschte Nachrichten, welche in großer Masse und ungezielt via E-Mail verteilt werden.

b) Immer wieder kommt es zu großen Cyberangriffen. Finden Sie den jeweiligen Fachbegriff zu den Attacken.

Gezielter Angriff auf Unternehmen / Organisationen. Cyberkriminelle versuchen dauerhaft Zugriff auf ein Netzwerk zu bekommen.	Ist ein Verbund von Rechnern, Smartphones und ähnlichen Systemen, die von einem fernsteuerbaren Schadprogramm befallen sind. Betroffenen Systeme werden von einem Command-and-Control-Server zentral kontrolliert und gesteuert. Die Betreiber bieten damit schädigende Attacken an.	Hierbei werden gekaperte Computer unbrauchbar gemacht bzw. verweigern ihren Dienst. Beispielsweise durch Massenanfragen auf Webserver.	Bezeichnet eine Angriffsmethode aus dem Internet bei der ein Zielsystem und seine Internetservices durch Überlastung für den User gar nicht mehr oder nur stark eingeschränkt nutzbar ist. In der Regel erfolgt ein Angriff aus einer Vielzahl von Anfragen eines ferngesteuerten Botnetzes.
---	--	--	--

APT
advanced
Persistent
Threat

Bot/
Botnetz

DoS
Denial
of
Service

DDoS
Distributed
Denial of
Service

4.3.6 Identitätsdiebstahl und Social Engineering



Beim Social Engineering wird der Mensch als Schwachstelle von Cyberkriminellen genutzt. Dabei wird versucht, dass Menschen von sich aus Daten preisgeben, damit Sicherheitsmaßnahmen umgangen werden können. Der Angreifer baut einen direkten Kontakt (z.B. über Chat, E-Mail oder soziale Netzwerke) auf und gibt gezielt Insiderwissen vor und appelliert dann an die Hilfsbereitschaft des Opfers. Die Täter gehen dabei sehr

geschickt vor, um die vermeintliche menschliche Schwäche wie Neugier oder Angst auszunutzen.

Arbeitsauftrag

Recherchieren Sie selbstständig zum Thema „Social Engineering“ und beantworten Sie folgende Fragen.

- a) Erklären Sie im Zusammenhang mit Social Engineering den Begriff „**Phishing**“.
- b) Im Rahmen von E-Mail-Angriffen gibt es sogenannte „**CEO-Fraud**“. Was versteht man darunter?
- c) Was ist ein „**Man-in-the-Middle-Angriff**“?

Phishing

Betrugsversuch, der häufig über massenweise E-Mails abläuft. Es werden echt wirkende Mails versendet → Opfer soll auf Link klicken und dort z.B. Passwort eingeben. normalerweise nicht zielgerichtet, sondern für "die Masse" gedacht, in der Hoffnung, dass ein Paar Opfer "anbeißen". Gezielter Angriff auf ein bestimmtes Opfer: Spear-Phishing

CEO-Fraud: z.B. über Mails von (vorgegebenen) Führungskräften werden Mitarbeiter im Sekretariat oder Buchhaltung unter Druck gesetzt und aufgefordert, in kurzer Zeit hohe Geldbeträge unter Geheimhaltung zu überweisen. (z.B. anstehende Firmenübernahme oder ähnliches)
Lösungsmöglichkeiten: Mitarbeiter (vorab) sensibilisieren; Überweisungslimit ab dem zwei Personen Auftrag freigeben müssen, etc

Man-In-the-middle:

Allgemeine Bezeichnung für einen Angriff, bei dem sich jemand in die Datenübertragung "einlinkt" und diese belauscht oder sogar abändert.
Lösungsmöglichkeiten: Ende-zu-Ende Verschlüsselung (VOM Absender BIS zum Empfänger durchgängige Verschlüsselung)

4.3.7 Maßnahmen gegen Cyberangriffe



Um sich gegen Cyberangriffe zur Wehr zu setzen können schon einfache Maßnahmen einen guten – wenn auch nicht vollumfassenden – Schutz bieten. Eine nahliegende Maßnahme ist die Verwendung von sicheren Passwörtern.

Das BSI empfiehlt hierzu im ORP.4.A22 Regelung zur Passwortqualität [IT-Betrieb] folgendes:

„IN ABHÄNGIGKEIT VON EINSATZZWECK UND SCHUTZBEDARF MÜSSEN SICHERE PASSWÖRTER GEEIGNETER QUALITÄT GEWÄHLT WERDEN. DAS PASSWORT MUSS SO KOMPLEX SEIN, DASS ES NICHT LEICHT ZU ERRATEN IST. DAS PASSWORT DARF NICHT ZU KOMPLIZIERT SEIN, DAMIT DER BENUTZER IN DER LAGE IST, DAS PASSWORT MIT VERTRETBAREM AUFWAND REGELMÄßIG ZU VERWENDEN.“

Arbeitsauftrag

- Überlegen Sie sich ein sicheres Passwort und leiten daraus allgemeine Regeln /Voraussetzung bei der Verwendung von Passwörtern ab.
- Vergleichen Sie Ihr Passwort mit dem Passwort eines Mitschülers. Was haben Ihre Passwörter gemeinsam, worin unterscheiden Sie sich?
- Prüfen Sie Ihr Passwort unter

<https://kurzelinks.de/ha00>



Machen Sie den Test, ob Ihr Passwort sicher ist.

Regeln für gute Passwörter:

- Passwörter nicht auf mehreren Seiten/ für mehrere Zugänge verwenden
- kleine und große Buchstaben verwenden
- Sonderzeichen verwenden
- Zahlen verwenden
- Lange Passwörter verwenden
- Keine bekannten Wörter (einzeln) verwenden, keine bekannten Namen, keine bekannten Daten
- Evtl. Passwort-Sätze benutzen mit individuellem Anhang

→ Passwort-Manager und zufällig erzeugte, ausreichend sichere individuelle Passwörter

- d) Passwörter sollen die Sicherheit gerade bei der Anmeldung gewährleisten. In diesem Zusammenhang wird auch von der **Zwei- oder Multi-Faktoren- (2FA) Authentifizierung** gesprochen. Erklären Sie was darunter zu verstehen ist.

Es wird ein zweiter Faktor (neben dem Passwort) zum Login / zur Freigabe einer Aktion benötigt.

Bsp: PIN + TAN, OTP, Yubikey, FIDO2

- e) Eine weitere Maßnahme ist der Einsatz von **Blacklisting** und **Whitelisting**. Grenzen Sie beide Begriffe voneinander ab.

Blacklist: verbote werden aufgelistet, alles andere ist zulässig
Whitelisting: Grundsätzlich alles verboten nur die "guten Ausnahmen" auf der Liste sind erlaubt.

- f) Welche Maßnahmen kennen Sie noch? Halten Sie diese stichpunktartig fest.

captcha: Nachweist, dass man k

4.3.8 Datensicherheit und technisch-organisatorische Maßnahmen


Der Begriff der Datensicherheit ist untrennbar mit dem Begriff des Datenschutzes verbunden. Dabei sind die Begriffe keine Synonyme füreinander.

Arbeitsauftrag


Die Begriffe Datenschutz und Datensicherheit werden oft als Synonym verwendet.

- Recherchieren** Sie zunächst nach einer **Definition** von **beiden Begriffen**.
- Füllen Sie die **Lücken zu den Definitionen** und die **beigefügte Abbildung** aus.

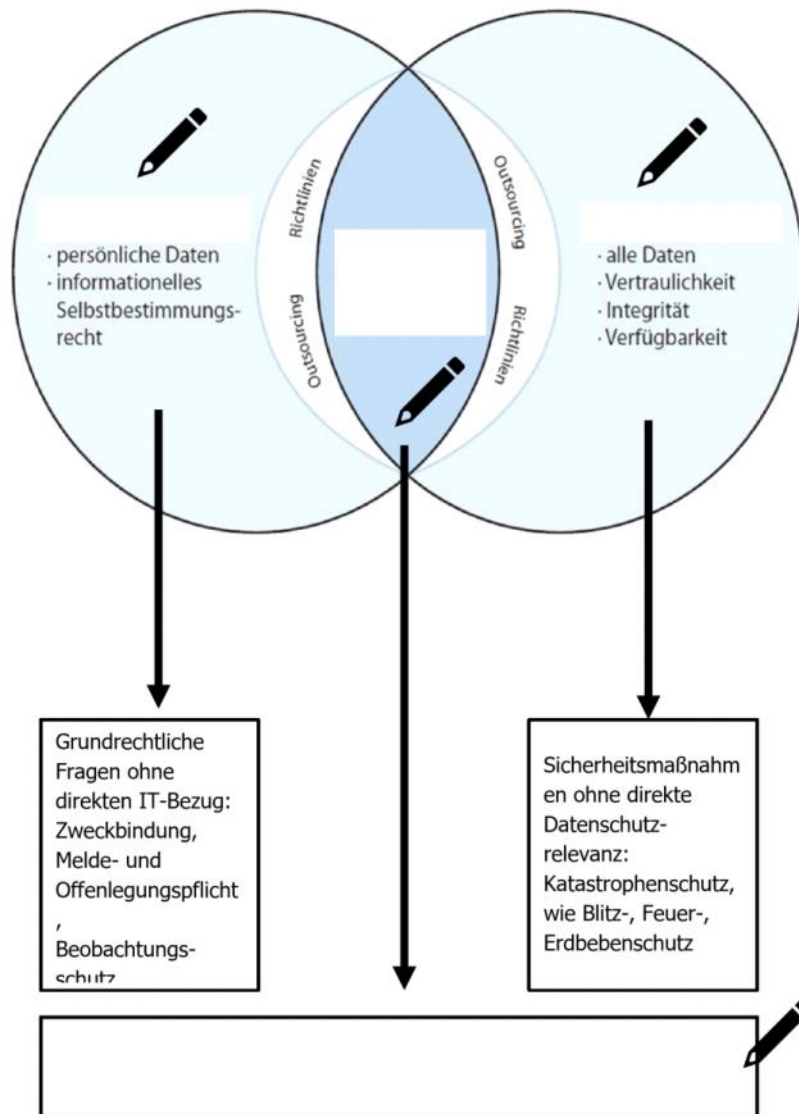
Datenschutz:

Unter Datenschutz wird der Schutz von vor 
Missbrauch während , und
 verstanden. Dabei soll das Recht auf
 gewährt bleiben.

Datensicherheit:

Unter Datensicherheit werden in der betrieblichen Datenverarbeitung alle 
 und
Maßnahmen zum Schutz von Daten vor ,
und verstanden.

Konvergenz zwischen Datenschutz und Datensicherheit



Angelehnt an: <https://www.all-about-security.de/security-artikel/management-und-strategie/single/konvergenz-zwischen-datenschutz-und-datensicherheit/>

Bei der Auswahl geeigneter technisch-organisatorischer Maßnahmen (TOM) bietet der § 64 BDSG eine Hilfestellung. Gemäß § 64 Bundesdatenschutzgesetz (BDSG) sind alle Stellen, welche personenbezogene Daten verarbeiten, erheben oder nutzen verpflichtet, technische und/oder organisatorische Maßnahmen (kurz: TOM) zu treffen, um zu gewährleisten, dass die Sicherheits- und Schutzanforderungen des BDSG erfüllt sind. Grundlage hierfür ist der Art. 32 DSGVO.

Arbeitsauftrag

- a) Finden Sie in Gruppenarbeit **konkrete Umsetzungsmaßnahmen** für die einzelnen Kontrollen, welche im § 64 BDSG zu finden sind. Stellen diese mittels Mind-Map dar.

- b) Bereiten Sie sich darauf vor, Ihre **Ergebnisse der Klasse vorzustellen** und **näher zu erläutern**.

Wenn Sie schon fertig sind ...

Bewerten Sie zudem die im § 64 BDSG genannten Maßnahmen. **Sind sie hilfreich?** Bestehen **Verbesserungsmöglichkeiten** vor dem Hintergrund sich **schnell ändernder technischer Systeme**?