



Unternehmen für Bildung.

Handout

Schutzbedarfsanalyse im eigenen
Arbeitsbereich durchführen

Modul: **ITG / D - Handout**

Version: 1.0
November 2021

Erstellt von: IT-Abteilung

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

Version, Datum: 1.0, November 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

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 Personennamen.	
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 Zubehörs	
e) Wenn fremde Marken für eigenes werbliches Handeln ohne Zustimmung des Rechteinhabers genutzt werden, kann es zu Markenrechtverletzungen kommen.	

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 | <input type="text"/> |
| b) Browser | <input type="text"/> |
| c) WLAN-Zugang | <input type="text"/> |
| d) Sicherheitsbeauftragter des Arbeitsplatzbereichs | <input type="text"/> |
| e) Stromschwankungen im Stromnetz | <input type="text"/> |
| f) IoT-Sensor beim kooperativen Roboter | <input type="text"/> |
| g) Vergabe eines Passwortes eines Arbeitsplatzes an mehrere Personen | <input type="text"/> |
| h) Notfallrichtlinie am Arbeitsplatz im Gefährdungsfall | <input type="text"/> |
| i) Ausspähen von Daten bei Softwaretests | <input type="text"/> |
| j) Datenverlust bei der Datensicherung am Arbeitsplatz | <input type="text"/> |

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		
<i>z. B. Stromausfall</i>	<i>z. B. Kunden können ihre Konten nicht aufrufen</i>	<i>z. B. Stromausfall durch USV beheben</i>
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 Paragraph der DSGVO verlangt die Sicherheit der Datenverarbeitung und was sind die wesentlichen Forderungen?

- f) In welche vier Schadenskategorien sollen Schäden eingestuft werden?

Lernzielkontrolle TAG 3

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

APT - Botnetz - Hoax - Phishing - PUA - Ransomware - 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

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.		
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) Bildschirmschutz 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.	

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.

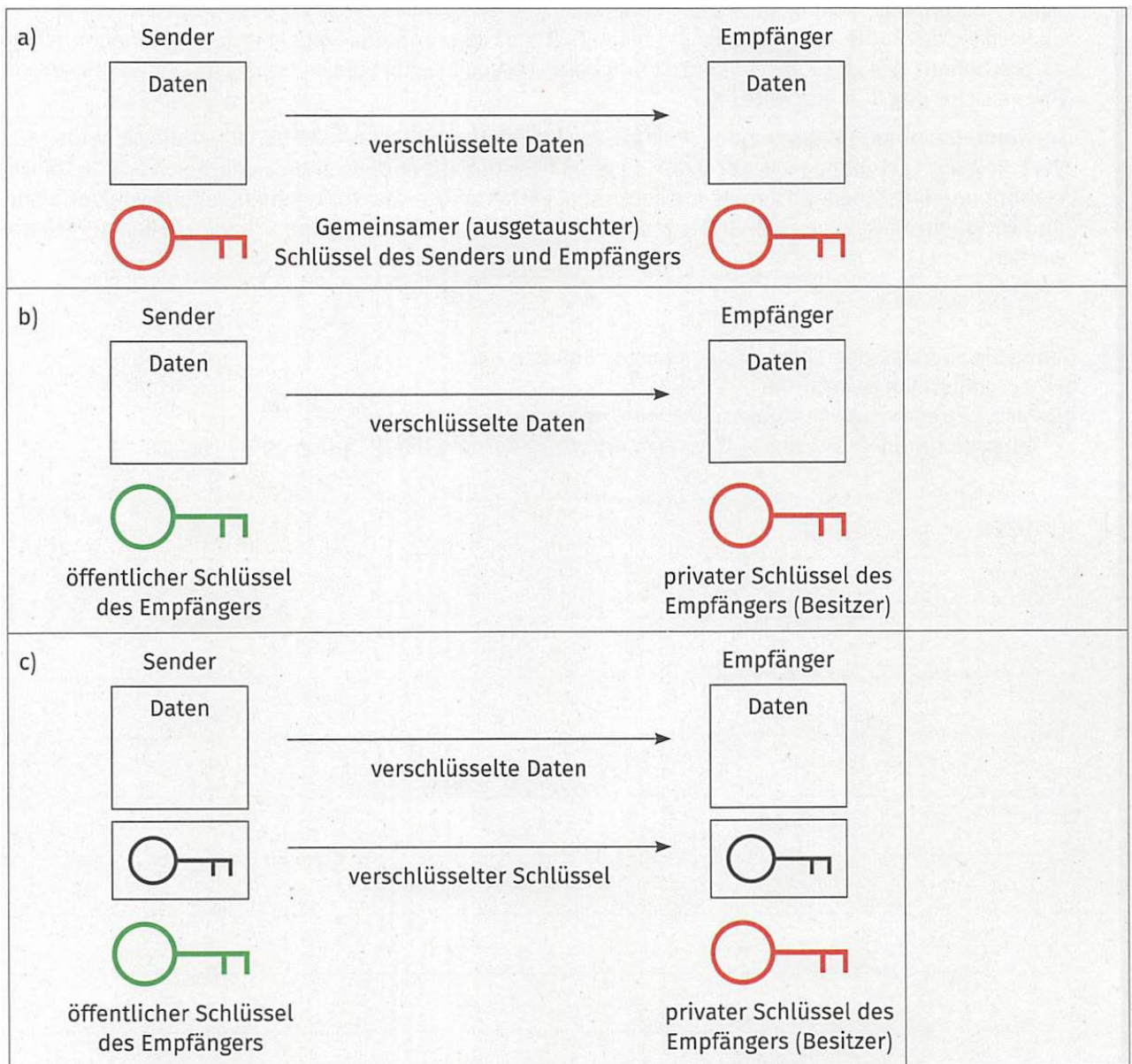
Auszug aus dem Glossar der JIKU IT-Solutions
Datenschutzbeauftragte/-r: Im § 38 BDSG ist festgelegt, dass Unternehmen dann zur Benennung einer/eines Datenschutzbeauftragten verpflichtet sind, wenn mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt 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 gerichts-feste 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.

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

Lernzielkontrolle TAG 6

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



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 installiert ist, um diese sicher vom PC zu entfernen.
- g) Wenn möglich sollte immer die gleiche Version eines Office-Produktes mit derselben Konfiguration auf allen Rechnern im Unternehmen installiert sein.
- h) Die Programmierung und Nutzung von Makros in Office-Produkten sollten einheitlichen Regeln unterworfen sein.
- i) 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

Lernsituation: Wir erarbeiten Schutzbedarfsfeststellungen bei der JIKU IT-Solutions GmbH

Holger Lübberstedt: Sie haben sich die Grundlagen zur Schutzbedarfsfeststellung erfolgreich erarbeitet und die entsprechenden Tests erfolgreich bestanden. Jetzt sollen Sie Ihr Wissen konkret anwenden. Dazu wiederholen Sie noch einmal kurz das dafür notwendige Basiswissen und führen anschließend einige Schutzbedarfsfeststellungen für verschiedene Arbeitsplätze durch. Dieses betrifft hauptsächlich erst einmal Ihre eigenen Arbeitsplätze in unserem Unternehmen. Hier können Sie notwendige Erfahrungen sammeln.

Julian Markus: Ist das Verfahren der Schutzbedarfsfeststellung sehr umfangreich?

Holger Lübberstedt: Das kommt ganz darauf an, wofür eine solche Schutzbedarfsfeststellung vorgenommen werden soll. Eine komplette Schutzbedarfsfeststellung für ein Unternehmen ist eine sehr umfangreiche und aufwendige Arbeit. Sie werden aber im kleinen Rahmen erst einmal für verschiedene Arbeitsplätze die Gefährdungslage und den Schutzbedarf ermitteln und danach verschiedene Schutzmaßnahmen vorschlagen.

Jannik Brunke: Welche Rolle spielen Daten und Anwendungen bei der Schutzbedarfsfeststellung?

Holger Lübberstedt: Daten und Anwendungen, welche an den einzelnen Arbeitsplätzen Einsatz finden, spielen eine zentrale Rolle bei der Schutzbedarfsfeststellung. Es muss dabei der Schutzbedarf bezüglich Vertraulichkeit, Verfügbarkeit und Integrität ermittelt werden. Darauf baut der gesamte Schutzbedarf des Arbeitsplatzes auf. Es gilt hier das Maximumprinzip.

Patrick Franke: Ich möchte Sie abschließend nochmal daran erinnern, dass Sie Ihre Arbeit ernst nehmen und gründlich und gewissenhaft durchführen, denn jedes kleinste Sicherheitsleck kann unserer Firma schaden. Gerade da wo man es am wenigsten vermutet, entsteht der meiste Schaden. Verantwortung fängt am eigenen Arbeitsplatz an. Auf der anderen Seite sind die Kunden unseres Unternehmens auch dankbar, wenn man Sie z.B. auf eventuelle Gefährdungslagen hinweist, auch wenn das nicht unmittelbar zum Auftrag gehört.

Schutzbedarfsfeststellung in Arbeitsbereichen von JIKU IT-Solutions durchführen

Holger Lübberstedt: Wie schon erwähnt, werden Sie die Schutzbedarfsfeststellung für die entsprechenden Arbeitsplätze wieder im Team durchführen. Dadurch lernen Sie voneinander und können sich gegenseitig unterstützen.

Laura Maier: Nachdem es das letzte Mal so gut geklappt hat, würde ich gerne wieder die Teamleitung übernehmen.

Holger Lübberstedt: Ja, ich kann aus meiner Sicht bestätigen, dass Sie beim letzten Projekt das Team sehr gut geleitet haben. Sie haben auch die höchste Punktzahl bei den vorherigen Tests erreicht und damit bewiesen, dass Sie ein sehr gutes Grundlagenwissen für die anstehenden Aufgaben mitbringen. Trotz der guten und sehr guten Leistungen, welche alle in den letzten Tests gezeigt haben ist es unerlässlich von Zeit zu Zeit sein Wissen zu überprüfen und aufzufrischen, damit Sie Gefährdungslagen erkennen und Schutzmaßnahmen angemessen auswählen können.

Aufgabe 1: Überprüfen und erweitern Sie Ihr Wissen über Bedrohungen und Schutzmaßnahmen von Software.

Beantworten Sie folgende Fragen und kreuzen an, was richtig ist.

Bedrohungen und Schutzmaßnahmen von Software	
1. Was sind typische Gefährdungen der Standardsoftware eines Arbeitsplatzes?	
a) Der Quelltext der Software geht verloren.	
b) Ein Computervirus nimmt an der Software Veränderungen vor.	
c) Durch unvorsichtiges Bestätigen eines Löschvorgangs gehen Daten verloren.	
d) Eine speziell auf die verwendete Hardware konfigurierte Software wird genutzt.	
2. Welche Schutzmaßnahmen für Standardsoftware sind korrekt?	
a) Die Software mithilfe von Originaldatenträgern installieren	
b) Vertrauenswürdige Testversionen der Software installieren	
c) Jeder Mitarbeiter ist für seinen Arbeitsplatz der Hauptverantwortliche	
d) Implementierung zusätzlicher Sicherheitsfunktionen	
3. Welche Schutzmaßnahmen sind bei Betriebssystemen anzuwenden?	
a) Verwendung von sicheren Passwörtern	
b) Generell nur Windows als Betriebssystem verwenden	
c) Nicht benötigte Ports sperren	
d) Sicherheitsupdates nur mit zeitlicher Verzögerung einspielen	
e) Um Möglichkeiten des Betriebssystems voll zu nutzen, immer alle Programme und Funktionalitäten installieren	
4. Welche Schutzmaßnahmen für Office-Produkte sind anzuwenden?	
a) Es sind immer Open-Source-Office-Produkte einzusetzen.	
b) Es sollen eventuell vorhandene Viewer-Funktionalitäten verwendet werden.	
c) Jeder Benutzer sollte kleine, auf seine Bedürfnisse abgestimmte Sicherheitsmakros implementieren.	
d) Um Angriffe zu erschweren, sollten verschiedene Versionen eines Office-Produktes installiert werden.	
5. Welche Gefährdungen sind beim Einsatz von Containern zu berücksichtigen?	
a) Schwachstellen des Container-Images	
b) Ausbruch aus dem Container	
c) Fehlende Persistenz	
d) Zu wenig Anwendungen bzw. Dienste pro Container	
e) Sicherung der Daten außerhalb des Containers	

6. Welche Schutzmaßnahmen sollten beim Einsatz von Containern berücksichtigt werden?	
a) Nutzung aller zur Verfügung stehenden Ressourcen für einen Container	
b) Möglichst viel Funktionalität (Anwendungen, Dienste) in einen Container	
c) Verschlüsselung der Datenhaltung bei Containern	
d) Sicherung des Host-Systems	

Aufgabe 2:

Werten Sie einen englischen Text über die Sicherheit von Betriebssystemen aus.

Ein Kunde soll beraten werden, welches Betriebssystem für den Arbeitsplatzrechner bezüglich des Themas „Sicherheit“ am geeignetsten wäre. Folgender englischer Text enthält dazu wichtige Aussagen.

Lesen Sie sich den Text durch und machen Sie sich dazu Notizen. Diskutieren Sie im Anschluss in Partnerarbeit oder in einem Team von drei bis fünf Mitgliedern den Inhalt, den Wahrheitsgehalt der Aussagen und tauschen Sie sich über Ihre konkreten Erfahrungen mit den entsprechenden Betriebssystemen aus.

1. Windows is the least Secure because of its install base

Windows is the most targeted of all the operating systems because the size of the install base makes it the most efficient to attack. If you write malware that can run on 88 % of the computers, you will most likely have the greatest success.

But that doesn't mean Windows is less secure than other OSs. You could also say that the popularity of Windows means that Microsoft has the most experience protecting against malware attacks. The real point is that there is more malware targeting Windows and that means you need a good security solution. But a good security solution should always be used, no matter what operating system you are using and how much malware exists for it.

2. Linux is the most Secure because it's Open Source

Many people say this all the time. The security theory that if many people look at a source code it is automatically safer, is obviously flawed. The SentinelOne Researcher Dor Dankner recently revealed that Linux has an undetected privilege escalation vulnerability. This was introduced in the Linux kernel in 2004. Although the code has been reviewed, nothing has been done to improve it. Likewise, openssl contained the Heartbleed bug for over two years before it was finally discovered.

3. macOS is the most secure because Apple

Apple has managed to position itself in public as "security conscious", due to the closed nature of their mobile platform and iOS. In Apple's marketing a lot of security is "built in", but the truth is that Mac security features like gatekeeper, XProtect and MRI are easy to do and not particularly comprehensive. Again, one could argue that having less experience in defending against malware, Apple are not as well-schooled as Microsoft in the art of building a hardened OS.

4. Linux is the most secure because it's highly configurable

It is true that something like SELinux probably has more ways to "harden" the system than macOS or Windows. But very few companies will use a locked down SELinux install as their desktop operating system, at least not when employees are supposed to do useful work. Security and usability go hand in hand, and users often make less confident decisions when they struggle against the operating system just to maintain their job.

Quelle: SentinelOne.com/o.A.: Which is More Secure: Windows, Linux, or macOS?, veröff. am 21.02.2019 unter www.sentinelone.com/blog/which-is-more-secure-windows-linux-or-macos/ [31.07.2020]

NOTIZEN

Aufgabe 3:

Führen Sie Schutzbedarfsfeststellungen für Arbeitsplatzsoftware durch.

Auf mehreren Rechnern in der Verwaltungsabteilung von JIKU IT-Solutions ist eine Software mit dem Namen „EasyTravel“ installiert. Mit dieser Software werden u.a. die Reisebuchungen und Reisekostenabrechnungen für Unternehmensmitarbeiter vorgenommen und bearbeitet. Es soll dabei zu keinen Verfälschungen oder Unstimmigkeiten kommen, weil das aufwendige Umbuchungen und Kosten nach sich ziehen würde. Die Daten werden in einer Datenbank gespeichert.

Notieren Sie sich zunächst einige konkrete Gefährdungen.

NOTIZEN

2. Ermitteln Sie für die Software „EasyTravel“ den Schutzbedarf, begründen Sie Ihre Entscheidungen und schlagen Sie konkrete Maßnahmen vor.

Grundwert	Schutzbedarf	Begründung	Maßnahmen
Vertraulichkeit			
Integrität			
Verfügbarkeit			

3. Führen Sie in Teamarbeit eine Schutzbedarfsfeststellung für Softwareprodukte durch. Orientieren Sie sich dabei an einem Arbeitsplatz in Ihrem Unternehmen, in der Berufsschule oder in Ihrem privaten Umfeld.

- Ermitteln Sie zunächst alle Softwareprodukte, welche am Arbeitsplatz installiert sind.
- Entscheiden Sie sich für zwei konkrete Anwendungen, für die Sie die Schutzbedarfsfeststellung durchführen wollen.
- Ermitteln Sie aus dem IT-Grundschutz-Kompodium des BSI die Bausteine, welche auf Ihre Anwendungen zutreffen.
- Ermitteln Sie den Schutzbedarf und begründen Sie Ihre Entscheidung.
- Empfehlen Sie im Anschluss konkrete Maßnahmen.
- Stellen Sie Ihre Ergebnisse den anderen Teams vor.

Schutzbedarfsfeststellung



Arbeitsbereich:

Thema: *Schutzbedarf „Anwendungen“*

Datum:

Ersteller:

Anwendung	Grundwert	Schutzbedarf	Begründung	Maßnahmen
	Vertraulichkeit			
	Integrität			
	Verfügbarkeit			
	Vertraulichkeit			
	Integrität			
	Verfügbarkeit			

Unterschrift:

Aufgabe 4: Überprüfen Sie Ihr Wissen über Bedrohungen und Schutzmaßnahmen von Clients.

Ordnen Sie den Ereignissen in der Tabelle entsprechende Gefährdungskategorien zu. Hinweis: Es sind mehrere Gefährdungen gleichzeitig möglich.

Gefährdungen

- (A) Verlust von Daten durch lokale Datenspeicherung
- (B) Verlust von Daten durch Hardware defekte
- (C) Verlust von Daten durch Schadprogramme
- (D) Unberechtigte Benutzung

Ereignisse	
1. Ein Außendienstmitarbeiter benötigt dringend Daten, findet die zuständige Kollegin aber nicht an ihrem Arbeitsplatz vor. Da ihr Rechner läuft und er direkten Zugang hat, kopiert er die notwendigen Daten auf seinen USB-Stick und schreibt der Kollegin zur Information eine Notiz.	
2. Eine verbaute SSD wird plötzlich nicht mehr erkannt.	
3. Ein Auszubildender „räumt“ seinen Rechner auf und löscht überflüssige Daten.	
4. Eine Blumenvase am Arbeitsplatz wird von einem unvorsichtigen Mitarbeiter umgestoßen und setzt u.a. den Arbeitsplatzrechner des Kollegen komplett unter Wasser.	
5. Da sich ein Auszubildender die vielen Passwörter nicht mehr merken kann, hat er sich 5. das Passwort für seinen Arbeitsplatzrechner auf einem Zettel notiert und diesen in seinem Schreibtisch „unsichtbar“ aufbewahrt.	

Aufgabe 5:

Führen Sie Schutzbedarfsfeststellungen für Clients eines Arbeitsplatzes durch.

Für Außendienstmitarbeiter von JIKU IT-Solutions sind mobile Arbeitsplatzrechner (Laptops) geplant. Über den Laptop werden neue Kunden- und Produktdaten erfasst und über eine Internetverbindung in die Firmendatenbank geschrieben. Über diesen Weg sollen auch aktuelle Daten abgerufen werden können. Wenn diese Informationen verfälscht werden oder in nicht autorisierte Hände gelangen, entsteht für die Firma ein beträchtlicher Schaden, welcher aber noch nicht existenzbedrohend ist. Außerdem besteht die Forderung, dass die Außendienstmitarbeiter auch auf die wichtigsten Daten zugreifen bzw. neue Daten erfassen können, wenn keine Internetverbindung zur Verfügung steht. Es darf dort zu keinen Problemen kommen, da das Image der Firma größeren Schaden nehmen könnte.

1. Notieren Sie sich zunächst einige konkrete Gefährdungen.

NOTIZEN

2. Ermitteln Sie für diese Clients (Laptop für Außendienstmitarbeiter) den Schutzbedarf, begründen Sie Ihre Entscheidungen und schlagen Sie konkrete Maßnahmen vor.

Grundwert	Schutzbedarf	Begründung	Maßnahmen
Vertraulichkeit			
Integrität			
Verfügbarkeit			

3. Führen Sie in Teamarbeit eine Schutzbedarfsfeststellung für Clients durch. Orientieren Sie sich dabei an einem Arbeitsplatz in Ihrem Unternehmen, in der Berufsschule oder in Ihrem privaten Umfeld.
 - a) Ermitteln Sie aus dem IT-Grundschutz-Kompodium des BSI die Bausteine, welche auf den Client zutreffen.
 - b) Ermitteln Sie den Schutzbedarf für den ausgewählten Client und begründen Sie Ihre Entscheidung.
 - c) Empfehlen Sie im Anschluss konkrete Maßnahmen und stellen Sie Ihre Ergebnisse den anderen Teams vor.

Schutzbedarfsfeststellung				
Arbeitsbereich: _____				
Thema: <i>Schutzbedarf „Client“</i>				
Datum: _____			Ersteller: _____	
Client	Grundwert	Schutzbedarf	Begründung	Maßnahmen
	Vertraulichkeit			
	Integrität			
	Verfügbarkeit			
Unterschrift: _____				

Aufgabe 6: Überprüfen Sie Ihr Wissen über Bedrohungen und Schutzmaßnahmen von mobilen Datenträgern.

1. Nennen Sie für jede Art mobiler Datenträger je zwei Beispiele

Art	Beispiele
Auswechselbare Datenträger (Wechseldatenträger)	
Externe Datenträger	
Datenträger, welche in mobile IT-Geräte integriert sind	

2. Nennen Sie drei Bedrohungen für mobile Datenträger und schlagen Sie jeweils eine geeignete Schutzmaßnahme vor.

Bedrohung	Schutzmaßnahme
1.	
2.	
3.	

3. Beschreiben Sie kurz, was Sie unter folgenden Schutzmaßnahmen verstehen und warum diese notwendig sind.

Schutzmaßnahme	Beschreibung
Sicheres Löschen der Datenträger vor und nach der Verwendung	
Verlustmeldung	
Einführung einer Datenrückmeldung	

4. Übersetzen Sie den folgenden Text und diskutieren Sie im Anschluss über die Verwendung von USB-Sticks zum Datenaustausch.

Data exchange has become an important part of everyday life these days. In many cases, USB sticks are still used for this. Unfortunately, USB sticks still carry an increased risk of infection for computers despite regular awareness campaigns with the most important rules of conduct. The latest Honeywell report paint a terrifying picture for any cybersecurity expert: 40% of USB sticks contain at least one potentially dangerous folder and 26% of these risks could cause malfunctions in the operating system. That why is in many companies, such as IBM, the use of USB is simply prohibited.

Aufgabe 7: Führen Sie Schutzbedarfsfeststellungen für mobile Datenträger durch.

Eine Anwaltskanzlei führt eine Schutzbedarfsfeststellung für den Umgang mit mobilen Datenträgern durch. Bisher gab es noch keine Festlegungen dafür. Bei einer Befragung von Mitarbeitern bezüglich der bisherigen Verwendung von mobilen Datenträgern ist herausgekommen, dass USB-Sticks sehr häufig zum Datenaustausch verwendet werden. Viele Mitarbeiter nehmen sich bei hohem Auftragsvolumen Arbeit mit nach Hause, bearbeiten die Unterlagen am privaten Rechner, bringen die Ergebnisse am nächsten Tag wieder mit in die Firma und spielen diese mithilfe Ihres Arbeitsplatzrechners wieder in die Datenbank. Das betrifft auch Informationen, deren Verlust oder Verfälschung zu einem Imageschaden und hohen finanziellen Schaden für die Kanzlei führen würde.

1. Notieren Sie sich zunächst einige konkrete Gefährdungen.

NOTIZEN

2. Ermitteln Sie den Schutzbedarf, begründen Sie Ihre Entscheidungen und schlagen Sie konkrete Maßnahmen vor.

Grundwert	Schutzbedarf	Begründung	Maßnahmen
Vertraulichkeit			
Integrität			
Verfügbarkeit			

3. Führen Sie in Teamarbeit eine Schutzbedarfsfeststellung mobiler Datenträger durch. Orientieren Sie sich dabei an einem Arbeitsplatz in Ihrem Unternehmen, in der Berufsschule oder in Ihrem privaten Umfeld.
 - a) Ermitteln Sie aus dem IT-Grundschutz-Kompendium des BSI die Bausteine, welche auf den Umgang mit mobilen Datenträgern zutreffen.
 - b) Ermitteln Sie den Schutzbedarf für mobile Datenträger und begründen Sie Ihre Entscheidung.
 - c) Empfehlen Sie im Anschluss konkrete Maßnahmen.
 - d) Stellen Sie Ihre Ergebnisse den anderen Teams vor.

Schutzbedarfsfeststellung				
Arbeitsbereich:				
Thema: <i>Schutzbedarf bei Verwendung mobiler Datenträger</i>				
Datum:		Ersteller:		
Daten	Grundwert	Schutzbedarf	Begründung	Maßnahmen
	Vertraulichkeit			
	Integrität			
	Verfügbarkeit			
Unterschrift:				