SCHÜLERMAPPE

SELBSTLERNEINHEIT

Berufsschüler BOTTOM-UP! für IT-Sicherheit

LERNEINHEIT 7: IT-SICHERHEIT FÜR LEITENDE IN KLEINEN UND MITTLEREN UNTERNEHMEN

Auch kleine und mittlere Unternehmen kommen heutzutage nicht mehr ohne anwendungs- und bedarfsspezifische IT aus. **Unabhängig von der konkreten Architektur der Unternehmens-IT** muss ein **ausreichend hohes Sicherheitsniveau** gewährleistet werden. Dies kann insbesondere bei Kleinstunternehmen bestandsgefährdend sein! Allerdings leisten sich viele Betriebe – zumeist aus Kostengründen – keinen speziell ausgebildeten IT-Fachmann. Stattdessen übernimmt dann der **Unternehmensinhaber oder leitende Angestellte** die Funktion der **IT-Betreuung**. Genau an diese Zielgruppe (aber nicht nur!) richtet sich diese Lerneinheit.

DIE THEMEN:

*Obwohl aus Gründen der Lesbarkeit im Text die männliche Form gewählt wurde, beziehen sich die Angaben auf Angehörige aller Geschlechter.

1. GESETZLICHE BESTIMMUNGEN

Was ist Informationssicherheit?

Der Begriff **Informationssicherheit** umfasst in Bezug auf elektronisch gespeicherte Informationen „traditionell“ drei Aspekte: **Vertraulichkeit, Verfügbarkeit** und **Integrität**. In einigen Definitionen kommt als viertes Kriterium noch die **Authentizität** hinzu.

Vertraulichkeit: Informationen müssen vor unbefugtem Zugriff geschützt sein.

Um die **Vertraulichkeit** von Informationen – beispielsweise von Kunden- und Personaldaten sowie Geschäftsgeheimnissen – zu gewährleisten, müssen sie unbedingt vor dem Zugriff durch Unbefugte geschützt werden.

Verfügbarkeit: Technik muss einsatzbereit sein, wenn sie benötigt wird.

Das Kriterium **Verfügbarkeit** bezieht sich darauf, dass alle Informationen zur gewünschten Zeit in vollem Umfang verfügbar, also lesbar und bearbeitbar, sein müssen. Das heißt, nicht nur die Informationen müssen vorhanden sein, sondern auch alle zum Übertragen, Lesen und Bearbeiten der Informationen erforderlichen Systeme – zum Beispiel Computer, Netzwerk und Anwendersoftware – müssen sicher funktionieren. In diesem Zusammenhang spielen etwa die Zuverlässigkeit produktionskritischer Infrastrukturen und die regelmäßige Datensicherung eine wichtige Rolle.

Integrität: Informationen, Hard- und Software müssen frei von Manipulationen und Verfälschungen sein.

Zur Sicherstellung der **Integrität** von Informationen gehört zum einen, zu verhindern, dass Informationen gefälscht bzw. falsche Informationen verarbeitet werden. Zum anderen ist sicherzustellen, dass sämtliche verwendete Hard- und Software frei von Manipulationen ist, die unerwünschte Funktionen ausführen und dadurch beispielsweise Daten verfälschen oder falsche Ergebnisse erzeugen. Daraus resultieren die vollständige Nachvollziehbarkeit von Änderungen an Informationen durch Logging und die Verwendung digitaler Signaturen, um einen maximalen Schutz vor unbefugten Änderungen an Informationen zu gewährleisten. Außerdem sollten alle betreffenden Mitarbeiter im Erkennen von kompromittierten (manipulierten) Systemen geschult sein.

Authentizität: Informationen stammen wirklich von der als Absender benannten Quelle.

Das teilweise verwendete Kriterium der **Authentizität** bezieht sich hauptsächlich auf Informationen, die auf elektronischem Wege übertragen werden, und soll sicherstellen, dass die Daten bzw. Informationen auch tatsächlich von der als Absender benannten Stelle kommen und nicht etwa von einer anderen Person, die sich als der erwartete Absender ausgibt.

LINK TIPP

DsiN-Sicherheitscheck für Unternehmen

Der Onlinetest bietet einen leichten Einstieg zur Ermittlung des IT-Sicherheitsniveaus in Unternehmen. In wenigen Minuten erhalten Teilnehmer eine Auswertung mit passenden Handlungsempfehlungen.

https://www.dsin-sicherheitscheck.de

ANREGUNG

Überlegen Sie: Welcher der drei Aspekte der Informationssicherheit ist nicht erfüllt, wenn Unbefugte auf Kundendaten zugreifen können?

Persönliche Haftung von Geschäftsführern

Gemäß KonTraG: Unternehmen müssen über ein System zur frühzeitigen Erkennung von Risiken verfügen

Der Bereich der IT wird von zahlreichen Gesetzeswerken und sonstigen Bestimmungen direkt oder indirekt tangiert, so dass hier eine Aufzählung im Einzelnen nicht möglich ist. Stellvertretend sollen hier nur das Kontroll- und Transparenzgesetz (KonTraG) und das Bundesdatenschutzgesetz (BDSG) genannt werden. Gemäß KonTraG müssen Unternehmen über ein **System zur frühzeitigen Erkennung** von den Fortbestand des Unternehmens **bedrohenden Entwicklungen und Risiken** verfügen. Dies schließt unter anderem auch die Pflicht zur regelmäßigen Datensicherung ein. So hat nach einem Urteil des Oberlandesgerichts Hamm die **Sicherung der Unternehmensdaten** täglich und eine Vollsicherung mindestens einmal wöchentlich zu erfolgen.

TIPP

Sämtliche Daten täglich sichern!

Das BDSG legt unter anderem einen verschuldensunabhängigen Schadensersatzanspruch fest

Sind durch die mangelhafte IT-Sicherheit eines Unternehmens anderen Unternehmen Schäden – zum Beispiel in Form von Produktionsausfällen oder durch das Entwenden vertraulicher Informationen – entstanden, kann es von den Geschädigten auf **Schadensersatz** verklagt werden. Fahrlässig oder grob fahrlässig ist es bereits, wenn die Geschäftsführung den „Stand der Technik“ nicht einsetzt. Durch die neueren Gesetze ist dieser Stand der Technik gleichzusetzen mit dem Einsatz eines **Management-Systems für Informationssicherheit.**

Stand der Technik aus Sicht des Gesetzgebers: ein Management-System für Informationssicherheit.

Bei Verstößen gegen den Datenschutz legt § 7 S. 1 des Bundesdatenschutzgesetzes einen **verschuldensunabhängigen Schadensersatzanspruch** fest. Das bedeutet konkret, dass Unternehmen für alle Schäden verschuldensunabhängig und unbegrenzt haften, die sie Dritten durch die unzulässige bzw. falsche Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten zufügen.

TIPP

Die Bestimmungen des Bundesdatenschutzgesetzes umfassend berücksichtigen, da die darin festgelegten verschuldens-unabhängigen Schadenersatzansprüche ein besonders hohes Risiko darstellen.

Das Haftungsrisiko betrifft grundsätzlich nicht nur den unmittelbaren IT-Verantwortlichen, sondern auch die Geschäftsführer. Eine Ausnahme macht ein **Urteil des Bundesgerichtshofs (BGH)** für GmbH-Geschäftsführer und -Eigentümer. Für sie gilt – abgesehen von einem vorsätzlichen Verhalten – das **Prinzip der schadensersatzrechtlichen Innenhaftung**. Sie können deshalb nur von der GmbH selbst haftbar gemacht werden.

Um rechtliche Risiken für Unternehmen so weit wie möglich zu reduzieren, sollte die Nutzung **nicht lizensierter Software** durch Mitarbeiter konsequent unterbunden werden. Außerdem empfiehlt sich der Abschluss einer speziellen **IT-Haftpflichtversicherung** mit ausreichender Versicherungssumme zur Abdeckung eventueller Schadensersatzansprüche.

TIPP

Nutzung nicht lizensierter Software im Unternehmen unterbinden. Als Alternative Open-Source-Lösungen in Betracht ziehen.

LINK TIPP

Bundesdatenschutzgesetz – Text und Erläuterung (Ausgabe Juli 2017) als Download von der Bundesbeauftragten für den Datenschutz und die Informationssicherheit (BfDI):

http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO1.pdf?__blob=publicationFile&v=12

Datenschutz-Wiki der Ruhr-Universität Bochum und Bundesverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.:

https://www.datenschutz-wiki.de

ANREGUNG

Überlegen Sie: Worin besteht das Prinzip der sogenannten schadensersatzrechtlichen Innenhaftung für GmbH-Geschäftsführer und –Eigentümer?

Datenschutz-Grundverordnung und IT-Sicherheitsgesetz

Die EU-DS-GVO regelt im Grundsatz den Schutz und den freien Verkehr personenbezogener Daten

Im Rahmen der Nutzung von IT sind zahlreiche Gesetzeswerke zu beachten. Eine große Rolle dabei spielt die **europaweit gültige Datenschutz-Grundverordnung,** kurz **EU-DS-GVO**. Sie ist im Mai 2016 in Kraft getreten und nach einer Übergangsfrist von zwei Jahren von Mai 2018 an anzuwenden. Das Bundesdatenschutzgesetz (BDSG) wurde im April 2017 neu verabschiedet, um das deutsche Recht an die Vorgaben der EU-DS-GVO anzupassen.

Die DS-GVO fokussiert im Grundsatz auf den Schutz und den freien Verkehr personenbezogener Daten und definiert in diesem Zusammenhang u.a. konkrete Rechte für Unternehmen, den einzelnen Bürger sowie Arbeitnehmer und Arbeitgeber. Zudem enthält sie Vorgaben für den Transfer von personenbezogenen Daten in Staaten außerhalb der Europäischen Union sowie Vorschriften zu Bußgeld- und Sanktionsmöglichkeiten.

Die Datenschutz-Grundverordnung hat folgenden sachlichen Anwendungsbereich (Art. 2 DS-GVO):

> „Diese Verordnung gilt für die ganz oder teilweise automatisierte **Verarbeitung personenbezogener Daten** sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen“.

Wesentlich sind dabei die Begriffe der personenbezogenen Daten: Sind bei der Verarbeitung keine personenbezogenen Daten betroffen, greift die Verordnung nicht. Allerdings kann schon eine IP-Adresse, die bei der Kommunikation übertragen oder gespeichert wird, ein personenbezogenes Datum darstellen. Somit findet die Verordnung schon in diesen Fällen Anwendung.

Die EU-DS-GVO umfasst auch handschriftliche Akten und Aufzeichnungen

Während die automatisierte Verarbeitung Computer und Systeme betrifft (Server, Laptops, Kameras), bezieht sich die Verordnung bei der nichtautomatisierten Verarbeitung auf handschriftliche Aufzeichnungen. Nach Art 4 Nr. 6 DGSVO sind damit „Akten, Aktensysteme und Deckblätter erfasst“.

Marktortprinzip greift bei EU-DS-GVO

Die DS-GVO bringt hinsichtlich ihrer räumlichen Anwendung eine weitere Neuerung mit: Nach Art. 3. Abs. 2. gem. dem sogenannten **Marktortprinzip** müssen auch Unternehmen, die weder ihren Sitz noch eine Niederlassung in der Europäischen Union haben, sich an die Vorgaben der DS-GVO halten, und zwar dann, wenn ein Unternehmen sein Angebot auf den EU-Markt richtet und beispielsweise EU-Bürgern Waren oder Dienstleistungen entgeltlich oder unentgeltlich anbietet. Auch der Einsatz von Profiling- oder Tracking-Tools, um das Verhalten von Nutzern zu beobachten, fällt unter die Vorgaben der Verordnung.

ANREGUNG

Überlegen Sie, wofür die EU-DSGV bestimmt ist, und wie sie den Alltag in Betrieben beeinflusst.

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (**IT-Sicherheitsgesetz**) betrifft im Prinzip alle Betreiber kommerzieller Internetseiten, was bei den allermeisten Unternehmen der Fall ist. Es stellt bestimmte Mindestanforderungen an die technischen und organisatorischen Maßnahmen, die diese Unternehmen zum Schutz ihrer Kundendaten und ihrer IT-Systeme zu erfüllen haben. In seinem Rahmen werden außerdem die so genannten KRITIS-Verordnungen erlassen, die sich speziell an die Betreiber kritischer Infrastrukturen wie etwa Strom- und Wasserversorgungsunternehmen richten.

ANREGUNG

Überlegen Sie: An welche Zielgruppe richten sich die Bestimmungen des IT-Sicherheitsgesetzes?

LINK TIPP

Informationen zum IT-Sicherheitsgesetz des Bundesamts für Sicherheit in der Informationstechnik:

https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/it_sig_node.html

Datenschutzbeauftragte

Müssen ab neun Personen im Betrieb benannt werden.

Das Bundesdatenschutzgesetz (BDSG) schreibt einen **Datenschutzbeauftragten** in allen öffentlichen Stellen und Unternehmen vor, **sobald personenbezogene Daten wie Personal- und Kundendaten automatisiert verarbeitet werden**. Bei Unternehmen gilt diese Vorschrift in der Regel dabei erst, wenn **mehr als neun Personen** mit dieser Datenverarbeitung beschäftigt sind. Findet die Datenverarbeitung nicht automatisiert statt, greift die Vorschrift erst ab 20 Personen.

Der Beauftragte wirkt dabei auf die Einhaltung der entsprechenden Gesetze und Vorschriften hin und kontrolliert die ordnungsgemäße Anwendung von Datenverarbeitungsprogrammen. Der Betrieb muss **spätestens nach einem Monat** nach Aufnahme des entsprechenden Geschäftsbetriebs den Datenschutzbeauftragten bestellen. Bei Nichtbestellung liegt eine **Ordnungswidrigkeit** vor und kann mit einem **Bußgeld** von bis zu 50.000 Euro geahndet werden.

Weisungsfrei und unabhängig von Vorgesetzten.

Nötige Fachkunde und Zuverlässigkeit Voraussetzung.

Datenschutzbeauftrage in Betrieben besitzen kein **Weisungsrecht**, sind ihrerseits allerdings **weisungsfrei und unabhängig** von Vorgesetzten. Sie sind der Geschäftsleitung direkt unterstellt und berichten ihr. Datenschutzbeauftragte verfügen in der Regel über **gute IT-Kenntnisse und über Kenntnisse des BDSG**. Es existiert keine formale Ausbildung zum Datenschutzbeauftragten. Datenschutzbeauftragte müssen die **nötige Fachkunde und Zuverlässigkeit** mitbringen, und können an entsprechende Fort- und Weiterbildungen teilnehmen, um die Fachkunde zu erhalten. Die Zuverlässigkeit erfordert, dass es keinen Interessenkonflikt bei der Wahrnehmung der Funktion gibt; somit fallen Geschäftsführer und Abteilungsleiter als Datenschutzbeauftragte in der Regel raus.

LINK TIPP

Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz vom Düsseldorfer Kreis:

http://www.bfdi.bund.de/DE/Infothek/Entschliessungen/DuesseldorferKreis/functions/DKreis_table.html?nn=5217228

Die **Bundesbeauftragte für den Datenschutz und die Informationsfreiheit**:

https://www.bfdi.bund.de

2. ORGANISATORISCHE PRÄVENTION

Technisch-Organisatorische Maßnahmen

Um einen möglichst umfassenden Schutz der Unternehmens-IT bzw. der darin gespeicherten Informationen zu gewährleisten, sollte man diese Aufgabe nicht nur den Lösungen Firewall und Antiviren-Programm überlassen. In vielen **Soft- und Hardwareprodukten** sind herstellerseitig **verschiedene Schutzfunktionen** implementiert, die eine sinnvolle Ergänzung darstellen.

TIPP

Die gesamte Palette an verfügbaren Sicherheitsfunktionen/-tools auch tatsächlich nutzen.

Automatische Updates ergänzen die klassischen Schutzsystemen Firewall und das Antivirus-Programm

Darüber hinaus sollten bei allen Softwareprodukten und dem Betriebssystem die **automatischen Updates** aktiviert sein, um auch gegen das Auftreten neuer Bedrohungen bestmöglich geschützt zu sein. Nicht zuletzt empfehlen sich **regelmäßige vollständige Scans** von Netzwerk und Computer mit der Antiviren-Software, da deren Echtzeiterkennung manche Bedrohungen nicht sofort erkennen.

TIPP

Regelmäßige Systemscans mit der Antivirensoftware durchführen.

Das Sicherheitsniveau lässt sich außerdem dadurch erhöhen, dass alle Daten bzw. Informationen konsequent nur in **verschlüsselter Form** gespeichert werden.

TIPP

Sämtliche Daten nur in verschlüsselter Form speichern.

Passwörter aus mindestens zwölf Zeichen sowie Groß- und Kleinbuchstaben mit Ziffern und Sonderzeichen kombinieren

Eine weitere wichtige Präventionsmaßnahme ist die Festlegung ausreichend **sicherer Passwörter**. Passwörter bieten nach derzeitigem Stand der Technik eine hohe Sicherheit, wenn sie aus mindestens zwölf Zeichen bestehen sowie Groß- und Kleinbuchstaben mit Ziffern und Sonderzeichen kombinieren. Da sich mit längerer Nutzungsdauer eines bestimmten Passworts – unabhängig von der Komplexität – die Gefahr erhöht, dass es gehackt und missbraucht wird, sollten Passwörter regelmäßig geändert werden.

TIPP

Ausschließlich ausreichend sichere Passwörter verwenden und diese zudem regelmäßig ändern.

Weiterhin verbietet sich die Nutzung der **automatischen Speicher- und Vorgabefunktion** von Passwörtern und Benutzername bei einem Login – wie es mittlerweile viele Internetbrowser vorschlagen – von selbst. Denn auf diese Weise kann ein Unbefugter ohne Kenntnis des genauen Passworts in eigentlich geschützte Bereiche eindringen. Darüber hinaus ist auch der sicheren Hinterlegung von Passwörtern eine hohe Aufmerksamkeit zu schenken – das einfache Abspeichern im Klartext in einer Textdatei erfüllt diese Anforderung nicht.

TIPP

Passwörter grundsätzlich nur in verschlüsselter Form abspeichern.

Gleiches gilt für die **Dokumentation der genauen IT-Systemkonfiguration** und der einzelnen verwendeten **Sicherheitsmaßnahmen**. Eine solche Dokumentation sollte unbedingt erstellt werden, damit im Bedarfsfall auch andere Mitarbeiter IT-Sicherheitsaufgaben durchführen können.
Das Sicherheitsniveau lässt sich auch durch eine gezielte Vergabe von Rechten erhöhen. Dabei gilt der Grundsatz, dass jeder Anwender nur genau jene Bearbeitungs- und Zugriffsrechte haben sollte, die er für seine Arbeit tatsächlich benötigt.

TIPP

Bearbeitungsrechte für Daten auf das jeweils tatsächlich nötige Maß einschränken.

Als wichtige Präventionsmaßnahme empfiehlt sich der bereits im letzten Abschnitt erwähnte Abschluss einer speziellen **IT-Haftpflichtversicherung**, damit die **finanziellen Auswirkungen** eventueller Schadensersatzansprüche auf das Unternehmen zumindest abgefedert werden können. Und um einen eventuellen Datenverlust unbeschadet überstehen zu können, sollten eine **tägliche Datensicherung** – also das Anlegen von Backups – sowie deren testweise Wiederherstellung zu Prüfzwecken zur Routine gehören. So können die gesicherten Daten im Ernstfall auch tatsächlich in vollem Umfang und auf dem aktuellen Stand wiederhergestellt werden.

Was gern vergessen wird: Ausrangierte Datenträger wie CD-ROMs, USB-Sticks oder Festplatten dürfen nicht einfach weggeworfen werden, sondern sind auf eine **sichere Weise zu löschen** bzw. auf eine sichere Weise **unbrauchbar** zu machen. Um dies zu gewährleisten, sollten produktbezogene und detaillierte Vorschriften vorhanden sein.

TIPP

Die Datenvernichtung von in Unternehmen ausrangierten Datenträgern sollten durch entsprechend zertifizierte Anbieter vorgenommen werden.

LINK TIPP

Checkliste zu §9 Bundesdatenschutzgesetz (BDSG)

*„Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die **technischen und organisatorischen Maßnahmen** zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“*

https://www.datenschutz-wiki.de/Checkliste_Technische_und_organisatorische_Ma%C3%9Fnahmen

Fokus Mitarbeiter

Aufmerksame Mitarbeiter sind für ein Unternehmen sehr wertvoll und nehmen eine wichtige Rolle in der Sicherheitsfrage ein

Ganz wesentlich ist die Einstellung der **betroffenen Mitarbeiter**: Sie müssen unbedingt für die Belange der **IT-Sicherheit sensibilisiert** werden. Schließlich sind die besten Sicherheitsstrategien nutzlos, wenn sich die Mitarbeiter nicht an definierte Vorsorgemaßnahmen halten. Sind Daten mit externen Stellen auszutauschen, sollte unbedingt konkret geregelt werden, wer an welche externen Personen welche Daten auf welche Weise weitergeben darf.

Aufmerksame Mitarbeiter sind trotz aller mittlerweile technisch weit fortgeschrittenen Schutzfunktionen immer noch die beste Versicherung gegen Sicherheitsbedrohungen. Allerdings müssen sie dafür – regelmäßig – **geschult** werden, um ausreichende **Kompetenzen beim Umgang mit den Gefahren** der modernen vernetzten Welt zu entwickeln.
Dazu gehört zum Beispiel, dann misstrauisch zu werden, wenn sich ein PC ohne ersichtlichen Grund plötzlich komplett anders verhält. Dass Anhänge von E-Mails insbesondere unbekannter Absender ein besonders großes Sicherheitsrisiko darstellen, sollte ebenfalls bekannt sein. Die Erstellung als sicher geltender Passworte, der Umgang mit Firewall und Virenschutzprogramm sowie die Relevanz regelmäßiger Updates von Betriebssystemen und Anwenderprogrammen sind allesamt wichtige Themen für Mitarbeiterschulungen.

TIPP

Geschäftsführer sollten alle betreffenden Mitarbeiter durch entsprechende Schulungen befähigen, potenzielle Bedrohungen der Unternehmens-IT sicher erkennen zu können.

Um die dabei vorherrschend technischen Sachverhalte problemlos verstehen zu können, müssen außerdem die Bedeutungen bestimmter Fachbegriffe und Abkürzung wie etwa **VPN** (= virtuelles privates Netz), **WLAN** (steht für engl. „wireless local area network“) oder BIA (steht für engl. „**Business Impact Analyse**“ und bedeutet sinngemäß „Folgeschädenabschätzung“) bekannt sein.

ANREGUNG

Überlegen Sie: Welche Themen sollten in den IT-Sicherheitsschulungen für Mitarbeiter unbedingt besprochen werden?

LINK TIPP

Leitfaden Social Engineering:

https://www.sicher-im-netz.de/sites/default/files/download/leitfaden_social_engineering.pdf

Ernennung eines IT-Sicherheits-beauftragen im Unternehmen

Informationssicherheitsbeauftragte

Egal, ob Einzelunternehmen, kleiner Handwerksbetrieb oder mittelständisches Unternehmen – die Verantwortung für die Sicherheit der unternehmenseigenen IT muss eindeutig und personenbezogen geregelt sein. Hierzu wird in der Regel einen **Informationssicherheitsbeauftragten (IT-Sicherheitsbeauftragten)** benannt. Zu seinen/ihren Aufgaben gehören unter anderem die Erstellung einer unternehmensspezifischen **Leitlinie zur Informationssicherheit** und die Kontrolle über deren Umsetzung und Einhaltung. Außerdem fallen die Notfallvorsorge (Notfallhandbuch), die Analyse und die Nachbearbeitung von Informationssicherheitsvorfällen in seinen/ihren Kompetenzbereich. Nicht zuletzt fungiert der/die Informationssicherheitsbeauftragte auch als Ansprechpartner*in bei allen Fragen der IT-Sicherheit im Unternehmen.

TIPP

Die Verantwortlichkeiten können bei Bedarf auch auf mehrere Schultern verteilt werden. In diesem Fall sollte die Aufgabenteilung klar definiert sein.

ANREGUNG

Überlegen Sie: Welche Aufgaben hat ein Informationssicherheitsbeauftragter im Wesentlichen zu erfüllen?

LINK TIPP

Beispiel einer **Dienstanweisung** für den IT-Sicherheitsbeauftragten

http://t1p.de/td0i (PDF - Gekürzter Link zum Bundesamt für Sicherheit in der Informationstechnik BSI)

Sicherheitsrichtlinien im Unternehmen

Die Sicherheitsrichtlinie benennt die grundlegenden Sicherheitsziele eines Unternehmens

Die **Sicherheitsrichtlinie** beinhaltet als **Basisdokument** nur die grundlegenden Sicherheitsziele, die sich ein Unternehmen individuell setzt. Außerdem enthält sie organisatorische Informationen und gibt allgemeine Rahmenbedingungen vor. Letztendlich besteht ihr Sinn darin, den hohen Stellenwert der IT-Sicherheit im und für das Unternehmen deutlich zu machen.

Die Sicherheitsrichtlinie unterscheidet sich damit von der **Sicherheitsrichtlinie zur IT-Nutzung**, die für jedes in der Sicherheitsrichtlinie definierte allgemeine Ziel **konkrete Inhalte** formuliert. Daraus leiten sich dann wiederum weiter spezialisierte Richtlinien und sonstige Anweisungen ab, die dann unter anderem auch durchzuführende Maßnahmen vorgeben.

Die Sicherheitsrichtlinie wird in der Regel vom **IT-Sicherheitsbeauftragten** angefertigt und gegebenenfalls mit der Geschäftsführung abgestimmt. Das Vorgehen zur Erstellung der Leitlinie kann dabei wie folgt sein: 1. Festhalten der Gesamtverantwortung der Geschäftsleitung für die gesamtbetriebliche Informationssicherheit; 2. Festlegen des Geltungsbereichs und des Inhalts; 3. Einberufen einer Entwicklungsgruppe; 4. Bekanntgeben der Leitlinie; 5. Aktualisieren der Leitlinie.

LINK-TIPP

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet Musterrichtlinien an:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/hilfmi/muster/musterrichtlinien/musterrichtlinien.html

ANREGUNG

Überlegen Sie: Worin liegt der Unterschied zwischen der Sicherheitsrichtlinie eines Unternehmens und der Sicherheitsrichtlinie zur IT-Nutzung?

3. SCHUTZ VOR WIRTSCHAFTSSPIONAGE

Auch KMU können Ziel von Wirtschafts-spionage werden und sollten sich dagegen schützen

Nahezu alle Unternehmen haben Informationen in elektronischer Form gespeichert, die für Wettbewerbsunternehmen prinzipiell von Interesse sein können. Darunter können auch auf den ersten Blick unscheinbare Dokumente wie etwa Lieferverträge sein, aus denen individuelle Lieferbedingungen, Kalkulationsfaktoren und Zahlungskonditionen ersichtlich sind. Solche Informationen über den Wettbewerber können schnell Vertragsverhandlungen mit dem Lieferanten beeinflussen.

TIPP

Schutzmaßnahmen gegen Wirtschaftsspionage sind grundsätzlich in Unternehmen aller Größen sinnvoll.

Angriffe von innen und außen

Dieses einfache Beispiel zeigt, dass es grundsätzlich auch für scheinbar uninteressante Angriffsziele wie kleine Handwerksbetriebe sinnvoll ist, sich gegen Wirtschaftsspionage zu schützen. Bei der konkreten Umsetzung sind zwei verschiedene Szenarien zu unterscheiden: **Spionageangriffe von innen** und von **außerhalb**. Während Zugriffsversuche von außen prinzipiell durch **Sicherheitssysteme** wie etwa eine Firewall erkannt bzw. verhindert werden können, ist der Schutz gegen Innentäter – dazu zählt auch vorübergehend im Unternehmen tätiges Fremdpersonal – deutlich eingeschränkt. Das liegt vor allem in ihren möglichen Kenntnissen über vorhandene Sicherheitsvorkehrungen sowie ihren eventuell vorhandenen Zugangs- bzw. Zugriffsberechtigungen begründet. Mögliche Ansatzpunkte sind die **Sicherung von Räumen und/oder Gebäuden** gegen unbefugten Zutritt sowie die **Verschlüsselung** von elektronisch gespeicherten Daten.

TIPP

Die Verschlüsselung aller gespeicherten Daten bietet selbst dann noch einen gewissen Schutz, wenn die Daten selbst bereits entwendet wurden.

Im ersten Fall lässt sich verhindern oder zumindest erschweren, dass sich Beschäftigte Zugang zu einem PC-Arbeitsplatz in einer anderen Abteilung verschaffen, für die sie nicht arbeiten. Der zweite Fall entfaltet dann eine Schutzwirkung, wenn sich zwar jemand Zugang zu einem fremden Arbeitsplatz verschaffen und von dort Daten erfolgreich entwenden konnte, diese aber anschließend aufgrund der Verschlüsselung nicht lesen kann.

ANREGUNG

Aufgabe: Erarbeiten Sie eine Liste an Abwehrmaßnahmen für die Wirtschaftsspionage durch Innentäter.

Zusammenarbeit mit Externen

Bei der Nutzung des Internets sowie dem Austausch mit anderen Organisationen ist jederzeit Vorsicht geboten

Besondere Bedeutung hat das Thema Informationssicherheit auch beim Datenaustausch mit anderen Unternehmen, Behörden und sonstigen Organisationen. Denn in diesem Fall verlassen die unternehmenseigenen Daten den (geschützten) internen Bereich und müssen über das allen offen stehende und damit entsprechend risikobehaftete Internet zum jeweiligen Empfänger transportiert werden.
Aus diesem Grund sollten Daten grundsätzlich nur in **verschlüsselter Form gesendet** werden. Geschieht die Datenübertragung mittels Upload auf eine Internetseite oder ein Cloud-Laufwerk, ist zusätzlich noch auf eine **gesicherte Verbindung** – erkennbar an der Webadresse „https://...“ – zu achten.

TIPP

Daten grundsätzlich nur in verschlüsselter Form an Dritte versenden.

Beim Empfang von Daten sollte man sich vergewissern, ob sie tatsächlich vom behaupteten Absender stammen. Ergeben sich dabei Zweifel, besser beim Absender telefonisch nachfragen. Denn eine E-Mail-Absenderadresse lässt sich schon auf einfache Weise fälschen, kann aber bei Verwendung eines bereits bekannten Namens trotzdem vertrauenswürdig aussehen.

TIPP

Grundsätzlich alle eingehenden E-Mails mit Anhang auf Echtheit prüfen.

Da in solchen Fällen E-Mail-Anhänge vom Empfänger oft bedenkenlos geöffnet werden, besteht hier ein besonders hohes Risiko, sich Schadsoftware einzufangen. Dies trifft insbesondere auf kleine und mittlere Unternehmen zu, da hier der Datenaustausch per E-Mail-Anhang – zum Beispiel für Rechnungsdokumente oder als Angebotsbeschreibungen – wegen seiner unkomplizierten Handhabung sehr weit verbreitet ist.

ANREGUNG

Überlegen Sie: In welchem Fall öffnen Empfänger von E-Mails angehängte Dokumente in der Regel bedenkenlos?

LINK-TIPP

Initiative Wirtschaftsschutz vom Bundesamt für Verfassungsschutz, Bundeskriminalamt, Bundesnachrichtendienst und Bundesamt für Sicherheit in der Informationstechnik:

https://www.wirtschaftsschutz.info

QUIZ Q7

(Mehrfachnennung möglich)

Sie können das folgende Quiz alternativ auch in Form eines Online-Spiels direkt auf ihrem Smartphone oder Computer durchführen.

Das Online-Quiz ist verfügbar auf der Bottom-Up-Webseite: https://www.dsin-berufsschulen.de/unsere-online-quiz.

1. Welche Aspekte fasst man unter dem Begriff „Informationssicherheit“ zusammen?

A Verfügbarkeit, Einsehbarkeit und Integrität von Informationen.
B Vertraulichkeit, Verfügbarkeit und die Integrität von Informationen.
C Unversehrtheit, Uneinsehbarkeit und Unantastbarkeit von Informationen.

2. Welche Standardlösungen für die IT-Sicherheit sollten auf keinem PC/Laptop bzw. in keinem Netzwerk fehlen?

A BIOS
B Firewall
C Antivirensoftware

3. Welches nachfolgende Beispiel widerspricht klar der Forderung nach einer möglichst sicheren Hinterlegung von Passwörtern?

A Abspeichern im Klartext in einer Textdatei.
B Hinterlegung nur in schriftlicher (nicht-elektronischer) Form.
C Per E-Mail selber zugesandt.

4. Was regelt die EU-Datenschutz-Grundverordnung?

A Den genauen Datenaustausch zwischen einem Unternehmen sowie Kund*innen und Lieferant*innen.
B Den Schutz und den freien Verkehr personenbezogener Daten innerhalb der Europäischen Union.
C Das Surfen auf Internetseiten der Europäischen Union.

5. Welche Aussagen treffen auf den/die Datenschutzbeauftragte/n zu?

A Unternehmen müssen eine/n Datenschutzbeauftragten einstellen, sobald mehr als neun Mitarbeiter*innen mit der Datenverarbeitung zu tun haben.
B Der/die Datenschutzbeauftragte haben ein Weisungsrecht gegenüber der Abteilungsleitung/Geschäftsführung.
C Der/die Datenschutzbeauftragte sind weisungsfrei von der Abteilungsleitung/Geschäftsführung.

6. Auf welche beiden Angriffsszenarien bezüglich Wirtschaftsspionage muss sich ein Unternehmen prinzipiell einstellen?

A Auf Angriffe durch Software und Angriffe durch Hardware.
B Auf Entwendung von Hardware wie Festplatten und auf die Entwendung elektronisch gespeicherter Daten.
C Auf Angriffe von außen und auf Angriffe durch Innentäter*innen.

7. Gemäß Kontroll- und Transparenzgesetz (KonTraG) müssen Unternehmen über ein System zur frühzeitigen Erkennung von den Fortbestand des Unternehmens bedrohenden Entwicklungen und Risiken verfügen. Welche wichtige Pflicht ergibt sich daraus?

A Alle Mitarbeiter*innen monatlich über neu aufgetretene Bedrohungssoftware schulen.
B Ein externes Unternehmen mit der Betreuung der eigenen IT zu beauftragen.
C Eine tägliche Datensicherung durchzuführen.

8. Welche sinnvollen Maßnahmen können Unternehmen ergreifen, um rechtliche Risiken zu reduzieren?

A Die Nutzung nicht lizenzierter Software durch Mitarbeiter*innen konsequent unterbinden.
B Den Einsatz von IT auf ein Minimum reduzieren.
C Eine IT-Haftpflichtversicherung mit ausreichender Versicherungssumme abschließen.

9. Welcher Aspekt der Informationssicherheit ist nicht erfüllt, wenn elektronisch gespeicherte Daten durch einen Hardwarefehler nicht gelesen werden können?

A Verfügbarkeit
B Unversehrtheit
C Einsehbarkeit

10. Wie sollte mit ausrangierten Datenträgern aus Sicherheitsgründen umgegangen werden?

A Sie können nach dem Löschen der Daten zum Verkauf angeboten werden.
B Sie sind auf jeden Fall auf eine sichere Weise zu löschen bzw. auf eine sichere Weise unbrauchbar zu machen.
C Man kann auf das sichere Löschen verzichten, wenn die Datenträger anschließend nur an Firmenmitarbeiter*innen verschenkt werden.

11. Was besagt das Marktortprinzip?

A Auf einem digitalen Marktplatz müssen sich alle Anbieter*innen an die Datenschutzregeln ihres jeweiligen Landes halten.

B Ein/e Betreiber*in eines Online-Shops braucht eine physische Filiale in den Ländern, wo er online Handel betreiben will.

C Unternehmen außerhalb der EU sind verpflichtet sich an die EU Datenschutz-Grundverordnung zu halten, wenn sich ihr Angebot an Kunden in der EU richtet.

Lösung: 1 B, 2 B+C, 3 A+C, 4 B, 5 A+C, 6 B+C 7 C, 8 A+C, 9 A, 10 B, 11 C

FRAGEBOGEN: WAS IST INFORMATIONSSICHERHEIT?

ARBEITSBOGEN

Arbeitsauftrag

1. Ordnen Sie durch Einzeichnen von Linien den aufgeführten Definitionen die jeweils korrekte Erklärung zu.
2. Bearbeiten Sie anschließend Aufgabe 1 bis 4.

Definition	Erklärung
Vertraulichkeit	In diesem Rahmen gilt es, alle Informationen vor unbefugten Zugriffen zu schützen.
Verfügbarkeit	Dieses Kriterium ist dann erfüllt, wenn der Inhalt der Informationen nicht verfälscht wurde.
Integrität	Bei auf elektronischem Wege übertragenen Informationen ist es wichtig, sicherzustellen, dass die Daten/Informationen auch tatsächlich von der als Absender benannten Stelle kommen.
Authentizität	Dieser Begriff bedeutet, alle Informationen und die nötige Technik immer dann nutzbar bzw. einsatzbereit zu halten, wenn sie gebraucht werden.

1. **Welcher der drei grundlegenden Aspekte der Informationssicherheit ist nicht erfüllt, wenn Unbefugte auf Kundendaten zugreifen können?**

---

2. **Ihr/e Chef*in sagt Ihnen, dass bestimmte Informationen nicht integer sind. Was schließen Sie daraus?**

   A Die Informationen stammen in Wirklichkeit von einem anderen Absender als behauptet.

   B Die Vertraulichkeit dieser Informationen ist nicht mehr gegeben.

   C Der Inhalt dieser Informationen wurde wahrscheinlich gefälscht.

   D Diese Informationen sind nur eingeschränkt verfügbar.

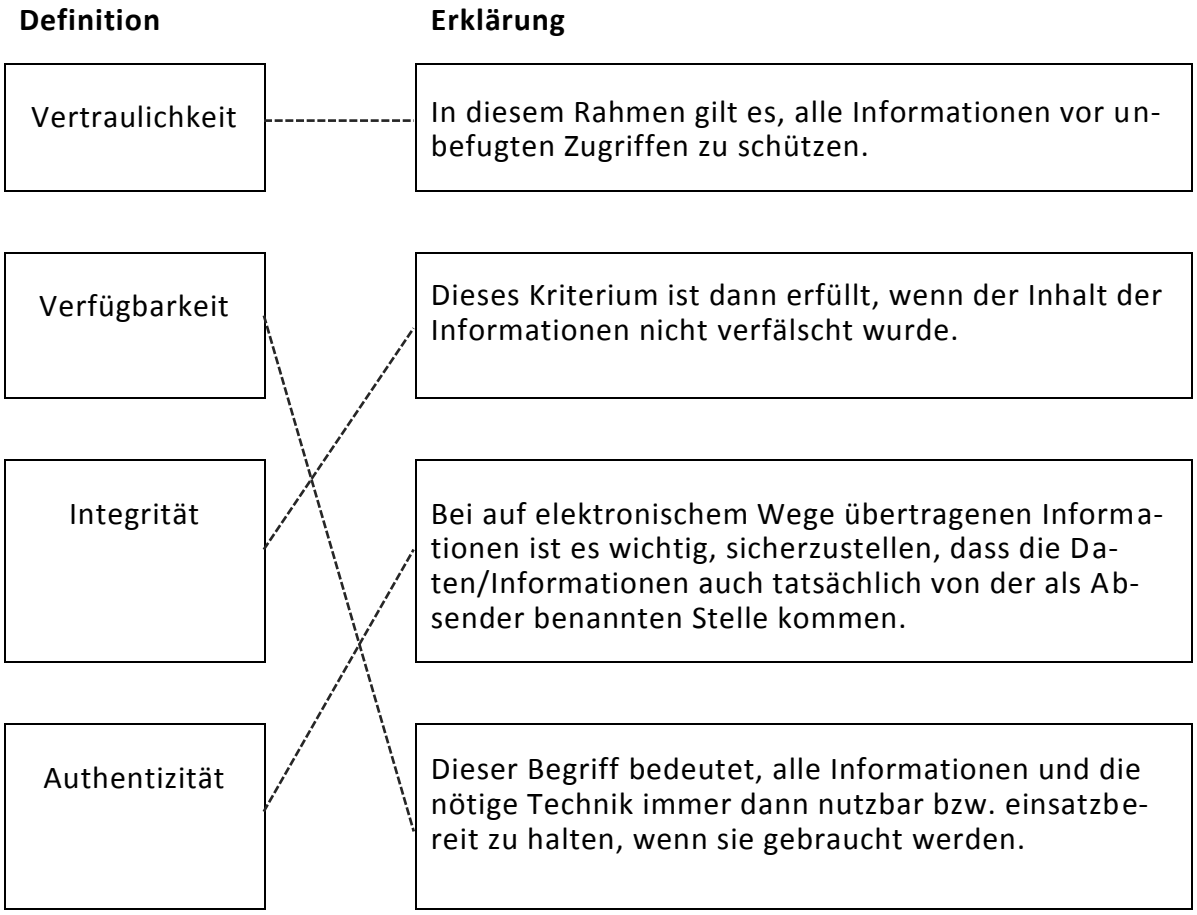
3. **Nennen Sie ein Beispiel für nicht-authentische Informationen**

---

4. **Informationssicherheit gilt allgemein als gewährleistet, wenn drei bestimmte Kriterien erfüllt sind. Welche drei Kriterien sind hier gemeint?**

FRAGEBOGEN: WAS IST INFORMATIONSSICHERHEIT?

LÖSUNG



1. Welcher der drei grundlegenden Aspekte der Informationssicherheit ist nicht erfüllt, wenn Unbefugte auf Kundendaten zugreifen können?

Die Vertraulichkeit

2. Ihr/e Chef*in sagt Ihnen, dass bestimmte Informationen nicht integer sind. Was schließen Sie daraus?

C Der Inhalt dieser Informationen wurde wahrscheinlich gefälscht.

3. Nennen Sie ein Beispiel für nicht-authentische Informationen

Der/die Absender*in der betreffenden Informationen hatte in Wirklichkeit eine andere Identität als angegeben.

4. Informationssicherheit gilt allgemein als gewährleistet, wenn drei bestimmte Kriterien erfüllt sind. Welche drei Kriterien sind hier gemeint?

Vertraulichkeit, Verfügbarkeit und Integrität

BOTTOM-UP:
BERUFSSCHÜLER FÜR IT-SICHERHEIT

hat zum Ziel, die Mitarbeiter von morgen bereits während der dualen Ausbildung auf die Herausforderungen des digitalen Arbeitsalltags im Hinblick auf IT-Sicherheit und Schutz von Daten vorzubereiten. Damit leistet Bottom-Up einen wichtigen Beitrag zu mehr IT-Sicherheit in kleinen und mittelständischen Unternehmen.

www.dsin-berufsschulen.de

Bottom-Up ist ein Angebot von

Deutschland sicher im Netz e.V.
Albrechtstraße 10
10117 Berlin

www.sicher-im-netz.de

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Im Rahmen der Initiative:

IT-Sicherheit IN DER WIRTSCHAFT

Ein Projekt von:

Deutschland sicher im Netz

Initiative „IT-Sicherheit in der Wirtschaft“ Die Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie will vor allem kleine und mittlere Unternehmen beim sicheren Einsatz von IKT-Systemen unterstützen. Gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung soll eine Grundlage dafür geschaffen werden, um die Bewusstseinsbildung in der digitalen Wirtschaft beim Thema IT-Sicherheit im Mittelstand zu stärken. Unternehmen sollen durch konkrete Unterstützungsmaßnahmen dazu befähigt werden, ihre IT-Sicherheit zu verbessern. Weitere Informationen zur Initiative und ihren Angeboten sind unter: **www.it-sicherheit-in-der-wirtschaft.de** abrufbar.