Baden-Württemberg
MINISTERIUM FÜR INNERES, DIGITALISIERUNG UND MIGRATION

Sicherheitsforum Baden-Württemberg
Die Wirtschaft schützt ihr Wissen

IT-Sicherheitskonzept

Handlungsempfehlungen für kleine und mittlere Unternehmen

Dieses IT-Sicherheitskonzept wurde erstellt durch ein Konsortium aus Goldmedia GmbH Strategy Consulting und dem Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule, Gelsenkirchen. Es wurde unter der Leitung von Prof. Norbert Pohlmann sowie den Studienautoren Johnny Hoang, Arbnor Memeti und Sandra Michalik im Zeitraum zwischen September 2018 und August 2019 erarbeitet.

Das Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg und das Sicherheitsforum Baden-Württemberg haben im Sommer 2018 dem Konsortium aus Goldmedia GmbH Strategy Consulting und dem Institut für Internet-Sicherheit - if(is) der Westfälischen Hochschule, Gelsenkirchen, den Auftrag zur Durchführung einer Studie zur Analyse von Gefährdungen in Unternehmen durch Ausspähungen, Know-how-Abflüsse und Datenmanipulation in baden-württembergischen Unternehmen erteilt.

Aus den Erkenntnissen der Studie wurde daraufhin ein IT-Sicherheitskonzept für kleine und mittlere Unternehmen erstellt, um diesen Handlungsempfehlungen zum Schutz vor Ausspähungen, Know-how-Abflüssen und Datenmanipulationen zu geben.

Genderhinweis: Aus Gründen der besseren Lesbarkeit wird im Text auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für beiderlei Geschlecht. Dies impliziert keine Benachteiligung des weiblichen Geschlechts, sondern ist im Sinne der sprachlichen Vereinfachung als geschlechtsneutral zu verstehen.

Inhalt

Abbildungen

1 Einleitung

Der ungewollte Abfluss von Informationen kann den wirtschaftlichen Erfolg eines Unternehmens erheblich beeinträchtigen oder sogar existenzbedrohend sein. Insbesondere kleine und mittelständische Unternehmen (KMU) mit innovativen Produkten oder Dienstleistungen bieten ein potenzielles Angriffsziel für Wirtschaftsspionage und Konkurrenzausspähung.

Laut der „SiFo-Studie 2018/2019 – Gefährdungen in baden-württembergischen Unternehmen durch Ausspähungen, Know-how-Abflüsse und Datenmanipulationen" haben in den letzten vier Jahren (2015-2018) rund 16 Prozent der befragten Unternehmen in Baden-Württemberg angegeben, Vorfälle oder Verdachtsfälle von unbefugten Zugriffen auf schützenswerte Daten des Unternehmens gehabt zu haben. Allerdings können 36 Prozent der Unternehmen die Anzahl der Vorfälle und Verdachtsfälle nicht beziffern, da es ihnen in der Regel an geeigneter Netzwerküberwachungstechnik fehlt. Angriffe werden daher häufig zu spät oder gar nicht erkannt.

Um sich Zugang zu verschaffen, haben die Angreifer sowohl menschliche als auch technische Angriffsvektoren genutzt. Rund 39 Prozent gaben an, dass Unbefugte durch digitalen Identitätsdiebstahl Zugriff auf schützenswerte Daten erlangten. Bei weiteren rund 36 Prozent erhielten Angreifer Zugriff auf schützenswerte Daten, indem sie die digitale Kommunikation des Unternehmens abgefangen oder mitgeschnitten hatten. Für Unternehmen besteht eine ständige Gefahr, durch Wirtschaftsspionage und Konkurrenzausspähung einen Schaden zu erleiden. Jedoch können geeignete IT-Schutzmaßnahmen das Risiko reduzieren.

Eine weitere Erkenntnis der SiFo-Studie 2018/2019 war, dass ein Großteil der befragten Unternehmen (ca. 69 Prozent) den Wunsch nach Leitfäden zur IT- und Unternehmenssicherheit als Unterstützungsangebot geäußert haben. Dieses IT-Sicherheitskonzept stellt deshalb Maßnahmen und Lösungsansätze vor, um Informationssicherheit in Unternehmen aufzubauen und zu steigern.

Was sind Informationen?

Informationen, ob digital oder analog, sind Unternehmenswerte, die für den Geschäftsbetrieb von Unternehmen und Organisationen eine zentrale Rolle spielen. Schützenswerte Informationen sind nicht nur Patente, Forschungsergebnisse und Betriebsgeheimnisse. Auch Kunden- oder Personaldaten sowie Informationen über verwendete technische Systeme und Informationen über verwendete Anlagen sind schützenswerte Informationen. Und diese immateriellen Unternehmenswerte müssen mindestens so gut gesichert werden, wie die materiellen Werte eines Unternehmens.

Um Informationen effizient schützen zu können, müssen diese nach ihrem Schutzbedarf klassifiziert werden. Schutzbedarfs- und Risikoanalysen helfen bei der Klassifizierung von Informationen. Das Ziel von Schutzbedarfs- und Risikoanalysen ist es zu identifizieren, welche Unternehmenswerte essenziell für das Unternehmen sind. Sie helfen dadurch bei der Ermittlung geeigneter IT-Maßnahmen für einen angemessenen Schutz. So kann bspw. die Unterteilung der Informationen in Schutzklassen sich am Ausmaß der Schäden orientieren, der bei einem Informationsabfluss verursacht werden könnte.

Informationssicherheit verfolgt die Zielsetzung der sicheren Aufbewahrung, des sicheren Austauschs und der sicheren Verarbeitung von Informationen. Daher unterscheidet man bei der Informationssicherheit auch grundsätzlich diese drei primären Schutzziele der Informationssicherheit: **Vertraulichkeit, Integrität und Verfügbarkeit**.

Was unterscheidet ein IT-Sicherheitskonzept von einem Informationsschutzkonzept?

Grundlegend besteht ein umfassendes Informationsschutzkonzept aus mehreren Bereichen, in denen Anweisungen und Richtlinien niedergelegt sind, damit Informationen überhaupt erst als schützenswerte Unternehmenswerte gelten können.

Hierzu zählen:

- **der personelle Bereich** (z.B. Auswahl, Betreuung und Schulung von Mitarbeitern)
- **der technische Bereich** (z.B. physische Objektsicherheit für das Firmenareal, Gebäude, Räume oder einzelne Objekte)
- **organisatorischer Bereich** (z.B. sicherheitskritische Verfahren und Anweisungen für Geschäftsreisen, Besucherverkehr oder auf Messen)
- **den IT-Bereich** (konkrete IT-Sicherheitsmaßnahmen)
- **der rechtliche Bereich** (z.B. Geheimhaltungsvereinbarungen mit Angestellten und Geschäftspartnern)

Das vorliegende IT-Sicherheitskonzept legt den Fokus auf den IT-Bereich und die IT-Sicherheit und ist demensprechend überwiegend auf IT-Sicherheitsmaßnahmen ausgerichtet. Zusätzlich wurden ausgewählte personell-organisatorische Maßnahmen als Folge der Erkenntnisse aus der SiFo-Studie 2018/2019 in das IT-Sicherheitskonzept aufgenommen, um auch im organisatorischen Vorgehen eine erste Hilfestellung zu leisten. Für tiefergehende Informationen und Schutzmaßnahmen müssen weitere Quellen herangezogen werden. Dazu dienen die Angaben am Ende eines jeden Kapitels.

In den einzelnen Kapiteln ist jeweils eine Übersichtstabelle mit Schutzmaßnahmen zu finden. Durch Ausfüllen der Tabellen können Sie überprüfen, ob Ihr Unternehmen ausreichend Maßnahmen für den Informationsschutz ergriffen hat und in welchen Bereichen noch nachgebessert werden kann.

Das Häkchen steht in diesem Zusammenhang für „**bereits vorhanden**“**,** der Kreis für „**teilweise vorhanden**“ und das Kreuz für „**nicht vorhanden**“.

Legende	
Ist bereits vorhanden	
Ist nur teilweise vorhanden	
Ist nicht vorhanden	

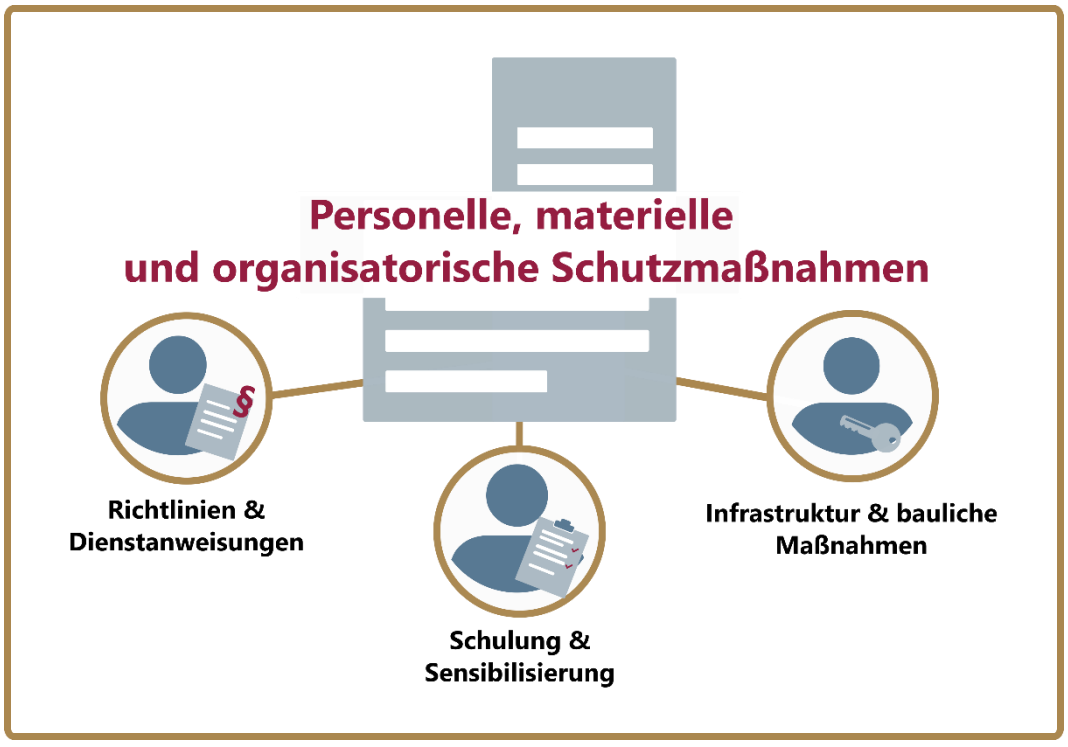
2 Personelle, materielle und organisatorische Schutzmaßnahmen

Personelle, materielle und organisatorische Maßnahmen zum Schutz der Informationssicherheit betreffen in erster Linie das Personal, Gebäude- und Geländesicherung sowie Verfahren und Prozesse des Unternehmens. Nur mit einer effizienten Sicherheitsstrategie und einer hohen Sicherheitskultur unter den Mitarbeitern kann ein funktionierendes Informationssicherheitsmanagement geschaffen und kontinuierlich weiterentwickelt werden.

Die organisatorischen Maßnahmen durchdringen die Organisationsstruktur des Unternehmens und haben direkten Einfluss auf das Personal und die Prozesse. Der sichere Umgang mit vertraulichen Informationen muss dem Personal beigebracht werden. Mithilfe von regelmäßigen Schulungen und Informationssicherheitsrichtlinien lernt das Personal den richtigen Umgang mit vertraulichen Informationen und IT-Sicherheitsmaßnahmen.

Zusätzlich müssen auch bauliche Maßnahmen umgesetzt werden, um das Firmengelände oder Gebäude gegen Unbefugte zu sichern. Zudem müssen Prozesse mit dem Ziel optimiert werden, weniger Angriffsfläche für Wirtschaftsspionage und Konkurrenzausspähung zu bieten.

Abb. 1: Personelle, materielle und organisatorische Schutzmaßnahmen



2.1 Erstellung von Richtlinien und Dienstanweisungen

In jedem Unternehmen müssen Richtlinien und Dienstanweisungen zur Wahrung der Informationssicherheit konzipiert werden, die für alle Mitarbeiter verpflichtend sind. Nur wenn Mitarbeiter verbindliche und verständliche Vorgaben für die Nutzung und Sicherheit von schützenswerten Unternehmenswerten erhalten, diese verstehen und auch umsetzen können, kann das die Gefahren durch Wirtschaftsspionage und Konkurrenzausspähung deutlich reduzieren. Die Leitung des Unternehmens ist dafür verantwortlich, dass die Einhaltung der Regelungen sichergestellt wird. Zudem ist es unabdingbar, Richtlinien und Dienstanweisungen regelmäßig auf ihre Aktualität hin zu überprüfen.

Abb. 2: Richtlinien und Dienstanweisungen

Die **wesentlichen Maßnahmen zu Richtlinien und Dienstanweisungen** stehen in der folgenden Überblickstabelle:

Personell-organisatorische Richtlinien	✓ ○ ✗
Ernennung eines Informationsschutzbeauftragten (ISB), der für die Belange der Informationssicherheit im Unternehmen zuständig ist.	☐ ☐ ☐
Mitarbeiter erhalten ausschließlich Zugänge und Benutzerrechte, die sie für ihre Aufgabenbewältigung benötigen.	☐ ☐ ☐
Der Umgang mit vertraulichen Informationen ist für das Personal klar und verständlich in Sicherheitsrichtlinien definiert (Zugriff, Bearbeitung, Aufbewahrung, Vervielfältigung).	☐ ☐ ☐
Die Sicherheitsrichtlinien berücksichtigen die Planung und Umsetzung von Schulungs- und Sensibilisierungsprogrammen für das Personal.	☐ ☐ ☐
Sicherheitsrichtlinien für Auslandsreisen (z.B. verschlüsselte Kommunikation und Datenspeicherung, dedizierte Reise-Hardware, eingeschränkte Zugangsrechte).	☐ ☐ ☐
Es sind Notfallmaßnahmen und Verhaltensregeln bei einem Sicherheitsverstoß definiert (z.B. Sperrung der Zugangsberechtigungen).	☐ ☐ ☐

Der Zugang zu vertraulichen Informationen ist für Fremdpersonal reguliert (z.B. Vertraulichkeitsvereinbarungen, eingeschränkte Zugangsmöglichkeiten, zeitlich begrenzter Zugang).	☐ ☐ ☐
Es sind Richtlinien für die Zusammenarbeit mit externen Dienstleistern, Fremdfirmen oder Lieferanten definiert worden (z.B. Zugriff und Austausch von vertraulichen Informationen).	☐ ☐ ☐
Fremdpersonal und externe Parteien werden bei den Schulungs- und Sensibilisierungsprogrammen berücksichtigt.	☐ ☐ ☐
Technische Richtlinien	✓ ○ ✗
Es existieren Sicherheitsrichtlinien für die betriebliche Nutzung von privaten Endgeräten (BYOD).	☐ ☐ ☐
Vertrauliche Kommunikation muss durch kryptografische Maßnahmen gesichert sein (z.B. verschlüsselte E-Mail).	☐ ☐ ☐
Einrichtung eines sicheren Zugriffsschutzes, um Geräte vor unbefugter Nutzung zu schützen (z.B. Passwortregelungen, Bildschirmsperren).	☐ ☐ ☐
Regelungen für die sichere Weitergabe und Ausmusterung von Geräten und Speichermedien.	☐ ☐ ☐
Maßnahmen beim Verlust oder Diebstahl von mobilen Endgeräten oder Speichermedien (z.B. Sperrung der Zugangsberechtigungen, Fernlöschung der Daten).	☐ ☐ ☐
Regelmäßige Sicherung von relevanten Informationen (Backups).	☐ ☐ ☐
Es gibt einen Aktualisierungszyklus für das Einspielen von aktuellen Sicherheitspatches/-updates für Anwendungsprogramme, Betriebssysteme und Treiber.	☐ ☐ ☐

Weiterführende Links zum Thema Erstellung von Richtlinien und Dienstanweisungen:

- **BSI - CON.7: Informationssicherheit auf Auslandsreisen**
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/BS_Auslandsreisen.pdf?__blob=publicationFile&v=12
- **BSI - OPS.3.1 Outsourcing für Dienstleister**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_3_1_Outsourcing_f%C3%BCr_Dienstleister.html
- **Wirtschaftsgrundschutz - Baustein MA1 - Reisesicherheit**
  https://www.wirtschaftsschutz.info/DE/Veroeffentlichungen/Wirtschaftsgrundschutz/Bausteine/Reisesicherheit.pdf?__blob=publicationFile&v=4

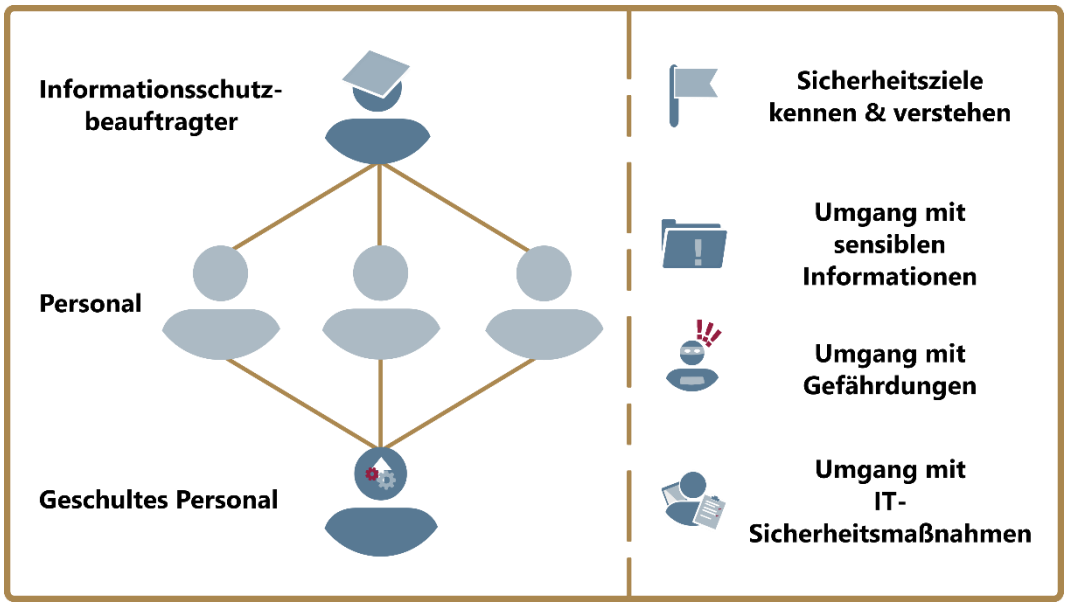
2.2 Schulung und Sensibilisierung der Mitarbeiter

Der Aufbau eines starken Sicherheitsbewusstseins und einer Sicherheitskultur innerhalb eines Unternehmens oder einer Institution hängt maßgeblich von der Integration der Mitarbeiter in das Sicherheitskonzept ab. Mitarbeitern ist oft nicht bewusst, welche Konsequenzen die Sorglosigkeit im Umgang mit vertraulichen Informationen, die Nichtbeachtung von Regelungen der Informationssicherheit oder Sicherheitslücken mit sich bringen. Dies schließt insbesondere die Unternehmensführung mit ein. Dementsprechend muss das gesamte Personal durch regelmäßige Schulungen mit den Sicherheitszielen und Werten des Unternehmens vertraut gemacht und die nötigen Kernkompetenzen vermittelt werden. Gleichermaßen entscheidend ist die kontinuierliche Sensibilisierung der Mitarbeiter gegenüber Cybergefährdungen. Schulungen und Sensibilisierung sollten sich ergänzen.

- **Schulungen** vermitteln den Mitarbeitern die nötigen Kenntnisse und Kompetenzen im Umgang mit IT-Sicherheitsmaßnahmen und vertraulichen Informationen.
- Eine **Sensibilisierung** der Mitarbeiter erhöht deren Wahrnehmung gegenüber den Gefahren durch Cyberbedrohungen wie Social Engineering.

Im Rahmen der SiFo-Studie 2018/2019 wurde deutlich, dass zwar etwas mehr als die Hälfte der befragten Unternehmen Mitarbeiterschulungen zum Schutz von Geschäftsgeheimnissen durchführen. Jedoch dürfte der Anteil der befragten Unternehmen, die nicht nur einmalig, sondern regelmäßig Mitarbeiterschulungen durchführen, deutlich geringer ausfallen.

Abb. 3: Schulung und Sensibilisierung



Die **wesentlichen Maßnahmen zur Schulung und Sensibilisierung** der Mitarbeiter stehen in der folgenden Überblickstabelle:

Organisatorische Planung	
Der Informationsschutzbeauftragte ist für die Planung und Umsetzung verantwortlich (z.B. ggf. externe Anbieter kontaktieren, Zeitplanung).	
Mitarbeiter erhalten einmalig Schulungs- und Sensibilisierungsmaßnahmen (bspw. zu Beginn des Arbeitsverhältnisses).	
Schulungsmaßnahmen für Mitarbeiter werden in regelmäßigen Abständen durchgeführt (z.B. quartalsweise).	
Sensibilisierungsmaßnahmen für Mitarbeiter werden in regelmäßigen Abständen abgehalten und ggf. durch qualifizierte externe Dienstleister durchgeführt (z.B. durch das Landesamt für Verfassungsschutz Baden-Württemberg).	
Schulungs- und Sensibilisierungsinhalte werden regelmäßig auf aktuelle Sicherheitsmaßnahmen und Cyberbedrohungen angepasst (z.B. nach Bekanntwerden einer Sicherheitslücke).	
Inhalte der Schulungsprogramme sind ausreichend dokumentiert und werden Mitarbeitern zur Verfügung gestellt.	
Schulung von Kompetenzen	
Neue Mitarbeiter erhalten zu Beginn des Arbeitsverhältnisses eine Einführung in die Richtlinien und Dienstanweisungen zur Informationssicherheit des Unternehmens (z.B. Passwortsicherheit, sicherer Umgang mit vertraulichen Informationen).	
Korrekte Anwendung von IT-Sicherheitsmaßnahmen (Soft- und Hardware) werden in Schulungseinheiten vermittelt (z.B. E-Mail-Verschlüsselung, Zwei-Faktor-Authentifizierung).	
Spezialisierte Fachschulungen nach Mitarbeitergruppen (z.B. Administratoren, Unternehmensleitung) werden durchgeführt.	
Schulungsinhalte zur Informationssicherheit werden entsprechend den Mitarbeitergruppen und ihren Aufgabenbereichen strukturiert und zugeschnitten.	
Sensibilisierung gegenüber Cyberbedrohungen	
Mitarbeiter werden gegenüber den Auswirkungen durch Cyberbedrohungen (z.B. Sicherheitslücken) sensibilisiert.	
Sensibilisierung der Mitarbeiter gegenüber Ausspähversuchen (z.B. auf Messen, Auslandsreisen).	
Mitarbeiter werden gegenüber den Gefahren durch Social Engineering (z.B. Phishing, CEO Fraud) sensibilisiert (z.B. Web- und E-Mail-Sicherheit, Nutzung von Sozialen Netzwerken).	
Schulungsinhalte zur Informationssicherheit werden entsprechend auf Mitarbeitergruppen und ihrer Aufgabenbereiche strukturiert und zugeschnitten.	

Weiterführende Links zum Thema Erstellung von Richtlinien und Dienstanweisungen:

- **BSI - ORP.3 Sensibilisierung und Schulung**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz Kompendium/bausteine/ORP/ORP_3_Sensibilisierung_und_Schulung.html
- **BSI - Umsetzungshinweise zum Baustein ORP.3 Sensibilisierung und Schulung**
  www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/ umsetzungshinweise/ORP/Umsetzungshinweise_zum_Baustein_ORP_3_ Sensibilisierung_und_Schulung.html
- **Kompetenzzentrum Digitales Handwerk - Routenplaner Cybersicherheit für das Handwerk, S. 19-22**
  https://www.handwerkdigital.de/deulocal/textbilder/images/PDF%20 Allgemein/routenplaner_cyber-sicherheit_klickbar.pdf
- **Secure-it.nrw - Mitarbeiter sensibilisieren für IT-Sicherheit und Datenschutz**
  https://www.nrw-units.de/fileadmin/user_upload/Download/Mitarbeiter_ sensibilisieren_f%C3%BCr_IT-Sicherheit_und_Datenschutz_01.pdf

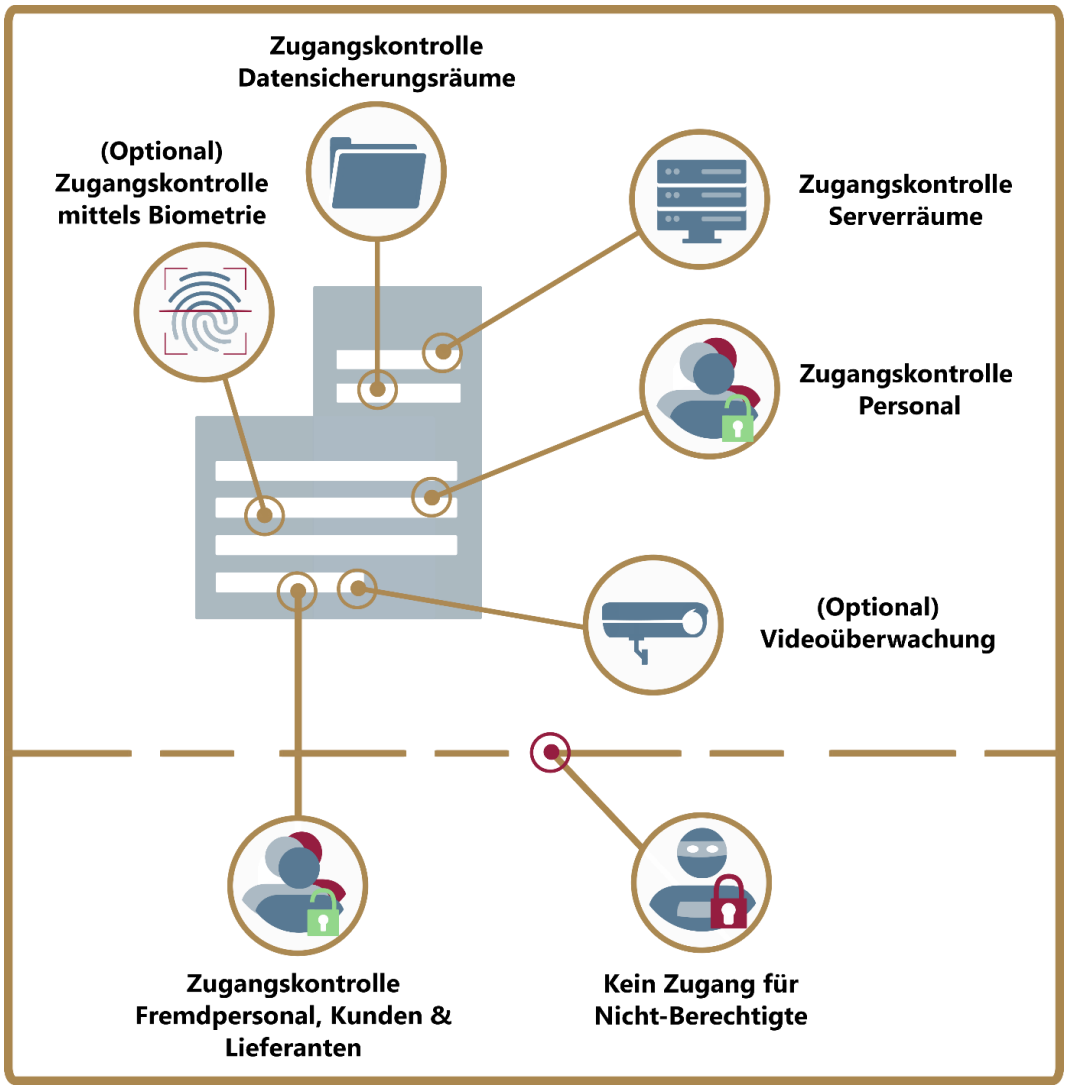
2.3 Infrastruktur und bauliche Maßnahmen

IT-Sicherheit beginnt bereits beim Betreten des Firmenareals oder -gebäudes. Es sind technische und bauliche Maßnahmen zu treffen, um Unbefugten den Zutritt zu verbieten und gleichzeitig den Personenverkehr zu kontrollieren.

Je nach Schutzdefinition und Sicherheitszielen des Unternehmens müssen Schutzmaßnahmen getroffen und umgesetzt werden. In Abhängigkeit der lokalen Gegebenheiten und der zuvor definierten Sicherheitsziele sollten Zugangskontrollen zum Firmengelände oder zu Gebäuden eingeführt werden, damit Unberechtigte keinen Zutritt erhalten und die physische Sicherheit der IT-Systeme nicht beeinträchtigen kann. Die Sicherheit der stationären Technik im Gebäude ist ein wesentlicher Sicherheitsaspekt, da in der Regel nicht nur Mitarbeiter, sondern auch Kunden oder Lieferanten das Gelände oder das Gebäude betreten.

Des Weiteren müssen Zugangskontrollen in zuvor definierten unternehmenskritischen Bereichen eingeführt werden, wie beispielsweise Server- oder Datensicherungsräumen. Prinzipiell darf der Zugang zu unternehmenskritischen Bereichen nur berechtigten Personen gewährt werden. Das schließt nicht nur das Fremdpersonal ein, sondern auch die eigenen Mitarbeiter. Die Zutrittsmöglichkeiten müssen für jeden Mitarbeiter auf das zur Erfüllung seiner Aufgaben Nötigste reduziert werden.

Abb. 4: Infrastruktur und bauliche Maßnahmen



Die **wesentlichen Handlungsempfehlungen zu Infrastruktur und baulichen Maßnahmen** stehen in der folgenden Überblickstabelle:

Technische Objektsicherheit	✓ ○ ✗
Sichtbare physische Barrieren zum Firmengelände schützen vor unbefugten Zutritten (z.B. Zäune, Tore).	☐ ☐ ☐
Der Zutritt zu Gebäuden ist durch technische oder bauliche Maßnahmen gegen Unbefugte geschützt (z.B. Ausweiskontrolle, Gebäudeschließanlagen).	☐ ☐ ☐
Raumumschließende Sicherheitsmaßnahmen wie Fenster und Türen sind nach Schutzbedarf ausgewählt worden.	☐ ☐ ☐
Der Zutritt zu Bereichen (z.B. Datensicherungs- und Serverräume), in denen vertrauliche Informationen verarbeitet oder gespeichert werden, ist nur für befugtes Personal (z.B. Administratoren) gestattet und mit Zugangskontrollen geschützt (z.B. PIN, sichere Türen).	☐ ☐ ☐
Besucher mit entsprechenden Zugangsberechtigungen werden erfasst und protokolliert.	☐ ☐ ☐

Zugangskontrollen und beschränkter Zutritt zu Sicherheitsbereichen für Fremdpersonal, Kunden oder Lieferanten.	☐ ☐ ☐
Telekommunikationsanlagen sind gegen unbefugten Zugang abgesichert.	☐ ☐ ☐
Es wurden Maßnahmen zum Diebstahlschutz von elektronischen (mobilen) Geräten getroffen, auf denen vertrauliche Informationen verarbeitet oder gespeichert sind (z.B. Kabelschlösser).	☐ ☐ ☐
Optionale Maßnahmen bei erhöhtem Schutzbedarf	✓ ○ ✗
Sicherheitsbereiche sind durch Alarm- und Einbruchsmeldeanlagen gesichert.	☐ ☐ ☐
Ein- und Ausgänge sowie kritische Sicherheitsbereiche werden zum Nachweis von potenziellen Sicherheitsverstößen durch eine Video-überwachungsanlage überwacht.	☐ ☐ ☐

Weiterführende Links zum Thema Infrastruktur und bauliche Maßnahmen:

- **BSI - INF: Infrastruktur**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz Kompendium/bausteine/INF/INF_Uebersicht_node.html
- **Wirtschaftsgrundschutz - Baustein IS1 Objektsicherheit**
  https://www.wirtschaftsschutz.info/DE/Veroeffentlichungen/ Wirtschaftsgrundschutz/Bausteine/Objektsicherheit.pdf?__blob=publication File&v=2
- **Wirtschaftsgrundschutz - Baustein IS3 - Kontinuität der Gebäudedienste**
  https://www.wirtschaftsschutz.info/DE/Veroeffentlichungen/ Wirtschaftsgrundschutz/Bausteine/Gebaeudedienste.pdf?__blob=publication File&v=1
- **Kompetenzzentrum Digitales Handwerk - Routenplaner Cybersicherheit für das Handwerk, S. 127-135**
  https://www.handwerkdigital.de/deulocal/textbilder/images/PDF%20 Allgemein/routenplaner_cyber-sicherheit_klickbar.pdf

3 IT-Sicherheitsmaßnahmen

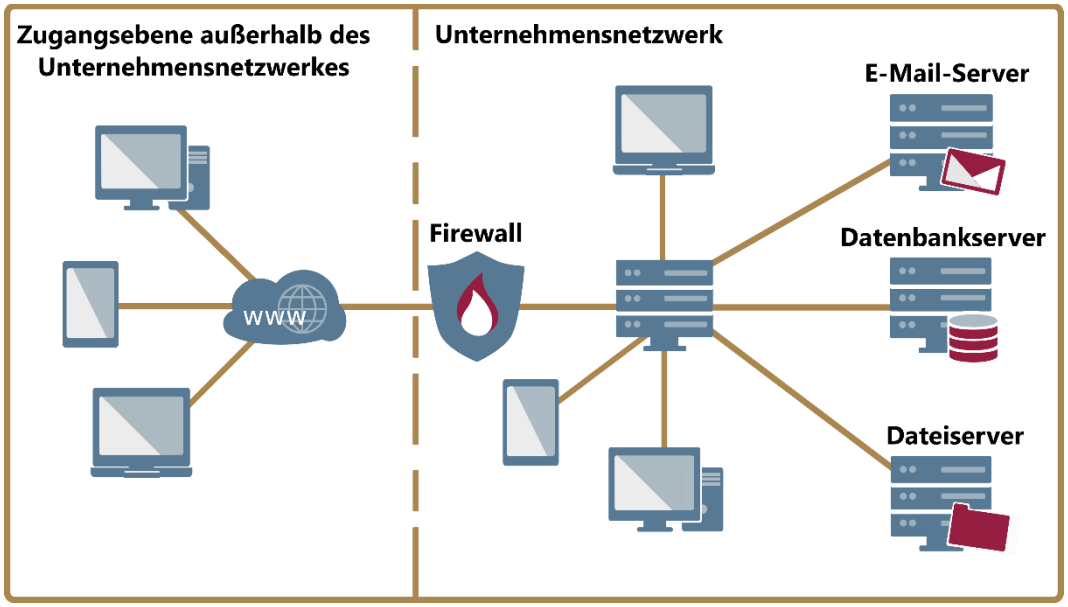
Ein weiterer essenzieller Punkt zur Umsetzung eines nachhaltigen Schutzes von unternehmenskritischen Daten (wie Kundendaten, Bauplänen, Forschungsergebnissen oder anderen vertraulichen Informationen und Dokumenten) gegen Informationsabflüsse durch Wirtschaftsspionage und Konkurrenzausspähung sind Maßnahmen zur Sicherung von IT-Systemen. Einer Vielzahl von Angriffsvektoren und Cyberangriffen kann durch technische IT-Sicherheitsmaßnahmen proaktiv und effektiv entgegengewirkt werden. Ein höheres IT-Sicherheitsniveau kann den Handlungsspielraum potenzieller Angreifer stark eingrenzen, da diese einen höheren materiellen und zeitlichen Aufwand für Cyberangriffe gegen ihr Unternehmen betreiben müssen. Folglich muss ein Angreifer abwägen, ob solch ein Cyberangriff noch lohnend erscheint.

Abb. 5: IT-Sicherheitsmaßnahmen

3.1 Sicherung des Unternehmensnetzwerks, Server, Arbeitsplatzrechner

Nahezu jedes Unternehmen besitzt und betreibt IT-Infrastrukturen. IT-Infrastrukturen können in ihrer Größe und Komplexität stark variieren. Sie können aus einem einfachen Zugang zum Internet bis hin zu großen Verbünden aus vielen Computern, Servern und Datenbanken bestehen. Daher sind Unternehmensnetzwerke ein wesentlicher Bestandteil eines Unternehmens. Sie bilden die Schnittstelle ab, die die Zusammenarbeit von Mitarbeitern, Unternehmenspartnern, Zulieferern und Kunden ermöglicht. Um einen hohen IT-Sicherheitsstandard für die IT-Infrastruktur zu gewährleisten, ist eine sichere Basiskonfiguration aller Bestandteile eines Unternehmensnetzwerks, wie Arbeitsplatzrechner, Server und Netzwerkkomponenten von größter Notwendigkeit.

Abb. 6: Sicherung des Unternehmensnetzwerks



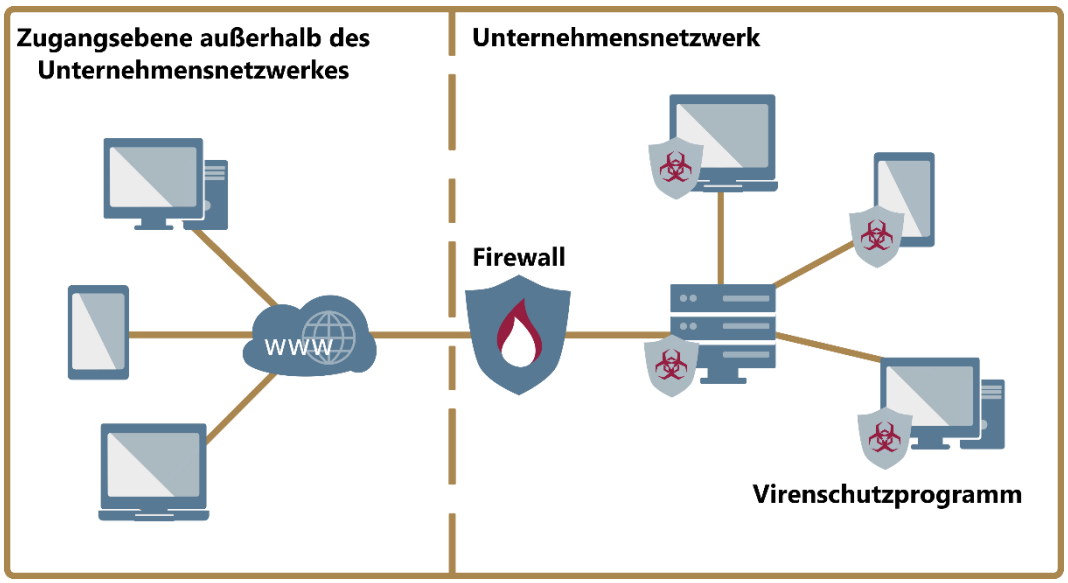
3.1.1 Schutz vor Schadprogrammen

Das Unternehmensnetzwerk und die einzelnen Netzwerkkomponenten der IT-Infrastruktur müssen über einen angemessenen Schutz vor Schadprogrammen verfügen. Der Basisschutz sollte unter anderem die Nutzung eines Firewall-Systems zum Schutz des Unternehmensnetzwerks und insbesondere der Netzwerkübergänge vor unbefugten Netzwerkzugriffen beinhalten.

Zusätzlich zu einer Firewall müssen die einzelnen Netzwerkkomponenten im Unternehmensnetzwerk wie Desktop-Rechner oder mobile Endgeräte über einen Schutz gegen Viren oder Schadprogrammen verfügen. Die eingesetzten Virenschutzprogramme sollten in der Lage sein, durch Viren befallene Dateien zu entdecken und das Ausführen von Schadprogrammen zu unterbinden. Schadprogramme können sich auf unterschiedliche Wege verbreiten, beispielsweise über Anhänge oder Links in E-Mails.

Betriebssysteme, Firmware, Treiber und Anwendungen aller Netzwerkkomponenten müssen regelmäßig aktualisiert werden. Neue Updates und Patches bringen nicht nur Neuerungen oder Fehlerkorrekturen, sondern schließen vor allem auch kritische Sicherheitslücken.

Abb. 7: Schutz des Unternehmensnetzwerks und der Clients



Die **wesentlichen Maßnahmen zum Schutz** des Unternehmensnetzwerks, der Server und Arbeitsplatzrechner **vor Schadprogrammen** stehen in der folgenden Überblickstabelle:

Schutz vor Schadprogrammen	✓ ○ ✗
Firewalls schützen das Unternehmensnetzwerk, alle Netzwerkkomponenten und angeschlossene Endgeräte vor unbefugten Zugriffen von außen.	☐ ☐ ☐
Verwendete Endgeräte verfügen über ein aktuelles Virenschutzprogramm.	☐ ☐ ☐
Deaktivierung und Deinstallation von nicht benötigten Komponenten (z.B. integrierten Mikrophonen, Apps, Kameras).	☐ ☐ ☐
Das Betriebssystem auf den Geräten befindet sich auf dem aktuellsten Stand.	☐ ☐ ☐
Neue Patches und Sicherheitsupdates werden mithilfe von Autoupdate-Mechanismen installiert.	☐ ☐ ☐
Web-Sicherheit	✓ ○ ✗
Der Zugang zum Internet wird durch aktuelle und sichere Web-Browser vorgenommen.	☐ ☐ ☐
Besuchte Internetseiten werden über HTTPS aufgerufen.	☐ ☐ ☐
Mit Schadprogrammen belastete Werbung wird durch Ad-Blocker blockiert.	☐ ☐ ☐

Deaktivierung von HTML beim E-Mail-Client, stattdessen werden E-Mails im Text-Format angezeigt.	☐ ☐ ☐
Verdächtige Links in E-Mails werden nicht geöffnet (z.B. von unbekannten Absendern).	☐ ☐ ☐
Das Herunterladen von E-Mail-Anhängen unbekannter Herkunft ist untersagt.	☐ ☐ ☐

Weiterführende Links zum Thema* Schutz *vor Schadprogrammen:

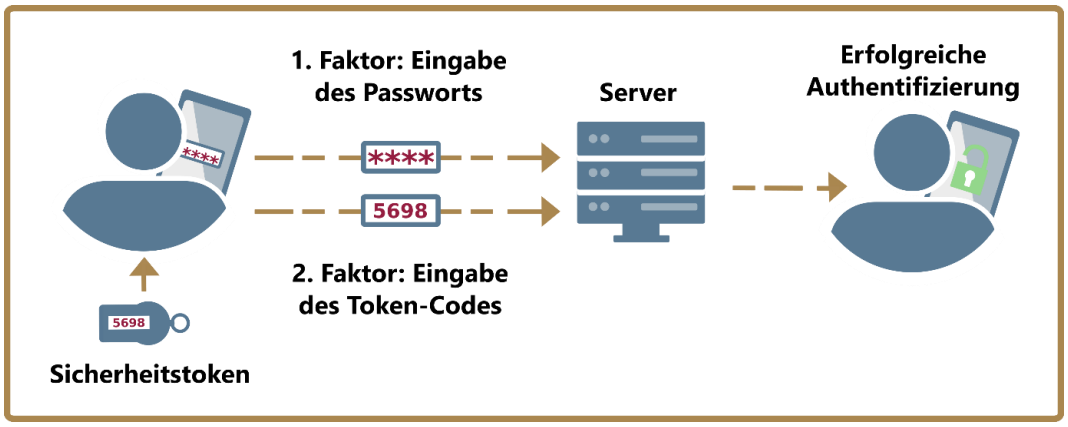
- **VdS - Cyber Security für kleine und mittlere Unternehmen (KMU) – 10.3.5 Schadsoftware, S. 22**
  https://vds.de/fileadmin/vds_publikationen/vds_3473_web.pdf
- **BSI - OPS.1.1.4 Schutz vor Schadprogrammen**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz Kompendium/bausteine/OPS/OPS_1_1_4_Schutz_vor_Schadprogrammen.html
- **BSI - NET.3.2 Firewall**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz Kompendium/bausteine/NET/NET_3_2_Firewall.html
- **BSI - APP.1.2 Web-Browser**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz Kompendium/bausteine/APP/APP_1_2_Web-Browser.html
- **BSI - OPS.1.1.3 Patch- und Änderungsmanagement**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz Kompendium/bausteine/OPS/OPS_1_1_3_Patch-_und_ %C3%84nderungsmanagement.html

3.1.2 Zugänge und Zugangsrechte

Eine Vielzahl von Akteuren kommuniziert und interagiert über das Unternehmensnetzwerk bzw. über das Intranet. Dementsprechend sollten die Zugänge zum Unternehmensnetzwerk und die darin enthaltenen Netzwerkkomponenten reglementiert und regelmäßig aktualisiert werden. Offene Zugänge zum Unternehmensnetzwerk bieten Angreifern ein potenzielles Einfallstor. Nur autorisierten Personen oder Personengruppen mit zugelassenen Geräten darf der Zugang zum Netzwerk gewährt werden.

Die Sicherung beginnt bereits am eigenen Arbeitsplatz. Arbeitsplatzrechner müssen gegen unbefugte Zugriffsversuche geschützt werden. Ebenso müssen Server und das Unternehmensnetzwerk mit IT-Sicherheitsmaßnahmen gegen unbefugte Zugriffe gehärtet werden. Wichtig ist zudem ein funktionierendes Passwortmanagement. Komplexe Zugangsinformationen helfen in der Praxis wenig, wenn diese nicht sicher vor Unbefugten aufbewahrt werden. Daher sind auch Maßnahmen zur sicheren Speicherung von Zugangsinformationen zu treffen.

Abb. 8: Zwei-Faktor Authentifizierung



Die **wesentlichen Maßnahmen, um Zugänge und Zugangsrechte zu reglementieren,** stehen in der folgenden Überblickstabelle:

Passwortmanagement	✓ ○ ✗
Passwortrichtlinie für ausreichend starke Passwörter (z.B. Sonderzeichen, festgelegte Länge, keine personenbezogenen Informationen) und deren Gültigkeitsdauer.	☐ ☐ ☐
Zugangsdaten werden sicher vor Einblicken Dritter aufbewahrt (z.B. mit einem Passwort-Manager, verschlüsselte Dateien).	☐ ☐ ☐
Es werden Backups der Zugangsdaten angelegt (z.B. in Papierform in abschließbaren Schränken).	☐ ☐ ☐
Arbeitsplatzrechner	✓ ○ ✗
Die Nutzung von Arbeitsplatzrechnern ist nur mit einem Authentisierungsverfahren möglich (z.B. Passwort, Security Token, Biometrie).	☐ ☐ ☐
Arbeitsplatzrechner können manuell oder nach einem festgelegten Inaktivitätszeitraum automatisch gesperrt oder abgemeldet werden (z.B. Bildschirmsperre).	☐ ☐ ☐
Verbaute Festplatten, auf denen sich ggf. vertrauliche Dateien befinden, werden durch kryptografische Funktionen des Betriebssystems oder zusätzliche Anwendungsprogramme verschlüsselt.	☐ ☐ ☐
Die Konfigurationseinstellung des Boot-Vorgangs können nur durch Administratoren verändert werden.	☐ ☐ ☐
Das Booten aus eingebauten Laufwerken oder externen Speichermedien kann nur durch Administratoren ausgeführt werden.	☐ ☐ ☐
Server	✓ ○ ✗
Es werden nur Server in Anspruch genommen, deren physikalischer Standort innerhalb des deutschen bzw. des EU-Rechtsraumes liegt.	☐ ☐ ☐
Server sind an physisch geschützten Sicherheitsbereichen mit Zugangskontrollen aufgestellt (Rechenzentren, Rechnerräumen, abschließbare Serverschränke).	☐ ☐ ☐
Administratoren nutzen für nicht-administrative Aufgaben weniger privilegierte Benutzer-Accounts.	☐ ☐ ☐

Für die Administratorschnittstelle werden anstatt des passwort-basierten SSH-Logins starke Authentifizierungsverfahren genutzt (z.B. Challenge-Response-Verfahren).	
Für das Server Login wird eine Zwei-Faktor- oder Multi-Faktor-Authentifizierung genutzt (z.B. Security-token, Smartcards).	
(Funk-)Netzwerke	
Vertrauliche Informationen sind nur aus dem Unternehmensnetzwerk abrufbar.	
Bei Funknetzwerken (WLAN) wird Wi-Fi Protected Access 2 (WPA2) oder eine höhere Version als Sicherheitsstandard bzw. Verschlüsselungsmethode verwendet.	
Alternativ wird ein MAC-Filter für stationäre Arbeitsplatzrechner verwendet werden, um nur zugelassenen Geräten den Zugang zum Netzwerk zu ermöglichen.	
Das Netzwerk ist nach Aspekten wie Standort, Benutzergruppen oder Sicherheitsanforderungen in mehrere logische Subnetze unterteilt (Subnetting), um den Austausch von vertraulichen Informationen auf bestimmte Subnetze zu reduzieren (z.B. Gastnetzwerke, VoIP-Netzwerk).	
Für sichere Fernzugriffe auf vertrauliche Informationen wird eine zugriffsgeschützte und verschlüsselte VPN-Verbindung genutzt.	
Für die VPN Authentisierung werden Zertifikate statt klassischer Passwörter benutzt.	

Weiterführende Links zum Thema Zugänge und Zugangsrechte:

- **VdS - Cyber Security für kleine und mittlere Unternehmen (KMU) – 10.3.7 Authentifizierung, S. 22**
  11 Netzwerke und Verbindungen, S. 26
  https://vds.de/fileadmin/vds_publikationen/vds_3473_web.pdf
- **BSI - ORP.4 Identitäts- und Berechtigungsmanagement**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz Kompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_ Berechtigungsmanagement.html
- **BSI - Wie Passwort-Manager Daten schützen**
  https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/ Passwort_Manager/Passwort_Manager_node.html
- **BSI - SYS.2.1 Allgemeiner Client**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz Kompendium/bausteine/SYS/SYS_2_1_Allgemeiner_Client.html
- **BSI - SYS.1.1 Allgemeiner Server**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz Kompendium/bausteine/SYS/SYS_1_1_Allgemeiner_Server.html
- **Kompetenzzentrum Digitales Handwerk - Routenplaner Cybersicherheit für das Handwerk, S. 109-116**
  https://www.handwerkdigital.de/deulocal/textbilder/images/PDF%20 Allgemein/routenplaner_cyber-sicherheit_klickbar.pdf

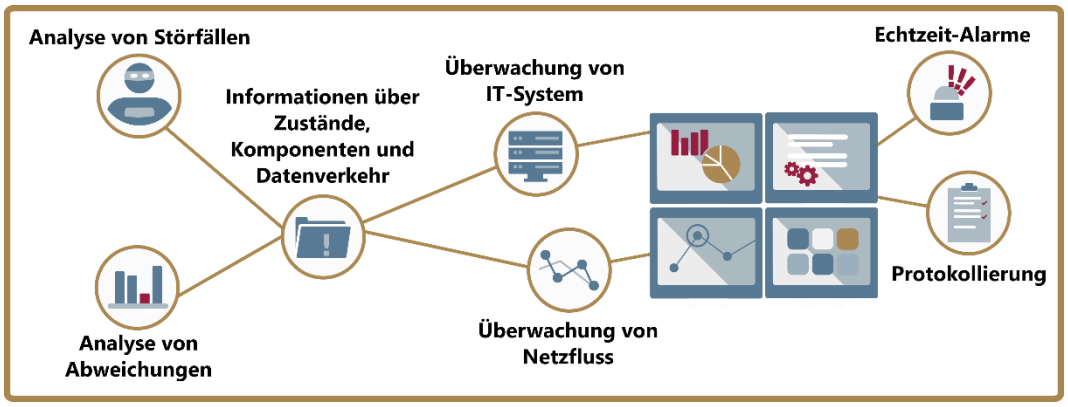
3.1.3 Monitoring der IT-Systeme und des Netzflusses

Neben der Prävention ist die **Detektion von Cyber-Sicherheitsvorfällen** ein essenzieller Baustein für die IT-Sicherheit. Dabei kommt dem Monitoring der IT-Systeme und des Netzflusses eine zentrale Bedeutung zu.

- Das **Monitoring** ist ein zentrales Mittel zur Identifizierung und Analyse von unbefugten Zugriffsversuchen, um den Schaden zu minimieren.
- Eine **Protokollierung** ermöglicht es, bei einem festgestellten Zugriff von außen die Dauer des Zugriffs und den Datenabfluss zeitlich zurückzuverfolgen und den Umfang des Schadens zu bewerten.
- **Intrusion Dectection System (IDS)**-Anwendungen analysieren unter anderem den Inhalt der Datenpakete des Datenverkehrs und erkennen ungewöhnliche und bedrohliche Inhalte und Verhaltensmuster.

Gerade bei der Quantifizierung von unbefugten Zugriffen auf schützenswerte Daten haben Unternehmen noch Defizite. Die SiFo-Studie 2018/2019 zeigt, dass rund 36 Prozent der befragten Unternehmen die Anzahl von unbefugten Zugriffen aufgrund eines fehlenden Monitorings nicht genau beziffern konnten. Besonders bei mittleren Unternehmen bis zu 249 Mitarbeiter wird das Defizit deutlich (rd. 55 Prozent).

Abb. 9: Monitoring des Unternehmensnetzwerks



Die **wesentlichen Maßnahmen zum Monitoring** der IT-Systeme und des Netzflusses stehen in der folgenden Überblickstabelle:

Vorbereitende Dokumentation	✓ ○ ✗
Die Netzwerktopologie wird erstellt und dokumentiert.	☐ ☐ ☐
Alle Netzwerkkomponenten (z.B. Server, Router, Switches) sind inventarisiert und die Konfiguration (z.B. Betriebssysteme, Firmware) dokumentiert.	☐ ☐ ☐
Alle am Netzwerk teilnehmenden Endgeräte (z.B. Arbeitsplatz-rechner, Notebooks, Smartphones) sind inventarisiert.	☐ ☐ ☐
Aktives Monitoring	✓ ○ ✗
Die Auslastung und Verfügbarkeit von Netzwerkkomponenten (z.B. Server, Router, Switches) wird erfasst.	☐ ☐ ☐
Der Datenverkehr innerhalb des Netzwerkes wird beobachtet. (z.B. Netzwerk-Ein- und Ausgänge, Geschäftsprozesse, verdächtige Aktivitäten).	☐ ☐ ☐
Unerlaubtes Hinzufügen oder Entfernen von Netzwerkkomponenten, Geräten oder auch Speichermedien (z.B. USB-Schnittstellen) wird festgestellt.	☐ ☐ ☐
Netzwerkzugänge (physikalische Netzwerkports) werden überwacht.	☐ ☐ ☐
Kritische Dateien werden überwacht (Zugriffe, Bearbeitung und Löschung).	☐ ☐ ☐
Dienste (z.B. Mailserver, Druckserver) werden überwacht.	☐ ☐ ☐
Bei Sicherheitsverstößen oder -problemen werden Alarmierungsbe-nachrichtigungen an Administratoren versendet.	☐ ☐ ☐

Protokollierung und Auswertung	✓	○	✗
Inhalt und Umfang der Protokollierungsdateien berücksichtigen datenschutzrechtliche Anforderungen.	☐	☐	☐
Der Datenverkehr im Netzwerk wird protokolliert (z.B. in Form von Netflows).	☐	☐	☐
Die Protokollierung sicherheitsrelevanter Ereignisse (z.B. Zugriff, Bearbeitung oder Löschung von kritischen Dateien) wird automatisch ausgeführt.	☐	☐	☐
Fehler- und Statusmeldungen werden zentral und persistent protokolliert.	☐	☐	☐
Protokolldateien werden auf Sicherheitsverstöße hin analysiert und ausgewertet.	☐	☐	☐
Protokollierungsdateien werden über einen vom Verwendungszweck abhängigen, festgelegten Zeitraum aufbewahrt (z.B. für die Analyse oder Beweissicherung).	☐	☐	☐
Es werden für zusätzliche Redundanz regelmäßige Backups von Protokolldateien erstellt.	☐	☐	☐
Intrusion Detection System (IDS)	✓	○	✗
Signaturen und Verhaltensmuster werden aktualisiert.	☐	☐	☐
IP-Adressen werden mit Whitelist bzw. Blacklist (z.B. für Spam-filterung) abgeglichen und gefiltert.	☐	☐	☐
Konfiguration von Netzwerkkomponenten werden überprüft (z.B. Scannen nach offenen Zugängen zum Netzwerk oder Diensten).	☐	☐	☐
In Ergänzung zum IDS können Intrusion Prevention Systeme (IPS) ergänzt werden, welche erkannte Angriffe stoppen können, bevor diese Schäden anrichten.	☐	☐	☐
Durchführung von Penetrationstests durch externe Dienstleister.	☐	☐	☐

Weiterführende Links zum Thema Monitoring der IT-Systeme und des Netzflusses:

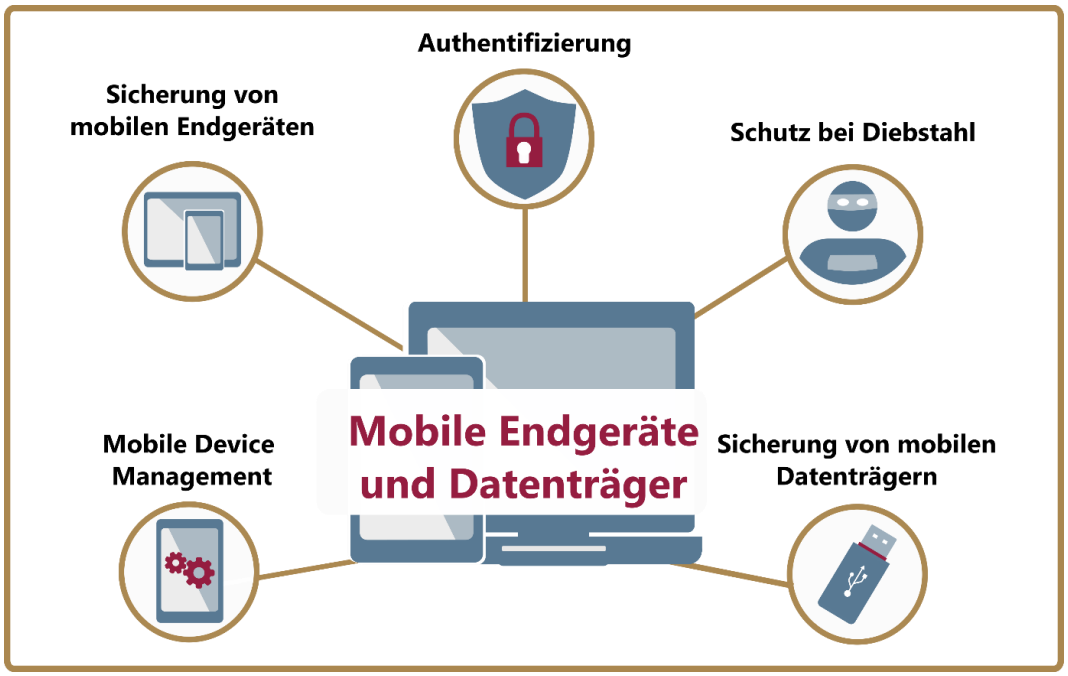
- **BSI - Monitoring und Anomalieerkennung in Produktionsnetzwerken**
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_134.pdf?__blob=publicationFile&v=5
- **BSI - OPS 1.1.5 Protokollierung**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_5_Protokollierung.html
- **BSI - DER Detektion und Reaktion**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/DER/DER_Uebersicht_node.html
- **BSI - Leitfaden zur Einführung von Intrusion Detection Systemen**
  https://www.bsi.bund.de/DE/Publikationen/Studien/IDS02/gr3_htm.html
- **VdS - Cyber Security für kleine und mittlere Unternehmen (KMU) -**
  10.3.3 Protokollierung, S. 22
  10.5.8 Überwachung, S. 25
  https://vds.de/fileadmin/vds_publikationen/vds_3473_web.pdf

3.2 Sicherung von mobilen Endgeräten und Datenträgern

Die Verwendung von mobilen Endgeräten, wie Laptops, Smartphones oder Tablets, in der betrieblichen Informationsverarbeitung ist im modernen Unternehmensumfeld keine Seltenheit mehr, sondern etablierter Standard. Genauso sind mobile Datenträger durch ihre Kompaktheit und einfache Bedienbarkeit weit verbreitet. Die Anzahl der betrieblichen mobilen Endgeräte und mobilen Datenträger steigt kontinuierlich an. Allerdings ist die Absicherung gegenüber Cyberbedrohungen nach wie vor eine Herausforderung für Unternehmen. Erschwerend kommt hinzu, dass auch private Geräte und Datenträger für betriebliche Aufgaben genutzt werden.

Im Unterschied zu klassischen stationären Arbeitsplatzrechnern, die sich an einem Unternehmensstandort und im Einflussbereich des Unternehmensnetzwerks befinden, kommunizieren mobile Endgeräte häufig über unsichere Netze und verfügen nicht immer über die IT-Sicherheitsmaßnahmen der stationären Arbeitsplatzrechner. Daher müssen IT-Sicherheitsmaßnahmen getroffen werden, um dem steigenden Sicherheitsrisiko durch mobile Endgeräte und Datenträger effektiv entgegenwirken zu können.

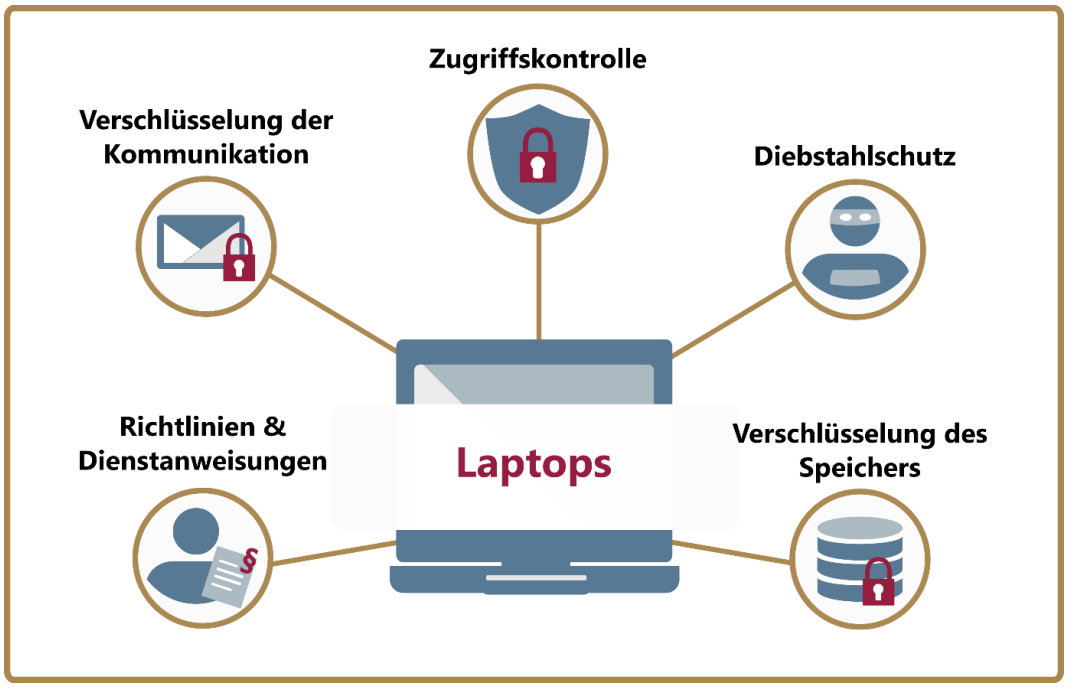
Abb. 10: Sicherheitsaspekte bei mobilen Endgeräten und Datenträgern



3.2.1 Basissicherung für Laptops

Laptops sind im Grunde mobile Arbeitsplatzrechner. In ihrer Funktionalität gibt eine große Schnittmenge zwischen Laptops und Arbeitsplatzrechnern. Die Mobilität von Laptops ist ein großer Vorteil, sie ermöglicht große Flexibilität, jedoch stellt die Flexibilität die IT-Sicherheit der Geräte vor weitere Herausforderungen. Denn häufig werden Laptops nicht nur am eigenen Unternehmensstandort eingesetzt, sondern werden auch in fremden Büroräumen, Hotels und anderen Umgebungen eingesetzt oder auch in Kraftfahrzeugen und anderen Verkehrsmitteln. Daher müssen Laptops häufig über unsichere Netze kommunizieren und sind einer größeren Bedrohung durch unbefugte Nutzung durch Dritte oder Diebstahl ausgesetzt. Folglich ist das Risiko für Wirtschaftsspionage und Konkurrenzausspähung höher als bei einem Arbeitsplatzrechner.

Abb. 11: Basissicherung von Laptops



Die **wesentlichen Maßnahmen zur Sicherung von Laptops** stehen in der folgenden Überblickstabelle:

Richtlinien zur sicheren Nutzung von Laptops	✓ ○ ✗
Es existieren Sicherheitsrichtlinien, die die sichere Nutzung von Laptops regulieren (z.B. Inbetriebnahme, Weitergabe, Ausmusterung).	☐ ☐ ☐
Die dienstliche Nutzung von privaten Endgeräten ist durch Sicherheitsrichtlinien klar reglementiert. (z.B. Sicherheitsanforderungen an die Endgeräte).	☐ ☐ ☐
Je nach Sicherheitsanforderungen ist die private Nutzung von Dienstgeräten eingeschränkt oder untersagt.	☐ ☐ ☐
Das nachträgliche Hinzufügen von zusätzlichen Programmen ist nur für die zur Aufgabenbewältigung notwendigen und vom Unternehmen freigegebenen Programmen erlaubt.	☐ ☐ ☐
Das Anschließen von unbekannten Speichermedien ist untersagt (z.B. USB-Sticks).	☐ ☐ ☐
Der Verlust oder Diebstahl eines Laptops mit darauf befindlichen Unternehmenszugängen oder Unternehmensdaten ist meldepflichtig und wird unter Sicherheitsgesichtspunkten analysiert.	☐ ☐ ☐

Technische Maßnahmen zur Sicherung von Laptops	✓ ○ ✗
Laptops verfügen über einen Zugriffsschutz, der eine unberechtigte Nutzung verhindert (z.B. PIN, Passwort, Sperrung im Verlustfall).	☐ ☐ ☐
Für die Aufgabenbewältigung wird statt eines Admin-Accounts ein weniger privilegierter Anwender Account ohne Administrationsrechte benutzt.	☐ ☐ ☐
Das Betriebssystem befindet sich auf dem aktuellsten Aktualisierungsstand.	☐ ☐ ☐
Der Gerätespeicher ist verschlüsselt (siehe 3.4.).	☐ ☐ ☐
Die elektronische Kommunikation wird verschlüsselt (siehe 3.3.).	☐ ☐ ☐
Fernzugriffe werden über sichere VPN-Verbindungen ausgeführt (z.B. in Hotels, fremden Büroräumen).	☐ ☐ ☐
Sicherheitsfunktionen eines Trusted Platform Module (TPM) werden genutzt (z.B. Aufbewahrung und Erstellung kryptografischer Schlüssel, Versiegelung von Daten).	☐ ☐ ☐
Es werden Maßnahmen zum Diebstahlschutz getroffen (z.B. Schlauchschloss, verschließbarer Aufbewahrungsort).	☐ ☐ ☐

Weiterführende Links zum Thema Basissicherung für Laptops:

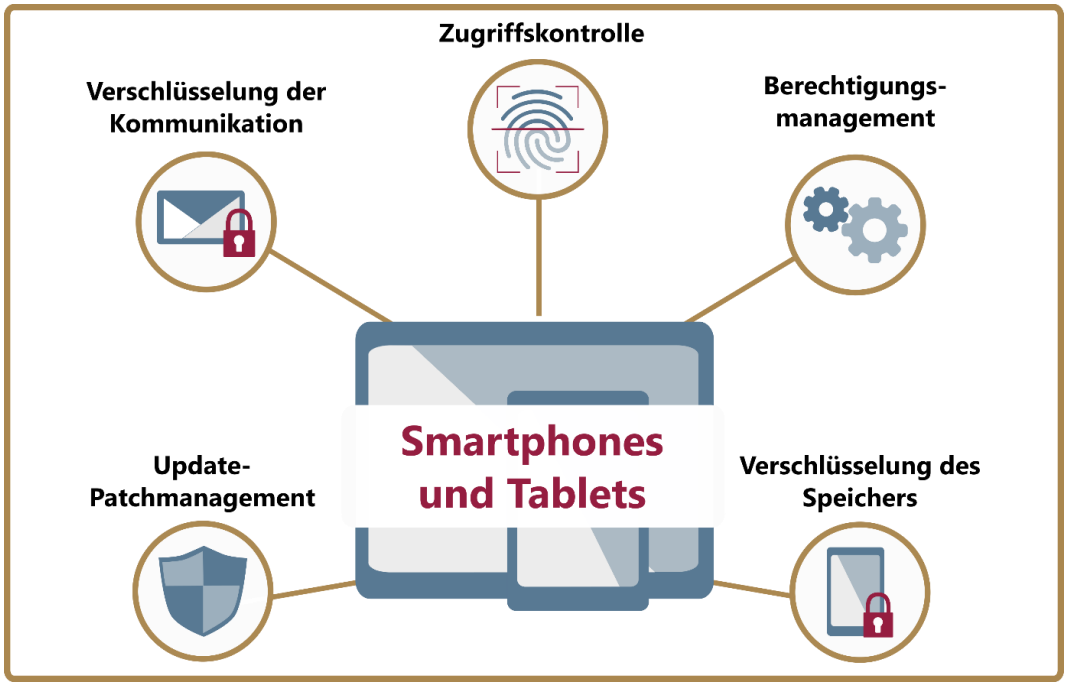
- **BSI - SYS.2.1 Allgemeiner Client**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_2_1_Allgemeiner_Client.html
- **BSI - SYS.3.1 Laptops**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_3_1_Laptops.html
- **BSI - NET.3.3 VPN**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_3_3_VPN.html
- **BSI - ORP.4 Identitäts- und Berechtigungsmanagement**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_Berechtigungsmanagement.html
- **BSI - Umgang mit Passwörtern**
  https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Umgang/umgang_node.html

3.2.2 Basissicherung für Smartphones und Tablets

Smartphones und auch Tablets werden immer häufiger für dienstliche Zwecke genutzt. Daher müssen sie für eine betriebliche Nutzung durch geeignete Maßnahmen gesichert werden. Smartphones sind Mobiltelefone mit einem Zugang zum Internet und einen größeren Funktionsumfang. Sie verfügen über weitreichende Sensorik, welche z.B. Ortungsdaten sammelt oder Biometrie-Verfahren ermöglicht. Tablets sind in ihrem Funktionsumfang ähnlich zu Smartphones, jedoch unterscheiden sie sich in ihrer Größe und dem optionalen Zugang zum Mobilfunknetz.

Befinden sich schützenswerte Informationen auf den Geräten oder haben die Geräte Zugang zu schützenswerten Informationen muss es Sicherheitsrichtlinien zur sicheren Nutzung der Geräte für die Mitarbeiter geben. Zusätzlich müssen Smartphones und Tablets sicher konfiguriert werden, um die Gefahren durch Wirtschaftsspionage und Konkurrenzausspähung zu reduzieren.

Abb. 12: Basissicherung für Smartphones und Tablets



Die **wesentlichen Maßnahmen zur Sicherung von Smartphones und Tablets** stehen in der folgenden Überblickstabelle:

Richtlinien zur Nutzung von Smartphones und Tablets	✓ ○ ✗
Es existieren Sicherheitsrichtlinien hinsichtlich der sicheren Nutzung und Kontrolle der Endgeräte.	☐ ☐ ☐
Die dienstliche Nutzung von privaten Endgeräten ist durch Sicherheitsrichtlinien klar reglementiert (z.B. Sicherheitsanforderungen an die Endgeräte).	☐ ☐ ☐
Je nach Sicherheitsanforderungen ist die private Nutzung von Dienstgeräten eingeschränkt oder untersagt.	☐ ☐ ☐
Der Austausch von vertraulichen Informationen über SMS- oder MMS-Dienste ist untersagt.	☐ ☐ ☐

Das nachträgliche Hinzufügen von Applikationen ist nur für geprüfte und vom Unternehmen freigegebene Applikationen erlaubt und wird unter Sicherheitsgesichtspunkten analysiert (z.B. Filterung durch Whitelists, Mobile Device Management).	☐ ☐ ☐
Die Installation von Applikationen aus unbekannten oder unsicheren Quellen ist grundsätzlich untersagt.	☐ ☐ ☐
Der Gerätename darf keine persönlichen oder unternehmensbezogenen Informationen beinhalten.	☐ ☐ ☐
Ältere Geräte, deren Support durch die Hersteller endet und die dadurch keine Sicherheitsaktualisierungen mehr erhalten, werden aussortiert und durch neue unterstützte Geräte ersetzt.	☐ ☐ ☐
Der Verlust oder Diebstahl eines Smartphones oder Tablets ist meldepflichtig.	☐ ☐ ☐
Technische Maßnahmen für Smartphones und Tablets	✓ ○ ✗
Smartphones und Tablets sind mit einem Zugriffsschutz (z.B. Biometrie, PIN, Bildschirmsperre) gegenüber unbefugter Nutzung geschützt.	☐ ☐ ☐
SIM-Karten sind mit einer sicheren PIN geschützt.	☐ ☐ ☐
Applikationen erhalten nur die benötigten Berechtigungen auf dem Gerät (z.B. Zugriff auf Standort, Einsicht in die Kontakte)	☐ ☐ ☐
Der Gerätespeicher und ggf. die Speichererweiterung sind verschlüsselt (siehe 3.4.).	☐ ☐ ☐
Die elektronische Kommunikation wird verschlüsselt (siehe 3.3).	☐ ☐ ☐
Das Betriebssystem befindet sich auf dem aktuellsten Aktualisierungsstand.	☐ ☐ ☐
Sobald Sicherheitsupdates verfügbar sind, werden diese auf den Geräten installiert.	☐ ☐ ☐
Die auf den Geräten befindlichen Applikationen werden regelmäßig auf die neueste Version aktualisiert.	☐ ☐ ☐
Das Anzeigen von Informationen auf dem Sperrbildschirm des Geräts ist deaktiviert (z.B. Push-Nachrichten).	☐ ☐ ☐
Deaktivierung von Funktionen und Diensten, die nicht genutzt oder benötigt werden (z.B. WLAN, Bluetooth, GPS, NFC).	☐ ☐ ☐

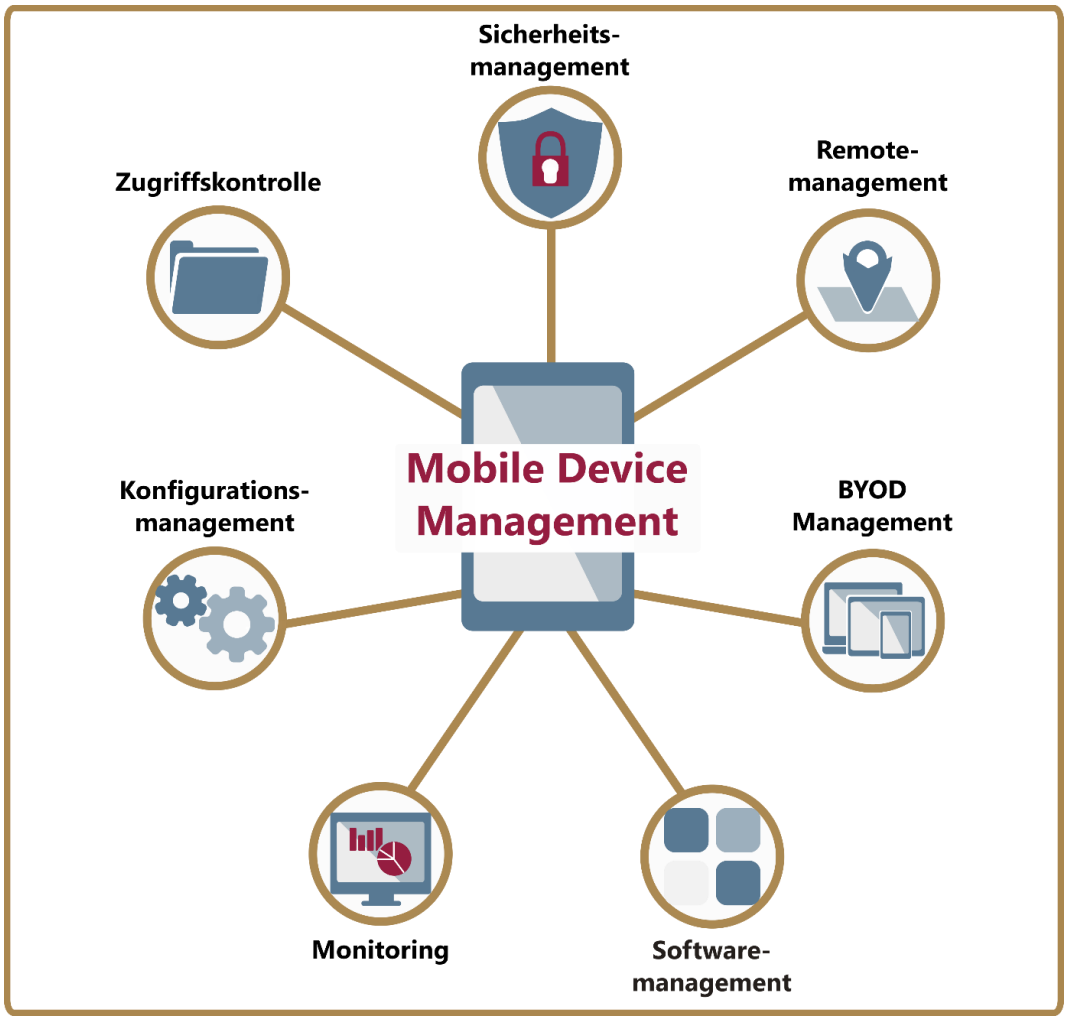
Weiterführende Links zum Thema Basissicherung für Smartphones und Tablets:

- **BSI - SYS.3.2.1: Allgemeine Smartphones und Tablets**
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2019.pdf?__blob=publicationFile&v=5#ub_dest_SYS.3.2.1
- **BSI - SYS.3.3 Mobiltelefon**
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Angebote/Routenplaner/SYS/sys_d.html?cms_pos=8
- **BSI - Zwei-Faktor-Authentisierung für höhere Sicherheit**
  www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/Zwei_Faktor_Authentisierung/Zwei-Faktor-Authentisierung_node.html
- **BSI - ORP.4 Identitäts- und Berechtigungsmanagement**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_Berechtigungsmanagement.html
- **Kompetenzzentrum Digitales Handwerk - Routenplaner Cybersicherheit für das Handwerk, S. 87-94**
  https://www.handwerkdigital.de/deulocal/textbilder/images/PDF%20Allgemein/routenplaner_cyber-sicherheit_klickbar.pdf
- **TeleTrust - Biometrische Authentisierung**
  www.teletrust.de/publikationen/broschueren/authentisierung/

3.2.3 Mobile Device Management

Steigt die Anzahl der mobilen Endgeräte (Mobile Devices) im Unternehmen an, sollte über die Einführung eines Mobile Device Management (MDM) nachgedacht werden. Je mehr Mitarbeiter und daraus folgend eine größere Anzahl, zum Teil unterschiedlicher, mobiler Endgeräte vorhanden sind, desto größer wird der Verwaltungsaufwand für die Geräte und die Sicherstellung einer angemessenen Sicherheit gegenüber Cybersicherheitsvorfällen für das Unternehmen. Die Integration von Sicherheitslösungen in mobile Geräte wird aufgrund der heterogenen Mobilgerätelandschaft erschwert. Diverse Geräteklassen von unterschiedlichen Herstellern, verschiedene Betriebssysteme und Anwendungsprogramme erschweren die Administration der Geräte. MDM-Lösungen ermöglichen eine Integration vieler gängiger, mobiler Betriebssysteme (iOS, Android, etc.) in die Gerätelandschaft des Unternehmens. Sie bringen nicht nur administrative Vorteile mit sich, sondern besitzen auch umfassende Sicherheitsfunktionen. Die Geräte lassen sich hinsichtlich der Sicherheitsrichtlinien und -regeln zentral sicher konfigurieren.

Abb. 13: Mobile Device Management (MDM)



Die **wesentlichen Maßnahmen zum Mobile Device Management** stehen in der folgenden Überblickstabelle:

Mobile Device Management (MDM)	✓ ○ ✗
Festlegung von erlaubten mobilen Endgeräten und Betriebssystemen, die in die MDM-Umgebung integriert werden und die Sicherheitsanforderungen des Unternehmens vollständig erfüllen.	☐ ☐ ☐
Es gibt eine Richtlinie, die die Integration von BYOD-Geräten in die MDM-Umgebung reguliert.	☐ ☐ ☐
Zentrale und automatische Inventarisierung aller mobilen Endgeräte des Unternehmens (Inventory Management).	☐ ☐ ☐
Bereitstellung eines Katalogs mit autorisierten Applikationen bzw. Anwendungen (z.B. Whitelists).	☐ ☐ ☐
Das MDM setzt ein Berechtigungsmanagement mit Benutzergruppen und Rechtesystem nach dem Minimalprinzip durch (z.B. Zugriff auf Informationen, administrative Rechte).	☐ ☐ ☐
Vor der Übergabe des mobilen Endgerätes an den Mitarbeiter wird der MDM-Client installiert.	☐ ☐ ☐

Die Konfigurationsroutine enthält eine möglichst selbständige und sichere Konfiguration aller relevanten Einstellungen des mobilen Endgerätes (z.B. E-Mail, VPN, WLAN).	☐ ☐ ☐
Auswahl benötigter Sicherheitsanwendungen, die automatisch bei der Konfigurationsroutine auf dem mobilen Endgerät installiert werden (z.B. Viren-Schutz, Verschlüsselungsanwendungen).	☐ ☐ ☐
Das MDM ermöglicht ein automatisiertes Einspielen von Updates und Patches.	☐ ☐ ☐
Das MDM verwaltet die Installation und Deinstallation von Zertifikaten auf den mobilen Endgeräten.	☐ ☐ ☐
Durch das MDM wird die Fernlöschung der Daten auf dem mobilen Endgerät und ggf. des externen Speichers ermöglicht (z.B. bei Verlust, Außerbetriebnahme).	☐ ☐ ☐
Mithilfe des MDM kann die Nutzung des mobilen Endgeräts per Fernzugriff eingeschränkt oder gesperrt werden (z.B. bei einem Sicherheitsverstoß).	☐ ☐ ☐
Der Gerätestatus, alle sicherheitsrelevanten Ereignisse und Konfigurationsänderungen werden datenschutzkonform protokolliert.	☐ ☐ ☐
Administratoren erhalten bei einem Sicherheitsverstoß oder sicherheitsrelevanten Ereignis eine Warnmeldung.	☐ ☐ ☐
Die Sicherheitseinstellungen des MDM werden regelmäßig überprüft, ob sie noch wirksam und ausreichend sind (z.B. bei neuen Betriebssystemversionen).	☐ ☐ ☐

Weiterführende Links zum Thema Mobile Device Management:

- **BSI - Mindeststandard des BSI für Mobile Device Management**
  https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards_Bund/Mobile_Device_Management/Mobile_Device_Management_node.html
- **BSI - SYS.3.2.2 Mobile Device Management (MDM)**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_3_2_2_Mobile_Device_Management_(MDM).html

3.2.4 Sicherung von mobilen Datenträgern

Im Unternehmensumfeld dienen vorrangig mobile Datenträger dazu, Daten zu transportieren und den Austausch von Daten zwischen Mitarbeitern und Projektpartnern an diversen Orten zu ermöglichen. Mobile Datenträger sind kostengünstig, leicht transportierbar und einfach in ihrer Nutzung.

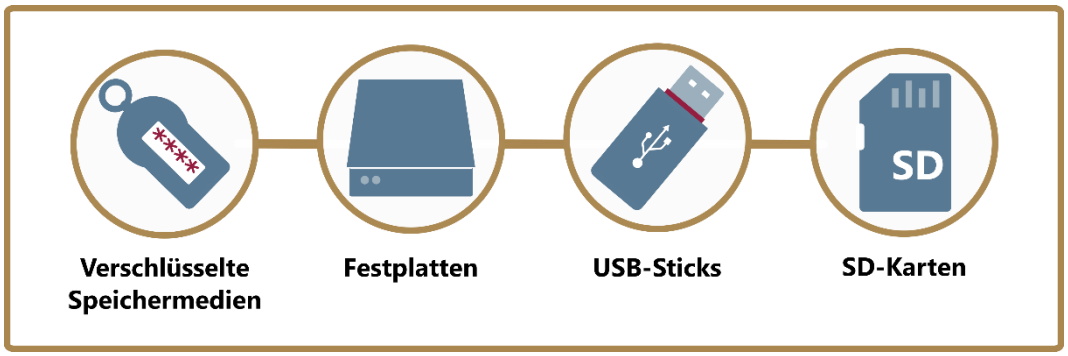
Unter den Begriff „**mobile Datenträger**" fallen jegliche Formen von transportierbaren Speichermedien, welche einmalig oder mehrmalig beschreibbar sind. Darunter fallen z.B.:

- Externe Festplatten
- USB-Sticks
- Speicherkarten
- CD-ROMs, DVDs

Werden vertrauliche Unternehmensdaten ohne Vorkehrungen auf mobilen Datenträgern abgelegt, stellt dies ein großes Sicherheitsrisiko dar. Bei Verlust oder Diebstahl eines solchen ungesicherten mobilen Datenträgers erlangen unberechtigte Personen widerstandslos Einblick in den Inhalt des Datenträgers.

Im Unterschied zu mobilen Endgeräten, bei denen das Betriebssystem eine Schutzschicht für den Datenspeicher bildet, stehen mobile Datenträger schutzlos da. Dies macht Daten auf mobilen Datenträgern gegenüber Missbrauch besonders anfällig. Um die Gefahr bei der Verwendung von mobilen Datenträgern zu minimieren, können neben organisatorischen Richtlinien auch technische Maßnahmen zum Schutz der Vertraulichkeit der Daten getroffen werden.

Abb. 14: Sicherung von mobilen Datenträgern



Die **wesentlichen Maßnahmen zur Sicherung von mobilen Datenträgern** stehen in der folgenden Überblickstabelle:

Richtlinien zur Nutzung von mobilem Datenträger	✓ ○ ✗
Auf die Speicherung von vertraulichen Dateien auf mobilen Datenträgern ist, falls möglich, zu verzichten.	☐ ☐ ☐
Sicherheitsrichtlinien regulieren den dienstlichen Einsatz von mobilen Datenträgern (z.B. welche Datenträger genutzt werden, welche Dateien nicht auf den Datenträgern abgelegt werden dürfen).	☐ ☐ ☐
Die dienstliche Nutzung von privaten mobilen Datenträgern ist verboten oder nur unter strengen Regularien erlaubt.	☐ ☐ ☐
Vor der Verwendung werden mobile Datenträger auf Schadsoftware untersucht (z.B. durch Virenschutzprogramme).	☐ ☐ ☐
Mobile Datenträger werden komplett oder teilweise verschlüsselt (siehe 3.4).	☐ ☐ ☐
Es werden Backups der Daten angelegt.	☐ ☐ ☐
Der Verlust oder Diebstahl von mobilen Datenträgern ist meldepflichtig und es existieren klare Meldewege oder Ansprechpartner (z.B. Informationsschutzbeauftragter, Administrator).	☐ ☐ ☐
Daten auf mobilen Datenträgern werden vor einer Weitergabe oder Ausmusterung sicher gelöscht.	☐ ☐ ☐

Weiterführende Links zum Thema Sicherung von mobilen Datenträgern:

- **BSI - SYS.3.4: Mobile Datenträger**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz Kompendium/bausteine/SYS/SYS_3_4_Mobile_Datentr%C3%A4ger.html
- **BSI - CON.3 Datensicherungskonzept**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz Kompendium/bausteine/CON/CON_3_Datensicherungskonzept.html
- **Kompetenzzentrum Digitales Handwerk - Routenplaner Cybersicherheit für das Handwerk, S. 95 f.**
  https://www.handwerkdigital.de/deulocal/textbilder/images/PDF%20Allgemein/routenplaner_cyber-sicherheit_klickbar.pdf

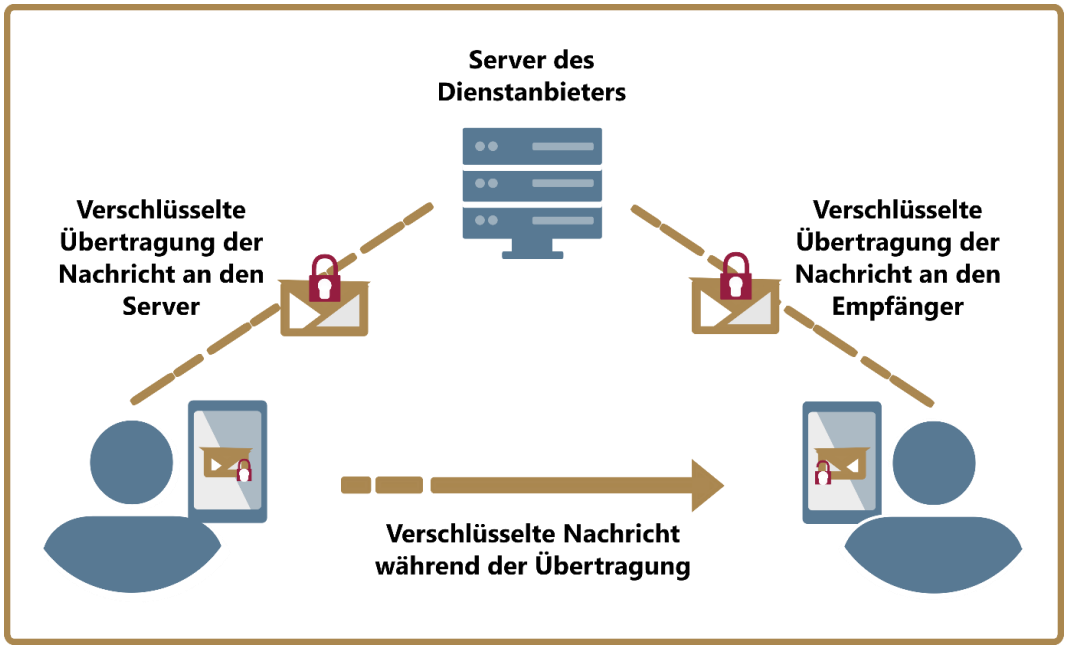
3.3 Verschlüsselung der elektronischen Kommunikation und Datenübermittlung

Die Möglichkeiten zur Unternehmenskommunikation sind vielfältig (z.B. E-Mail, VoIP, Messaging-Dienste). In der Regel werden auch vertrauliche Informationen elektronisch übertragen. Während der elektronischen Übertragung sind unternehmenskritische Daten und Dokumente ungeschützt und können potenziell durch Dritte abgefangen und mitgeschnitten werden. Um eine unberechtigte Einsicht durch Dritte zu vermeiden und eine vertrauliche elektronische Kommunikation zu ermöglichen, müssen zusätzliche IT-Sicherheitsmaßnahmen in Form einer Ende-zu-Ende-Verschlüsselung zur Sicherstellung der Vertraulichkeit, Integrität und Authentizität der übermittelten Daten getroffen werden. Dies kann durch eine Ende-zu-Ende-Verschlüsselung der Kommunikation erfolgen. Wird z.B. eine E-Mail versendet, wird die E-Mail auf dem Transportweg zum Anbieter und vom Anbieter zum Empfänger verschlüsselt. Der Anbieter wäre jedoch theoretisch in der Lage den Nachrichteninhalt der E-Mail einzusehen. Bei einer Ende-zu-Ende-Verschlüsselung kennen nur der Absender und Empfänger den Inhalt der Nachricht. Die Ende-zu-Ende-verschlüsselten E-Mails liegen beim E-Mail-Anbieter nur in verschlüsselter Form vor.

- Die **Vertraulichkeit** des Nachrichteninhaltes wird durch eine **Ende-zu-Ende-Verschlüsselung** gewährleistet.
- Die **Authentizität** der Absender kann verifiziert werden.

Eine der häufigsten Ursachen für unberechtigte Zugriffe bei Unternehmen war laut der SiFo-Studie 2018/2019 das Abfangen digitaler Kommunikation (E-Mail, VoIP). Rund 36 Prozent der befragten Unternehmen gaben an, dass die Täter auf diese Weise unberechtigten Zugriff auf vertrauliche Informationen erhalten haben. Dies spiegelt auch die unzureichende Nutzung von Präventions- und Sicherheitsmaßnahmen im Bereich Datensicherheit und Verschlüsselung wider. Nur etwas mehr als die Hälfte der Unternehmen (rd. 54 Prozent) verfügt über eine verschlüsselte E-Mail-Kommunikation.

Abb. 15: Ende-zu-Ende-Verschlüsselung einer E-Mail-Kommunikation



Die **wesentlichen Maßnahmen zur Verschlüsselung der elektronischen Kommunikation und Datenübermittlung** stehen in der folgenden Überblickstabelle:

Technologien für E-Mail-Verschlüsselung	✓ ○ ✗
Der Datenverkehr mit dem E-Mail-Anbieter wird mit TLS transportverschlüsselt (z.B. SMTPS, IMAPS).	☐ ☐ ☐
Ein E-Mail-Gateway wird als zentrale Ver- und Entschlüsselungsinstanz im Unternehmensnetzwerk verwendet (keine Ende-zu-Ende-Verschlüsselung).	☐ ☐ ☐
Falls keine Ende-zu-Ende-Verschlüsselungslösung vorhanden ist, wird eine manuelle Dateiverschlüsselung für den Anhang der E-Mail genutzt (z.B. eine verschlüsselte PDF-Datei).	☐ ☐ ☐
Inhalt der E-Mail wird mithilfe von Verschlüsselungsstandards wie GNUPG/PGP (Pretty Good Privacy) oder S/MIME (Secure/Multipurpose Internet Mail Extensions) Ende-zu-Ende verschlüsselt. Zugleich wird die Authentizität der Absender verifiziert.	☐ ☐ ☐
VoIP (Voiceover IP)-Sprachtelefonie	✓ ○ ✗
Vermeidung von VoIP-Software auf Arbeitsplatzrechnern, stattdessen werden physische VoIP-Telefone für Telefonate genutzt.	☐ ☐ ☐
SRTP (Secure Real Time Protocol) wird verwendet, um die Sprachdaten von der VoIP-Telefonanlage zum Anbieter zu verschlüsseln.	☐ ☐ ☐
SIPS (Session Initiation Protocol Secure) wird verwendet, um die Signaldaten (Verbindungsaufbau) zu verschlüsseln.	☐ ☐ ☐
Für VoIP-Telefonie wird ein separates Subnetz genutzt.	☐ ☐ ☐
Für eine Ende-zu-Ende-Verschlüsselung nutzen die eingesetzten VoIP-Telefone proprietäre Applikationen.	☐ ☐ ☐
Messaging-Dienste	✓ ○ ✗
Die Übertragung oder Verifikation von öffentlichen Schlüsseln zwischen den Kommunikationspartnern kann über zusätzliche Methoden erfolgen (z.B. Scannen eines QR-Codes, Verifikation der Mobilfunknummer).	☐ ☐ ☐
Chatverläufe, private Schlüssel und andere vertrauliche Daten werden verschlüsselt auf dem Endgerät gespeichert.	☐ ☐ ☐
Der Messaging-Dienst nutzt keine gesammelten Metadaten für eigene Zwecke (z.B. Zeitstempel verschickter Nachrichten, Empfänger, Anzahl der gesendeten Nachrichten).	☐ ☐ ☐
Die genutzten Messaging-Dienste haben eine Ende-zu-Ende-Verschlüsselung implementiert.	☐ ☐ ☐

Weiterführende Links zum Kapitel Verschlüsselung der elektronischen Kommunikation und Datenübermittlung:

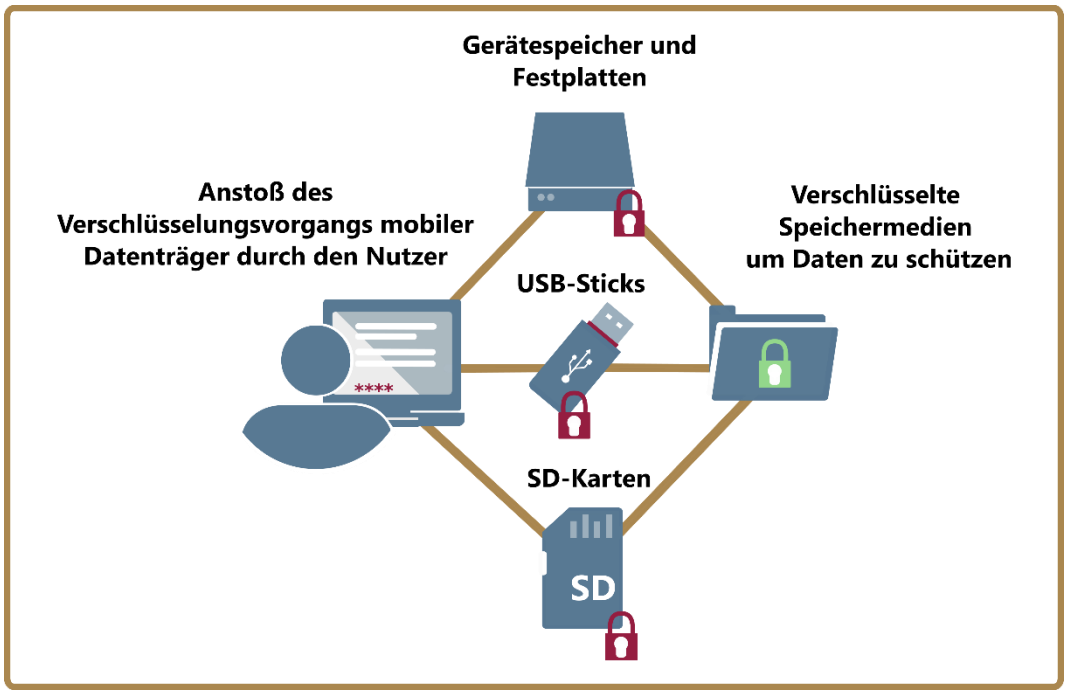
- **BMWi - Kompass IT-Verschlüsselung -**
  1 Daten übertragen - so geht es sicher und verschlüsselt!, S. 6 - 31
  https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/kompass-it-verschluesselung.html
- **Informationsbroschüre von DATEV und Deutschland sicher im Netz e.V.**
  www.teletrust.de/vim/verschluesselung-datev
- **BSI - E-Mail-Verschlüsselung in der Praxis**
  https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/EMail_Verschluesselung/In_der_Praxis/EMails_verschluesseln_in_der_Praxis_node.html
- **BSI - Leitlinie zur Internet-Sicherheit IP-Telefonie**
  www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_voip_leitlinie_pdf.pdf?__blob=publicationFile
- **BSI - Instant Messaging: Tipps**
  https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/KommunikationUeberInternet/Messenger/instantMessenger_node.html
- **Verbraucherzentrale - Messaging-Alternativen: die Datenschutzregeln im Überblick**
  www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen-die-datenschutzregeln-im-ueberblick-13055

3.4 Verschlüsselung des Gerätespeichers

Sobald vertrauliche Daten lokal auf dem Gerätespeicher abgelegt werden, müssen die Gerätespeicher oder bestimmte Bereiche sicher verschlüsselt werden. Viele Betriebssysteme bieten bereits vorhandene Verschlüsselungsfunktionen mit starken kryptografischen Verfahren an, um den Gerätespeicher zu verschlüsseln.

Zur Erhöhung der Plattformunabhängigkeit oder falls das Betriebssystem selbst keine Verschlüsselungsfunktion anbietet, können zusätzliche Anwendungsprogramme verwendet werden, um den Gerätespeicher zu verschlüsseln. Des Weiteren kann der Einsatz von verschlüsselten Container-Dateien in Erwägung gezogen werden. Dabei wird nicht zwingend der gesamte Gerätespeicher verschlüsselt, sondern eine verschlüsselte Container-Datei für vertrauliche Daten angelegt, welche durch eine Passphrase oder eine andere Art der Authentifizierung geschützt wird. Die Einfuhr von verschlüsselter Hardware ins Ausland stellt eine weitere Herausforderung für Unternehmen dar. In zahlreichen Staaten (z.B. Russische Föderation, China) kann die Herausgabe des Passworts oder anderer Merkmale zur Authentifizierung für die verschlüsselten Geräte durch die Sicherheitsbehörden erzwungen werden. Daher sollte bereits vor der Einreise die Rechtslage bekannt sein. Gegebenenfalls sollte auf die Einfuhr von verschlüsselten Geräten verzichtet und stattdessen auf dedizierte Reise-Hardware zurückgegriffen werden (z.B. Reiselaptops ohne sensible Firmendaten, „Wegwerfhandys“).

Abb. 16: Verschlüsselung von mobilen Datenträgern



Die **wesentlichen Maßnahmen zur Verschlüsselung des Gerätespeichers** stehen in der folgenden Überblickstabelle:

Verschlüsselung des Gerätespeichers	✓ ○ ✗
Die kryptografischen Verfahren erfüllen aktuelle Sicherheitsanforderungen (z.B. AES 256, Twofish).	☐ ☐ ☐
Der Gerätespeicher wird durch die Verschlüsselungsfunktion des Betriebssystems verschlüsselt.	☐ ☐ ☐
Es werden zusätzliche Anwendungsprogramme genutzt, um den Gerätespeicher zu verschlüsseln.	☐ ☐ ☐
Speichererweiterungen werden ebenfalls verschlüsselt (z.B. (Micro-) SD-Karten).	☐ ☐ ☐
Vertrauliche Dateien auf dem Gerätespeicher sind dateiverschlüsselt (z.B. verschlüsselte PDF-Dateien).	☐ ☐ ☐
Auf dem Gerätespeicher befinden sich für vertrauliche Dateien verschlüsselte Partitionen, in denen sie abgelegt sind.	☐ ☐ ☐
Es werden verschlüsselte Container-Dateien auf dem Gerätespeicher für die Speicherung von vertraulichen Dateien benutzt.	☐ ☐ ☐

Verschlüsselung mobiler Datenträger	
Vertrauliche Dateien werden durch Anwendungsprogramme verschlüsselt, bevor sie auf dem mobilen Datenträger abgelegt werden (z.B. passwortgeschütztes Archiv).	☐ ☐ ☐
Auf dem mobilen Datenträger werden vertrauliche Dateien in verschlüsselte Container abgelegt.	☐ ☐ ☐
Der komplette Speicher der mobilen Datenträger wird mithilfe der kryptografischen Funktionen des Betriebssystems oder zusätzlichen Anwendungsprogrammen softwareseitig verschlüsselt.	☐ ☐ ☐
Die eingesetzten mobilen Datenträger besitzen eine Hardwareverschlüsselung und sind z.B. durch PIN vor dem Zugriff Unbefugter geschützt.	☐ ☐ ☐

Weiterführende Links zum Thema Verschlüsselung des Gerätespeichers:

- **BMWi - Kompass IT-Verschlüsselung – 2 Daten sicher ablegen – dank Verschlüsselung!, S. 32 - 37**
  https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/kompass-it-verschluesselung.html
- **BSI - Verschlüsselung auf mobilen Geräten**
  https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/VerschluesselungMobil/verschluesselungMobil_node.html
- **BSI - Kryptografische Verfahren: Empfehlungen und Schlüssellängen**
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile
- **BSI - CON.1 Kryptokonzept**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_1_Kryptokonzept.html
- **BSI - CON.3 Datensicherungskonzept**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_3_Datensicherungskonzept.html

3.5 Sichere Weitergabe und Ausmusterung

Für die sichere Weitergabe und Ausmusterung von mobilen Endgeräten oder Datenträgern müssen Sicherheitsrichtlinien und entsprechend sichere Verfahren existieren. Wird die Weitergabe und Ausmusterung ohne die nötige Sorgfalt betrieben, können vertrauliche Informationen an Dritte gelangen und für das Unternehmen gravierende Sicherheitsrisiken entstehen. Zum Beispiel sind Firmengeräte häufig Leasing-Produkte, die nach Auslaufen des Nutzungszeitraums zurückgegeben werden müssen. Die Geräte werden oft anschließend weiterverkauft, was das Risiko eines Informationsabflusses weiter steigern könnte, wenn die Informationen nicht sicher gelöscht werden.

Vor jeder Weitergabe oder Ausmusterung muss der Datenspeicher der mobilen Endgeräte oder Datenträger gelöscht und mehrfach überschrieben werden. Zum einen dient dies dazu, die vorhandenen Daten auf den Geräten unwiderruflich zu löschen, und zum anderen die Daten vor unrechtmäßigen Zugriffen zu schützen. Werden die Daten eines Datenspeichers gelöscht, aber nicht mehrmalig überschrieben, können Dritte unter Umständen die gelöschten Daten wiederherstellen. Denn beim Löschen werden nicht die Daten selbst gelöscht, sondern nur die Verweise darauf. Die Daten können durch entsprechende Anwendungsprogramme extrahiert werden. Daher besteht eine sichere Löschung stets aus einem mehrmaligen Überschreiben des Datenspeichers.

Dieser Vorgang ist auch bei mobilen Endgeräten anzuwenden, deren Gerätespeicher zuvor verschlüsselt wurden. Angreifer könnten über Angriffsvektoren an das Passwort zur Entschlüsselung gelangen. Damit hätten sie Zugriff auf die vermeintlich sicher verschlüsselten Daten des weitergegebenen oder des zu entsorgenden Datenspeichers des Gerätes. Mobile Betriebssysteme bieten Funktionen an, um den Datenspeicher auf die ursprüngliche Werkseinstellung zurückzusetzen, wobei der Datenspeicher gelöscht und überschrieben wird. Auch Betriebssysteme für Laptop und Desktop-Rechner können durch zusätzliche Anwendungsprogramme ein mehrmaliges Überschreiben des Datenspeichers ermöglichen.

Abb. 17: Weitergabe und Ausmusterung

Die **wesentlichen Maßnahmen zur sicheren Löschung, Weitergabe und Ausmusterung von Endgeräten und Datenträger** stehen in der folgenden Überblickstabelle:

Weitergabe und Ausmusterung	✓ ○ ✗
Es gibt Sicherheitsrichtlinien für die sichere Weitergabe und Ausmusterung von Geräten.	☐ ☐ ☐
Eine Auswahl geeigneter Verfahren zur sicheren Löschung und Vernichtung von Datenträgern wurde zusammengestellt.	☐ ☐ ☐
Bevor Daten sicher gelöscht werden, findet ggf. vorher eine Datensicherung statt.	☐ ☐ ☐
Bevor mobile Datenträger oder Geräte weitergegeben werden, findet eine sichere Löschung durch mehrmaliges Überschreiben der darauf befindlichen Daten statt.	☐ ☐ ☐
Vor einer Ausmusterung von Datenträgern oder Geräten werden die darauf befindlichen Daten sicher gelöscht.	☐ ☐ ☐
Es wird stichprobenartig überprüft, ob sich auf den gelöschten Datenspeichern noch wiederherstellbare Informationen befinden.	☐ ☐ ☐
Die Vorgänge zur Löschung, Weitergabe und Ausmusterung werden protokolliert.	☐ ☐ ☐
Die eingesetzten Verfahren werden jährlich überprüft, ob diese dem aktuellen Stand der Technik entsprechen.	☐ ☐ ☐
Die eingesetzten Verfahren und Sicherheitsrichtlinien sind ausreichend dokumentiert.	☐ ☐ ☐
(Optional) werden ausgemusterte Datenspeicher und Geräte physisch zerstört.	☐ ☐ ☐
(Optional) werden vertrauenswürdige externe Dienstleister zur Entsorgung von zu vernichtendem Datenträger beauftragt.	☐ ☐ ☐

Weiterführende Links zum Thema sichere Weitergabe und Ausmusterung bei mobilen Endgeräten:

- **BSI - CON.6 Löschen und Vernichten**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz Kompendium/bausteine/CON/CON_6_L%C3%B6schen_und_Vernichten.html
- **DsiN-Blog - Löschen und Vernichten von Daten**
  https://www.dsin-blog.de/2019/04/17/loeschen-und-vernichten-von-daten/
- **Kompetenzzentrum Digitales Handwerk - Routenplaner Cybersicherheit für das Handwerk, S. 37 f.**
  https://www.handwerkdigital.de/deulocal/textbilder/images/PDF%20 Allgemein/routenplaner_cyber-sicherheit_klickbar.pdf
- **Deutsche Gesellschaft für Datenschutz**
  https://dg-datenschutz.de/wp-content/uploads/2018/10/DGD_Service_Flyer_ Datenloeschung_DE-min.pdf

3.6 Cloud-Computing

Cloudbasierte Dienste nehmen einen zunehmend hohen Stellenwert in vielen Unternehmen ein. Dieser teilweise bereits integrale Bestandteil vieler IT-Infrastrukturen bedarf dabei besonderer Sicherheitsrichtlinien und IT-Sicherheitsmaßnahmen im Rahmen des IT-Sicherheitskonzepts. Der Begriff Cloud-Computing beschreibt IT-Systeme und Ressourcen, die ggf. auch von Drittanbietern bereitgestellt werden und über das Internet erreichbar sind. Bei der Auswahl eines passenden Cloud-Anbieters spielt insbesondere die Frage, welches Datenschutzrecht Anwendung findet, eine zentrale Rolle. Lagern Cloud-Anbieter ihre Dienstleistungen außerhalb des Rechtsraums der EU aus, sollte eine Grundsatzüberlegung getroffen werden, diesen Anbieter überhaupt zu nutzen. Es sollte zwingend festgestellt werden, welche Daten grundsätzlich in der Cloud verarbeitet und gespeichert werden sollten.

Der Zugang oder die Nutzung von Cloud-Diensten ist in der Regel nur über ein internetfähiges Gerät möglich. Daher muss der Zugang zu Cloud-Diensten besonders geschützt werden. Um die Daten in der Cloud vor Einblicken Dritter und Datendieben zu schützen, müssen die Zugänge mit starken Authentifizierungsmechanismen ausgestattet werden. Zusätzlich müssen die Daten während der Übertragung (Data-in-Motion) und Speicherung (Data-at-Rest) in der Cloud mit kryptografischen Verfahren sicher verschlüsselt werden, um einen hohen Sicherheitsstandard gewährleisten zu können. Zudem müssen die Geräte, von denen auf die Cloud zugegriffen werden, ausreichend gegen Cyber-Bedrohungen gehärtet sein.

Abb. 18: Sicherheitsaspekte beim Cloud-Computing

Die **wesentlichen Maßnahmen zum sicheren Cloud-Computing** stehen in der folgenden Überblickstabelle:

Sichere Nutzung von Cloud-Diensten	✓ ○ ✗
Streng vertrauliche Informationen, deren Diebstahl sich verheerend für das Unternehmen auswirken würde, sind von der Speicherung in der Cloud ausgeschlossen.	☐ ☐ ☐
Es existiert eine Sicherheitsrichtlinie für die sichere Nutzung von Cloud-Diensten.	☐ ☐ ☐
Die Nutzung von Cloud-Anbietern aus Ländern mit niedrigem Datenschutzniveau oder außerhalb der EU ist ausgeschlossen.	☐ ☐ ☐
Der physische Standort der genutzten Cloud-Infrastruktur des Cloud-Anbieters liegt im deutschen bzw. im EU-Rechtsraum.	☐ ☐ ☐
Die Auswahl eines Cloud-Anbieters wurde unter Berücksichtigung der eigenen Sicherheitsanforderungen getroffen (z.B. Einsatz von Verschlüsselung, physischer Speicherort der Daten, Rückgabe bzw. Datenlöschung nach Beendigung).	☐ ☐ ☐
Der Cloud-Anbieter erbringt in regelmäßigen Abständen Nachweise über seine Sicherheitsstandards (z.B. nach BSI-Grundschutz, ISO 27001).	☐ ☐ ☐
Der Cloud-Dienstleister ist zur unverzüglichen Meldung von etwaigen Sicherheitsvorkommnissen verpflichtet.	☐ ☐ ☐
Nach Möglichkeit ist der Zugang zum Cloud-Dienst mit einer Zwei-Faktor-Authentifizierung geschützt (z.B. Biometrie, TAN, Security-Token).	☐ ☐ ☐
Die End-Point-Security der Endgeräte, von denen auf Cloud-Dienste zugegriffen wird, haben ein hohes Sicherheitsniveau (z.B. aktuelle Sicherheitsupdates, Firewall).	☐ ☐ ☐
Die Datenübertragung zum Cloud-Anbieter ist mit einer Transportverschlüsselung verschlüsselt (Data-in-Motion).	☐ ☐ ☐

Dateien oder Ordner werden vor der Datenübertragung in den Cloud-Speicher clientseitig verschlüsselt, sodass nur verschlüsselte Dateien hochgeladen werden (Data-at-Rest).	
Links für freigegebene Dateien oder Ordner haben ein festgelegtes Ablaufdatum.	
Der Zugang zu freigegebenen Dateien ist mit einem starken Passwort oder anderem Authentifizierungsverfahren geschützt.	

Weiterführende Links zum Thema Cloud-Computing:

- **BMWi - Kompass IT-Verschlüsselung - 2.3 Cloud-Speicher-Dienste und Verschlüsselung, S. 40**
  www.bmwi.de/Redaktion/DE/Publikationen/Studien/kompass-it-verschluesselung.html
- **BSI - Überblickspapier Online-Speicher**
  www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Online-Speicher_pdf.pdf?__blob=publicationFile
- **BSI - Sichere Nutzung von Cloud-Diensten**
  www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sichere_Nutzung_Cloud_Dienste.pdf?__blob=publicationFile&v=8
- **Kompetenzzentrum Digitales Handwerk - Routenplaner Cybersicherheit für das Handwerk, S. 55 f.**
  https://www.handwerkdigital.de/deulocal/textbilder/images/PDF%20Allgemein/routenplaner_cyber-sicherheit_klickbar.pdf

4 Glossar

Ad-Blocker	Auch Werbeblocker genannt. Ein zusätzliches Programm, das beim Surfen im Browser Werbung blockiert.
Administrator	ist ein Benutzer bzw. eine Benutzergruppe mit erweiterten Zugriffsrechten bzw. Zugriffkontrolle.
Applikationen	werden auch Apps genannt und sind Programme, die sowohl auf Desktop-Rechnern als auch in mobilen Endgeräten wie Smartphones zu finden sind.
Authentifikation	Identitätsprüfung eines Benutzers als Zugangs- und Rechtekontrolle für ein System (z. B. durch Passwort).
Authentifizierung	Prüfung der behaupteten Authentisierung auf Echtheit.
Authentisierung	Nachweis einer Person, ob sie wirklich diejenige Person ist, die sie vorgibt zu sein.
Authentizität	ist eines der Schutzziele der Informationssicherheit. Sie beschreibt die Echtheit von Daten.
Biometrie	Darunter sind biologische Merkmale zu verstehen, die eine Person identifizieren oder verifizieren können.
BYOD (Bring Your Own Device)	ist die Nutzung von privaten Endgeräten für den betrieblichen Einsatz.
CEO-Fraud	ist eine spezielle Phishing-Methode, welche unter falscher Identität der Unternehmensführung zur Überweisung von Geld verführen soll.
Cloud-Computing	stellt die Nutzung von nicht lokalen Diensten oder einer IT-Infrastruktur über das Internet dar.
Container	sind verschlüsselte virtuelle Behälter für die Lagerung von Dateien.
Data at Rest	bezeichnet Daten, die auf Datenträger gespeichert sind.
Data in Transit	sind Daten, die über ein öffentliches Netzwerk wie das Internet fließen, und Daten, die im Rahmen eines privaten Netzwerks wie eines lokalen Firmen- oder Unternehmensnetzwerks (LAN) fließen.
E-Mail Gateway	ist ein zentraler Knotenpunkt im Netzwerk, in dem ausgehende und eingehende E-Mails automatisiert verschlüsselt bzw. entschlüsselt werden können.
Ende-zu-Ende-Verschlüsselung	Die übertragenen Daten werden auf der Senderseite verschlüsselt und erst auf der Empfängerseite wieder entschlüsselt, sodass die Datenübertragung über alle Übertragungsstationen hinweg verschlüsselt ist und von keinem Dritten eingesehen werden kann.
Firewall	Programm, das vor unberechtigten Zugriff schützt.
Firmware	Software, die in elektronischen Geräten eingebettet ist.
GNUPG (GNU Privacy Guard)/ PGP (Pretty Good Privacy)	Bei GNUPG/PGP handelt es sich um eine Software, die verwendet werden kann, um Daten zu verschlüsseln und elektronisch zu signieren. Oft wird GNUPG/PGP benutzt, um E-Mails zu verschlüsseln. Es wird ein asymmetrisches Public-Key-Verfahren verwendet, um die Nachrichten zu verschlüsseln bzw. wieder zu entschlüsseln.

GPS (Global Positioning System)	ist ein globales Navigationssatellitensystem zur Ortsbestimmung.
IDS (Intrusion Detection System)	analysiert den Inhalt des Datenverkehrs eines Netzwerkes auf bedrohliche Inhalte oder Verhaltensmuster und informiert den Administrator.
IMAPS (Internet Message Access Protocol)	ist ein E-Mail-Protokoll, welches zum Lesen und Verwalten von E-Mails dient. Die Verbindung zwischen E-Mail-Client und Server wird mithilfe von TLS verschlüsselt.
Informationsschutzbeauftragter (ISB)	plant und setzt Maßnahmen zum Schutz von Informationen um. Ziel ist es die Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit von aufbewahrten und übermittelten Daten zu gewährleisten. Gleichzeitig ist ein ISB Ansprechpartner für alle Belange der Informationssicherheit.
Integrität	ist eines der Schutzziele der Informationssicherheit. Sie beschreibt die Unversehrtheit der Daten vor unautorisierten Modifikationen Dritter.
Intranet	ist dem eigentlichen Internet ähnlich. Es ist ein standortübergreif-endes Netzwerk, welches ausschließlich die Netzwerk-Infrastruktur des Unternehmens nutzt. Ausschließlich autorisierte Mitarbeiter haben Zugang.
IPS (Intrusion Prevention System)	In der Funktionsweise ähnlich zu IDS, jedoch mit dem Unterschied, nicht nur Angriffe zu erkennen, sondern auch abzuwehren.
IT-Infrastruktur	besteht meistens aus dem Unternehmensnetzwerk, den Servern und den Desktop-Computern.
LAN (Local Area Network)	beschreibt ein lokales Heim- oder Unternehmensnetzwerk.
MAC-Adresse (Media-Access-Control-Adresse)	ist eine eindeutige Hardware-Adresse des Netzwerkadapters. Sie dient zur eindeutigen Identifikation in Rechnernetzen. Je nach Betriebssystem ist sie auch unter Physikalischer Adresse oder Ethernet-ID bekannt.
MAC-Filter	dient als Netzwerkzugangsschutz, der Geräten nur mit bestimmter MAC-Adresse Zugang gestattet.
Master-Passwort	siehe Passwortmanager.
Messaging-Dienste	sind Softwarelösungen zum Austausch von Kurznachrichten, zumeist in Textform oder aber auch in anderen Datenformaten wie Audio- und Videoform.
Mobile Device Management	dient zur zentralen Konfiguration und Verwaltung von mobilen Endgeräten im Unternehmensumfeld.
Monitoring	(Dauer-)Beobachtung eines Systems.
Multi-Faktor-Authentifizierung (MFA)	benötigt mehrere Merkmale, um die Zugangsberechtigung zu autorisieren.
Multimedia Messaging Service (MMS)	ist eine Weiterentwicklung der SMS (siehe Short Message Service). Sie ermöglicht multimediale Nachrichten (Dokumente, Bilder, etc.) zu verwenden.
Near Field Communication (NFC)	ist eine kontaktlose Übertragungstechnologie.
Netflow	Ist ein Netzwerkprotokoll zur Erfassung von IP-Datentransfer.

Passwort-Manager	oder Passwort-Safe ist eine Anwendung, die Eingabeinformationen wie Passwörter verwaltet und auch generieren kann. Der Zugriff wird durch ein Master-Passwort gesichert.
Phishing	ist ein Verfahren, mit dem Cyberkriminelle versuchen, Benutzer auf betrügerische Weise zu verleiten, Passwörter oder Nummern von Kreditkarten, Sozialversicherungen oder Bankkonten preiszugeben. Es werden gefälschte E-Mails versendet oder Benutzer werden auf eine gefälschte Webseite umgeleitet.
Risikoanalyse	ist eine systematische Analyse zur Identifikation und Quantifizierung von Risiken.
S/MIME (Secure/Multipurpose Internet Mail Extensions)	ist ein Standard zum Verschlüsseln und Signieren von Dateien anhand von digitalen und zentral ausgestellten Zertifikaten.
Schadsoftware	oder Malware ist schädlicher Quellcode, welcher das Ziel hat, auf dem infizierten informationstechnischen System Schaden anzurichten. Bekannte Beispiele dafür sind Viren, Würmer oder auch Trojaner.
Schlüsseldatei	ist eine Datei, welche als Faktor zur Authentisierung dient. So kann z.B. für das Öffnen einer Datei neben einem Passwort noch zusätzlich eine Schlüsseldatei benötigt werden.
Security-Token (Sicherheitstoken)	fungieren ähnlich wie eine Schlüsseldatei zur Authentisierung. Allerdings ist ein Sicherheitstoken eine Hardwarekomponente meist in Form eines USB-Sticks.
Server	ist ein Rechner, der über das Netzwerk erreichbar ist. Der Server stellt seine Ressourcen für andere Rechner oder Anwendungen bereit, der für andere in einem Netzwerk bestimmte Aufgaben übernimmt und von dem diese ganz oder teilweise abhängig sind.
Short Message Service (SMS)	ist ein Telekommunikationsservice, welcher Kurznachrichten überträgt.
SIPS (Session Initiation Protocol Secure)	ist ein Protokoll für den Austausch von Signaldaten für Echtzeitkommunikation (z.B. für Verbindungsaufbau und -abbau von VoIP-Telefonie). Die Verbindung wird zusätzlich durch TLS verschlüsselt.
Smartcard	ist eine Chipkarte mit kryptografischen Sicherheitsfunktionen.
SMTPS (Simple Mail Transfer Protocol Secure)	ist ein E-Mail-Protokoll zum Versenden von E-Mails. Der Transport der E-Mails wird zusätzlich über TLS verschlüsselt.
Social Engineering	beschreibt die zwischenmenschliche Beeinflussung von Personen, um diese so für die eigenen Zwecke zu instrumentalisieren.
SRTP (Secure Real-Time Transport Protocol)	ist ein Transportprotokoll für Echtkommunikation und verschlüsselt mittels TLS (z.B. bei VoIP-Telefonie).
SSH (Secure Shell)	ist sowohl ein Netzwerkprotokoll als auch entsprechende Programme, die verschlüsselte Netzwerkverbindungen zu einem entfernten Gerät herstellen.
SSL (Secure Sockets Layer)	ist ein Verschlüsselungsprotokoll für den Datentransfer auf der Transportschicht des TCP/IP-Protokollstapels und Vorgänger von TLS.

Subnetting	Segmentierung eines Netzwerkes in mehrere kleinere logische Teilnetzwerke.
TLS (Transport Layer Security)	ist ein Verschlüsselungsprotokoll für den Datentransfer auf der Transportschicht des TCP/IP-Protokollstapels und Nachfolger von SSL.
TPM (Trusted Platform Module)	sind spezielle Hardwarekomponenten mit kryptografischen Funktionen.
Treiber	sind Programme zur Steuerung von Geräten.
Virenschutzprogramme	schützen das Gerät vor Viren und Schadsoftware.
VoIP (Voice-over-IP)	beschreibt die paketvermittelnde Telefonie über das Internet.
VPN (Virtual Private Network)	sind in sich geschlossene virtuelle Kommunikationsnetzwerke, welche genutzt werden, um einen Fernzugriff auf ein Netzwerk zu ermöglichen.
Web-Browser	Programm zur Darstellung von Webseiten. Ermöglicht das Inter-agieren mit Webseiten.
Whitelists	ist eine Positivliste oder Ausnahmeliste, in der Elemente (Personen, Unternehmen oder Programme), welche vertrauenswürdig sind, aufgelistet sind.
WPA (Wi-Fi Protected Access)	ist eine veraltete Verschlüsselungsmethode für drahtlose Netzwerke.
WPA2 (Wi-Fi Protected Access 2)	ist der Nachfolger von WPA und eine Verschlüsselungsmethode für drahtlose Netzwerke.
Zwei-Faktor-Authentifizierung	beschreibt ein Authentifizierungsverfahren, das zwei unterschiedliche Faktoren zur erfolgreichen Authentifizierung benötigt. Z. B. werden ein richtiges Passwort und eine Schlüsseldatei benötigt, um erfolgreich authentisiert zu werden.


Baden-Württemberg
MINISTERIUM FÜR INNERES, DIGITALISIERUNG UND MIGRATION


Sicherheitsforum
Baden-Württemberg
Die Wirtschaft schützt ihr Wissen


Baden-Württemberg
MINISTERIUM FÜR WIRTSCHAFT, ARBEIT UND WOHNUNGSBAU


IHK
Die Industrie- und Handelskammern
in Baden-Württemberg


Baden-Württemberg
LANDESAMT FÜR VERFASSUNGSSCHUTZ


Landesverband der
Baden-Württembergischen
Industrie e. V.


ASW
Baden-Württemberg


KIT
Karlsruher Institut für Technologie


BOSCH
Technik fürs Leben


EnBW


DAIMLER


POLIZEI
BADEN-WÜRTTEMBERG


VDMA


Steinbeis


SAP


BWHT