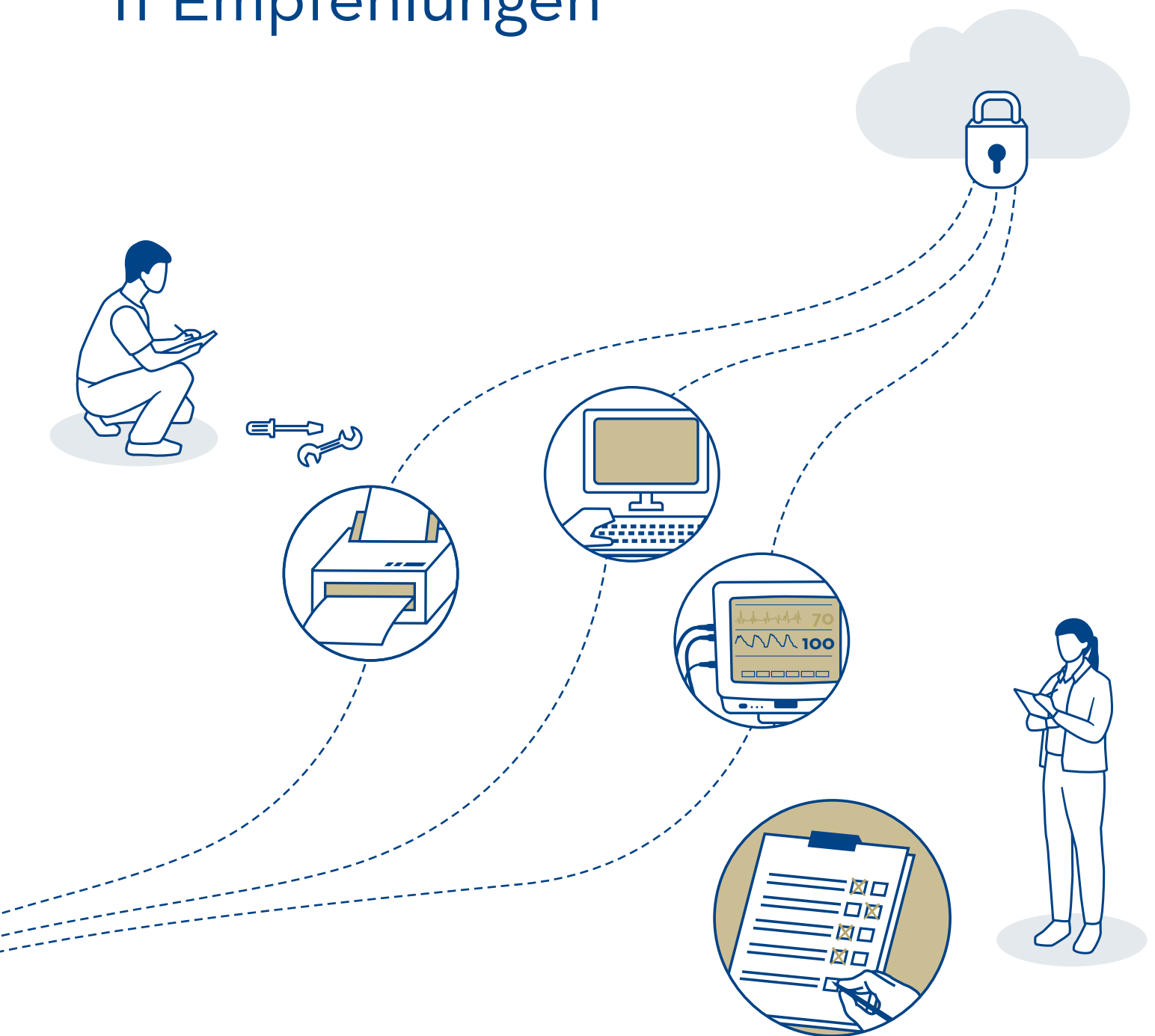


Minimalanforderungen IT-Grundschutz für Praxisärztinnen und Praxisärzte

11 Empfehlungen



Inhaltsverzeichnis

Einleitung	3
Empfehlungen	
Empfehlung 1: Verantwortlichkeiten bestimmen und Vorgaben erlassen	10
Empfehlung 2: ICT-Mittel in ein Inventar aufnehmen	12
Empfehlung 3: Zugriffsschutz regulieren und Benutzerrechte verwalten	14
Empfehlung 4: Praxismitarbeitende für Datensicherheit sensibilisieren	17
Empfehlung 5: Endgeräte vor Schadsoftware schützen	20
Empfehlung 6: Netzwerk schützen	22
Empfehlung 7: ICT-Umgebung konfigurieren und warten	24
Empfehlung 8: Digitale Daten sicher ablegen	26
Empfehlung 9: Digitale Daten sicher austauschen	28
Empfehlung 10: Vorkehrungen für die Behandlung von Sicherheitsvorfällen treffen	30
Empfehlung 11: Externe Dienstleister beauftragen und überwachen	32
Anhang	35
Bearbeitungsverlauf	35
Verwendete Hilfsmittel und Referenzen	35
Glossar	37

Einleitung

Die zunehmende Digitalisierung und Vernetzung im Gesundheitswesen eröffnet neue Möglichkeiten und trägt damit zur Verbesserung der Behandlungsabläufe und zur Entwicklung der Qualität in der Medizin bei. Neben den Vorteilen birgt sie jedoch auch Risiken im Bereich des Datenschutzes und der Datensicherheit: Cyberangriffe auf Gesundheitsdaten und auf die ICT-Umgebung können die Privatsphäre von Patientinnen und Patienten beeinträchtigen, das Tagesgeschäft einer Arztpraxis stark einschränken, finanziellen sowie Reputationsschaden nach sich ziehen und nicht zuletzt die Behandlung der Patienten beeinflussen.

Gleichzeitig ist das Vorhandensein von elektronischen Daten ein wichtiger Erfolgsfaktor, wenn es darum geht, die Effizienz einer Praxis zu steigern. Im Rahmen ihrer Tätigkeit erstellen oder mutieren Praxismitarbeitende täglich personenbezogene Daten mit mitunter sehr sensitivem Inhalt und legen diese in digitaler oder analoger Form ab. Die jeweilige Arztpraxis ist dabei für die Gewährleistung des Datenschutzes und der Datensicherheit der durch sie verarbeiteten Daten verantwortlich. Der Gesetzgeber hat medizinische personenbezogene Daten im Bundesgesetz zum Datenschutz (DSG) als besonders schützenswerte Personendaten eingestuft, sodass umfangreiche Massnahmen für einen angemessenen Schutz dieser Daten erforderlich sind. Aufbau, Unterhalt und Wartung einer sicheren ICT-Umgebung, die Erarbeitung von Sicherheitsanforderungen und die Sensibilisierung der Mitarbeitenden zugunsten einer angepassten Datenschutz- und Sicherheitskultur sind umfassende Aufgaben, die personelle und finanzielle Ressourcen erfordern. Um Praxisinhaberinnen und -inhaber zu unterstützen und weil auf Bundesebene bisher keine Empfehlungen vorliegen, hat die FMH Minimalanforderungen zum IT-Grundschutz für Arztpraxen erarbeitet. Diese Minimalanforderungen haben Empfehlungscharakter und beinhalten Anforderungen, die ein Mindestniveau an Sicherheit für Daten, Informationen und die ICT-Umgebung sicherstellen. Die fokussierte Zielgruppe sind kleinere bis mittelgrosse Arztpraxen mit Infrastrukturen von geringer Komplexität.

Datensicherheit und Datenschutz ist ein Teilbereich der Informationssicherheit und umfasst den Schutz der Daten vor Einsicht und Veränderbarkeit durch unautorisierte Parteien (Vertraulichkeit und Integrität) sowie die Aufrechterhaltung des reibungslosen Betriebs der ICT-Umgebung (Verfügbarkeit). Zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit sowie zur Sicherstellung der Konformität mit dem DSG ist die Umsetzung organisatorischer, technologischer und menschlicher Massnahmen erforderlich. Die nachfolgenden Empfehlungen sollen Ihnen helfen, den Aufbau und den Erhalt des Datenschutzes und der Datensicherheit in Ihrer Arztpraxis zu gewährleisten.

Zielgruppe

Die Empfehlungen der FMH richten sich an kleine und mittelgrosse Arztpraxen und die dazugehörige ICT-Umgebung. Die Anforderungen und Massnahmen wurden in Interviews mit Praxisinhabern validiert und sind für Arztpraxen mit bis zu zwölf Ärzten zweckmässig. Direkter Adressat dieser Empfehlungen sind die Ärzteschaft, Mitarbeitende der Praxis sowie beauftragte Dritte (z.B. ICT-Dienstleister).

Zielsetzung

Zur Sicherstellung der Datensicherheit und des Datenschutzes in der Arztpraxis wurden Minimalanforderungen zum IT-Grundschutz im Sinne von elf Empfehlungen ausgearbeitet. Bei der Ausarbeitung der Empfehlungen wurden die Grösse, die Komplexität der ICT-Landschaft, die Anzahl der Mitarbeitenden sowie das Risikoprofil der Arztpraxen mitberücksichtigt. Der Umfang der Empfehlungen wurde dementsprechend auf die vorhandenen personellen und finanziellen Ressourcen angepasst.

Die Empfehlungen der FMH sollen zu einem angemessenen Schutz sensibler Daten in Arztpraxen beitragen. Dabei wird den gesetzlichen Anforderungen an den Schutz besonders schützenswerter Personendaten Rechnung getragen.

Gefahren

In der Arztpraxis wird täglich bei der Patientenaufnahme, der Disposition, der Behandlung oder bei der Abrechnung mit sensiblen Informationen, den medizinischen und den Patientendaten, gearbeitet. Die Daten sind unter Berücksichtigung von technologischen, organisatorischen und menschlichen Faktoren unterschiedlichen Gefahren ausgesetzt. Diese Gefahren bilden aufgrund von Schwachstellen, beispielsweise in der Hard- und Software, in den Prozessen oder im Verhalten der Praxismitarbeitenden und der Ärzteschaft potentielle Bedrohungen. Wenn ein Angreifer diese Schwachstellen ausnutzt, kann dies die Vertraulichkeit, Verfügbarkeit oder Integrität von medizinischen und Patientendaten gefährden. Gefahren sind sowohl technischer Natur als auch das Ergebnis fehlender Sensibilisierung von Praxismitarbeitenden und der Ärzteschaft, die somit zu einem beliebten Angriffsziel bei Social-Engineering-Attacken werden. Die nachfolgende Grafik zeigt beispielhaft die ICT-Umgebung einer Praxis und die Interaktion mit externen ICT-Dienstleistern, Patientinnen und anderen Gesundheitseinrichtungen, wie zum Beispiel Spitälern. Die gelben Kreise mit den Ausrufezeichen zeigen mögliche Gefahren auf.

1. Schadsoftware sind Programme, die entwickelt wurden, um unerwünschte und gegebenenfalls schädliche Funktionen auf Endgeräten auszuführen, zum Beispiel Ransomware, auch Erpressungssoftware genannt, die auf dem Gerät installiert wird. Diese Art von Software blockiert den Zugriff auf die Daten sowie die Nutzung des Endgeräts und fordert für die Freigabe eine Lösegeldsumme. Schadsoftware kann via Datenträger (USB-Stick), E-Mail-Anhänge oder über Cloud-Dienste auf das Endgerät gelangen.
2. Social-Engineering-Angriffe haben den Menschen als Ziel und versuchen, durch manipulative E-Mails, Anrufe oder Instant Messages, Kreditkarteninformationen oder Passwörter herauszufinden, um so den Zugang zum Endgerät zu erhalten. Unachtsamkeit beim Surfen im Internet oder bei der Kommunikation per E-Mail, beispielsweise durch das Öffnen von E-Mail-Anhängen, kann dazu führen, dass Schadprogramme auf das Endgerät gelangen. Ausserdem können wesentliche Bedrohungen im Zusammenhang mit menschlichen Fehlern entstehen, beispielsweise der Versand von Patientinformationen an einen falschen Empfänger.
3. Der unverschlüsselte Datenaustausch per E-Mail zwischen Arztpraxis, Patienten und den Akteuren der Gesundheitsbranche ermöglicht es einem Angreifer, die Kommunikation mitzulesen und sensible Informationen abzufangen. Zudem können Fehlzustellungen zu einer Offenlegung von sensitiven Informationen führen.

4. Die Nutzung von Cloud-Diensten zur Datenablage für primäre Daten oder des Backups kann potenzielle Bedrohungen in Sachen Vertraulichkeit und Integrität von Daten mit sich bringen, da je nach gewähltem Cloud-Modell die Einsicht durch den Anbieter nicht unterbunden werden kann. Die unverschlüsselte Ablage in der Cloud oder der unverschlüsselte Up- und Download in die und von der Cloud ermöglicht es Angreifern, die Daten abzufangen oder einzusehen. Die Abhängigkeit der Arztpraxis vom Anbieter und von der Cloud-Lösung schwächen die Position der Arztpraxis. Die Möglichkeiten zur Kontrolle der vertraglichen Vereinbarung bezüglich des Datenschutzes und der Datensicherheit sowie der Datenbearbeitung durch den Anbieter sind oftmals eingeschränkt, weshalb der Leistungsbezug auf Vertrauen basiert. Angriffe auf Cloud-Plattformen sind aufgrund der Skalierbarkeit des Angriffes ein lohnendes Ziel, da mehr Schaden angerichtet respektive mehr Daten kapitalisiert werden können.

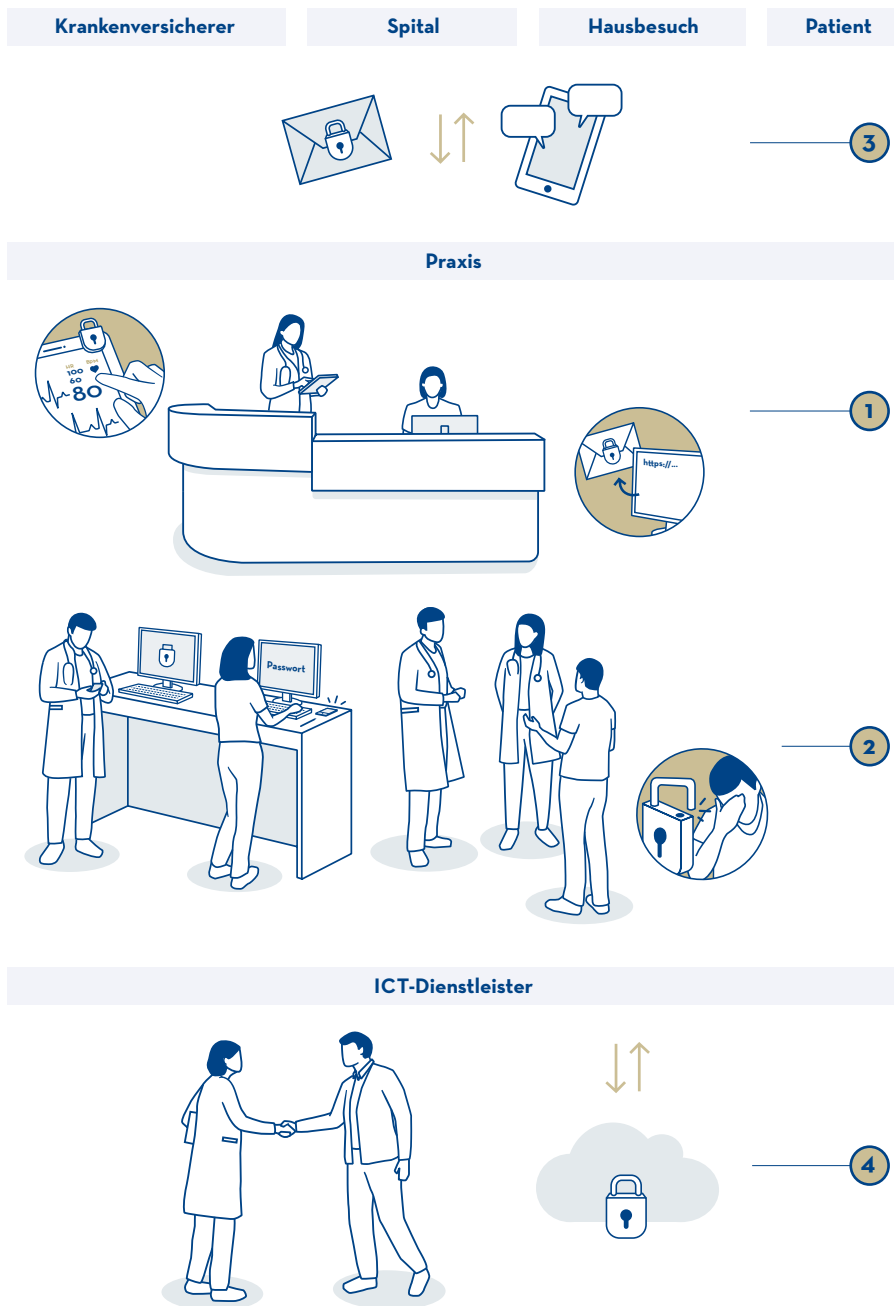


Abbildung 1
Beispiel einer ICT-
Umgebung einer Praxis

Das nachfolgende Szenario soll beispielhaft aufzeigen, wie sich die erläuterten Gefahren in einer Praxis manifestieren können. Angreifer sind vor allem an Daten, die sie kapitalisieren können, oder an der direkten Erbeutung von Geld interessiert. Diese Ziele können auf verschiedene Weise erreicht werden. Der Angreifer sendet beispielsweise eine E-Mail mit Schadsoftware, die in einem Bewerbungsdokument eingebettet ist, oder eine E-Mail mit einem Link zu einem Gewinnspiel. Beim Anklicken des angehängten Dokuments oder des Links verbreitet sich die Schadsoftware auf dem Endgerät und blockiert den Zugriff auf den Computer und entsprechende Ressourcen. Dies nennt man einen Ransomware-Angriff, bei welchem der Angreifer den Zugriff auf den Computer erst wieder freigibt, nachdem die von ihm geforderte Geldsumme bezahlt wurde.

Ein Angreifer kann sich auch als Support-Mitarbeitender eines Softwareherstellers getarnt bei Mitarbeitenden der Praxis melden, um die Verifizierung von Passwörtern und Benutzernamen einzufordern. Geben Mitarbeitende ihm diese Informationen preis, hat er je nach Aufbau der Infrastruktur die Möglichkeit, auf Endgeräte zuzugreifen. Diese Art von Angriffen nennt man Phishing (per Mail) oder Vishing (per Telefon); sie sind dem Social Engineering zuzuordnen. Um an die Endgeräte zu gelangen, verschafft sich ein Angreifer unbemerkt Zugang zur Praxis oder er geht mit dem Vorwand, auf jemanden zu warten, in die Praxis. Sobald er unbeaufsichtigt ist, kann er sich in einem Behandlungszimmer Zugang zu einem Endgerät verschaffen. Ein nicht gesperrter Computer, schwache Passwörter oder umfängliche Benutzerberechtigungen erleichtern ihm den Zugriff auf sensible Daten.

Die Liste der genannten Gefahren ist nicht abschliessend und wird sich zukünftig verändern und erweitern, da die Entwicklung innovativer Technologien auch die Weiterentwicklung von Angriffsmethoden vorantreibt. Die Bedrohungen der Sicherheit und des Schutzes von Informationen und personenbezogenen Daten werden infolge der zunehmenden technologischen Veränderungen, die sowohl private als auch geschäftliche Bereiche tangieren, zunehmen. Gleichzeitig werden sich die regulatorischen Vorgaben im Bereich Datenschutz durch den Gesetzgeber der Schweiz oder der Europäischen Union intensivieren und zum Ausbau der nötigen Schutzmassnahmen führen.

Die Publikation des IKT-Minimalstandards der Bundesverwaltung, das Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union sowie die Überarbeitung des Schweizerischen Bundesgesetzes zum Datenschutz (DSG) sind lediglich die ersten Schritte in diese Richtung. Die Wahrnehmung und das Sicherheitsbewusstsein sowohl der Praxismitarbeitenden und der Ärzteschaft als auch derjenigen, die Berührungspunkte mit schützenswerten Daten und Informationen haben, müssen künftig noch vermehrt mit Sensibilisierungsmassnahmen gesteigert werden. Die konventionellen Bereitstellungsmodelle, beispielsweise die Dauerlizenz (einmaliger Kauf) für die Nutzung auf einem Endgerät, werden zukünftig höchstwahrscheinlich nicht mehr zur Verfügung stehen und durch Cloud-Lösungen kontinuierlich substituiert.

Verbindlichkeit

Das vorliegende Dokument enthält Empfehlungen zur Sicherstellung des IT-Grundschutzes und damit verbunden zur Aufrechterhaltung und Gewährleistung einer angemessenen Datensicherheit und leistet somit einen Beitrag zur Einhaltung des gesetzlich geforderten Datenschutzniveaus in Arztpraxen.

Aufbau

Die Minimalanforderungen IT-Grundschutz beinhalten elf Empfehlungen für Praxisinhaberinnen und -inhaber, Praxismitarbeitende und externe ICT-Dienstleister und bestehen aus drei Dokumenten mit zunehmendem Detaillierungsgrad der Ausführungen für die entsprechenden Zielgruppen.

Das erste Dokument ist eine grafische Übersicht der elf Empfehlungen. Das zweite Dokument beinhaltet die elf Empfehlungen mit zusammenfassenden Informationen zu den Massnahmen (11-Punkte-Programm). Das dritte und vorliegende Dokument zu den detaillierten Massnahmen enthält ausführliche Informationen zu den elf Empfehlungen und den konkreten Massnahmen. Die grafische Übersicht und das 11-Punkte-Programm richten sich primär an Praxisinhaberinnen und -inhaber sowie Mitarbeitende. Die detaillierten Massnahmen (in diesem Dokument) richten sich primär an externe ICT-Dienstleister und in zweiter Linie an die Praxisinhaber und deren Mitarbeitenden. Die nachfolgende Grafik zeigt die Dokumenthierarchie der Minimalanforderungen IT-Grundschutz und die Zielgruppe pro Dokumentstufe (siehe Abbildung 2).




	 Grafische Übersicht	 11-Punkte Programm	 Detaillierte Massnahmen
Praxisinhaber/-in	○	○	●
Praxismitarbeiter/-in	○	○	●
ICT-Dienstleister/-in	×	×	●

Abbildung 2
Dokumenthierarchie
Minimalanforderungen
IT-Grundschutz und
Zielgruppe pro Dokument

Die Minimalanforderungen IT-Grundschutz beinhalten die folgenden elf Empfehlungen:

- Empfehlung 1: Verantwortlichkeiten bestimmen und Vorgaben erlassen
- Empfehlung 2: ICT-Mittel in einem Inventar aufnehmen
- Empfehlung 3: Zugriffsschutz regulieren und Benutzerrechte verwalten
- Empfehlung 4: Praxismitarbeitende für Datensicherheit sensibilisieren
- Empfehlung 5: Endgeräte vor Schadsoftware schützen
- Empfehlung 6: Netzwerk schützen
- Empfehlung 7: ICT-Umgebung konfigurieren und warten
- Empfehlung 8: Digitale Daten sicher ablegen
- Empfehlung 9: Digitale Daten sicher austauschen
- Empfehlung 10: Vorkehrungen für die Behandlung von Sicherheitsvorfällen treffen
- Empfehlung 11: Externe Dienstleister beauftragen und überwachen

Jede Empfehlung ist grundsätzlich identisch aufgebaut und enthält nach der Einführung die Abschnitte Ziel und Zweck sowie Konkrete Massnahmen zur Umsetzung und Sicherstellung der Empfehlung. Im Folgenden werden Empfehlungen mit E und einer Ziffer bezeichnet: E1 bezeichnet die Empfehlung 1, E2 die Empfehlung 2 usw. Die Empfehlungen beinhalten sowohl zwingende als auch optionale Massnahmen. Zwingende Massnahmen sind erforderlich, um ein minimales Sicherheitsniveau zu erreichen. Optionale Massnahmen führen zu mehr Sicherheit und sind als Ergänzung zu den zwingenden Massnahmen zu verstehen.

Zwingende Massnahmen sind in zwei verschiedene Formulierungen anzutreffen:

- «Es sind sichere Passwörter zu verwenden.»
- «Es dürfen nur sichere Passwörter verwendet werde.»

Optionale Massnahmen, welche zu mehr Sicherheit führen, sind in der folgenden Form anzutreffen:

- «Es sollten sichere Passwörter verwendet werden.»

Zur Unterscheidung der Massnahmen und der weitergehenden Informationen wurde eine Identifikationsnummer pro Massnahme und Information verwendet. Die Bestandteile der Identifikationsnummern M-1.01 und I-1.01 haben folgende Bedeutung:

- M oder I steht für Massnahme oder Information.
- 1.01: Die Ziffer vor dem Punkt referenziert auf die Empfehlung.
- 1.01: Die zweistellige Ziffer nach dem Punkt ist der Zähler der Massnahmen oder die Informationen.

Die Beispiele M-1.01 und I-1.01 referenzieren somit auf die Massnahmen und die Information eins der Empfehlung eins.

Abgrenzungen

Das vorliegende Dokument unterliegt den folgenden Abgrenzungen:

- Die vorliegenden Empfehlungen zu den Minimalanforderungen IT-Grundschutz beschränken sich auf Aspekte des technischen und prozessualen Datenschutzes und der Datensicherheit.
- Der Fokus der Empfehlungen zu den Minimalanforderungen IT-Grundschutz liegt auf der elektronischen Datenverarbeitung. Informationen in Papierformat und andere analoge Informationen werden weitgehend ausgeblendet.
- Die vorliegenden Empfehlungen zu den Minimalanforderungen IT-Grundschutz beinhalten ausgewählte Themen, welche gemeinsam mit den Anspruchsgruppen festgelegt wurden.
- Die vorliegenden Empfehlungen zu den Minimalanforderungen IT-Grundschutz erheben keinen Anspruch auf inhaltliche Vollständigkeit und auf eine abschliessende Behandlung der Themenbereiche.
- Die vorliegenden Empfehlungen zu den Minimalanforderungen IT-Grundschutz sind als unabhängig von den Sicherheitsanforderungen im Zusammenhang mit dem elektronischen Patientendossier (EPD) zu betrachten.
- Die Umsetzung der Empfehlungen zu den Minimalanforderungen IT-Grundschutz garantiert keine vollumfängliche Sicherheit.
- Den Empfehlungen liegt ein Risikoprofil einer kleinen und mittleren Arztpraxis zu Grunde. Im Einzelfall kann eine Praxis über ein erhöhtes Risikoprofil verfügen (z.B. Behandlung von Personen mit öffentlichem Interesse, Exposition durch Lage – beispielsweise erhöhte Einbruchgefahr usw.).

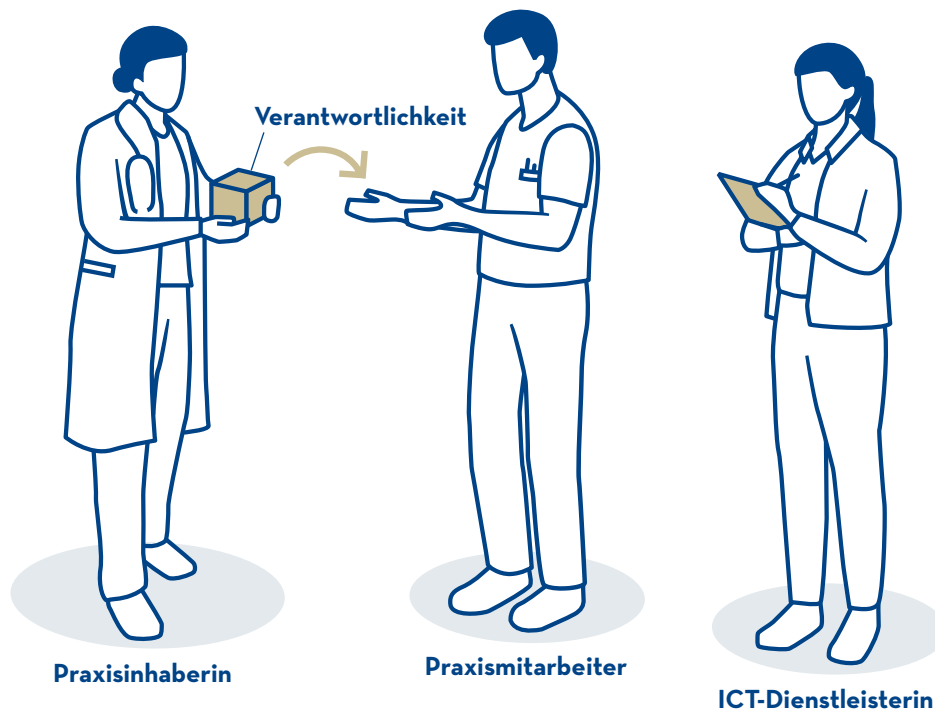
Grundvoraussetzungen

Eine wesentliche Grundvoraussetzung ist die angemessene physische Sicherheit der Praxisräumlichkeiten. Folgende Massnahmen müssen dabei getroffen worden sein:

- Die Praxisräumlichkeiten verfügen über einen Zutrittsschutz. Die Räumlichkeiten sind ausserhalb der Öffnungszeiten abgeschlossen und nur für Berechtigte zugänglich. Während den Öffnungszeiten sind die Räumlichkeiten so ausgelegt, dass eine eintretende Person vom Personal bemerkt wird.
- Fenster und Türen sind ausserhalb der Öffnungszeiten geschlossen und bei erhöhtem Einbruchrisiko (z.B. Erdgeschoss, erhöhte Einbruchszahlen in der Umgebung) durch zusätzlich Massnahmen geschützt.
- Unterlagen in Papierform, welche sensitive Informationen beinhalten, werden in einem abgeschlossenen Behältnis aufbewahrt. Während der Bearbeitung dieser Unterlagen wird die Zwischenlagerung so gehandhabt, dass unberechtigte Personen keine Einsicht haben können.
- Bildschirme innerhalb der Praxisräumlichkeiten sind so positioniert, dass unberechtigte Personen keine Einsicht haben können.
- Server, Netzwerkkomponenten, Speicher und externe Festplatten müssen soweit möglich in einem Raum betrieben und aufbewahrt werden, welcher für Patienten nicht zugänglich ist. Dieser Raum muss abgeschlossen sein. Besteht kein separater Raum, müssen die Komponenten in einem dafür konzipierten, abschliessbaren Schrank betrieben werden.

E1

Verantwortlichkeiten bestimmen und Vorgaben erlassen



Einleitung

Die Geschäftsführerin (Praxisinhaberin) trägt die Gesamtverantwortung, und zwar sowohl für die Sicherheit als auch für den Schutz der Daten, den Betrieb der ICT-Umgebung und ihre Mitarbeitenden. Im organisatorischen Kontext einer Praxis können folgende Rollen identifiziert werden:

- Datenschutz- und Datensicherheitsverantwortlicher (DSDS-V)
- ICT-Betriebsverantwortlicher

Der Datenschutz- und Datensicherheitsverantwortliche übernimmt in seiner Rolle typischerweise die Verantwortung für den Erlass von Sicherheitsvorgaben und je nachdem für die Umsetzung und Überwachung der Einhaltung der Sicherheitsvorgaben. Die Rolle des Datenschutz- und Datensicherheitsverantwortlichen kann durch den Praxisinhaber selbst, den externen ICT-Dienstleister oder einen Praxismitarbeitenden und die Ärzteschaft übernommen werden. Der DSDS-V regelt, wer auf welche Daten und Ressourcen zugreifen darf, und verwaltet die dazugehörigen Berechtigungen.

Die Rolle der DSDS-V ist abzugrenzen von der Rolle der ICT-Betriebsverantwortlichen, die für den Aufbau, den Betrieb und den Unterhalt der ICT-Umgebung verantwortlich ist. Das Verhältnis dieser beiden Rollen ist so zu verstehen, dass die DSDS-V die Anforderungen an den Datenschutz und die Datensicherheit erlässt und die Implementierung auf technischer Ebene an die ICT-Betriebsverantwortliche delegiert.

Die erläuterten Rollen können durch eine oder mehrere Personen wahrgenommen werden.

Die Mitarbeitenden haben die Aufgabe, die Sicherheitsvorgaben der DSDS-Verantwortlichen einzuhalten.

Zweck/Ziel

Die Festlegung der Verantwortlichkeiten bezweckt, dass die Datensicherheit und der Datenschutz praxisintern eine thematische Bedeutung erlangen und dass gleichzeitig eine Ansprechperson für Herausforderungen und Fragen zur Verfügung steht.

Massnahmen

M-1.01 Die Rollen des DS/DS-Verantwortlichen und des ICT-Betriebsverantwortlichen und entsprechende Stellvertretungen sind zu besetzen.

Die Kontaktdaten der Personen, die diese Rollen innehaben, müssen in einer Liste zusammengefasst und allen Praxismitarbeitenden sowie der Ärzteschaft zugänglich und bekannt gemacht werden.

M-1.02 Auf Basis der elf Empfehlungen sind praxisinterne Sicherheitsvorgaben sowie Handlungsanweisungen auszuarbeiten. Mindestens müssen folgende Themen adressiert werden:

- Passwörter und PINs (siehe **E3: Zugriffsschutz regulieren und Benutzerrechte verwalten**)
- Klassifizierung von Daten: Es sollte mindestens zwischen Patientendaten, medizinischen und nicht-medizinischen Daten unterschieden werden.
- Umgang mit ICT-Mitteln (siehe **E3: Zugriffsschutz regulieren und Benutzerrechte verwalten**, **E4: Praxismitarbeitende für Datensicherheit sensibilisieren**, **E5: Endgeräte vor Schadsoftware schützen**)
- Umgang und Austausch von Daten (siehe **E8: Digitale Daten sicher ablegen**, **E9: Digitale Daten sicher austauschen**)
- Vorgehen bei Sicherheitsvorfällen (siehe **E10: Vorkehrungen für die Behandlung von Sicherheitsvorfällen treffen**)
- Zugriffsmatrix und Ablauf Berechtigungsvergabe und -entzug (siehe **E3: Zugriffsschutz regulieren und Benutzerrechte verwalten**)

M-1.03 Die Umsetzung und Einhaltung der Sicherheitsvorgaben (siehe **M-1.02**) sind zu überwachen.

Es ist zu prüfen, ob die Praxismitarbeitenden und die Ärzteschaft die Vorgaben einhalten.

Die Umsetzung der Sicherheitsvorgaben kann anhand einer Checkliste mit den Massnahmen dieses Dokuments geprüft werden. Sofern die ICT-Betriebsverantwortung an einen externen ICT-Dienstleister übertragen wird, sollten die folgenden Nachweise mindestens einmal pro Quartal eingefordert werden:

- Bericht über die Erfüllung der definierten Verfügbarkeitswerte (SLA-Reporting)
- Das Inventar der ICT-Mittel
- Bestätigung bezüglich des Funktionierens der Datensicherung und -wiederherstellung

Die Nachweise sollten je nach Bedarf auch in kürzeren Abständen eingefordert werden können (beispielsweise tägliche Bestätigung des erfolgten Backups oder eine aktualisierte Inventarliste nach jeder Änderung).

M-1.04

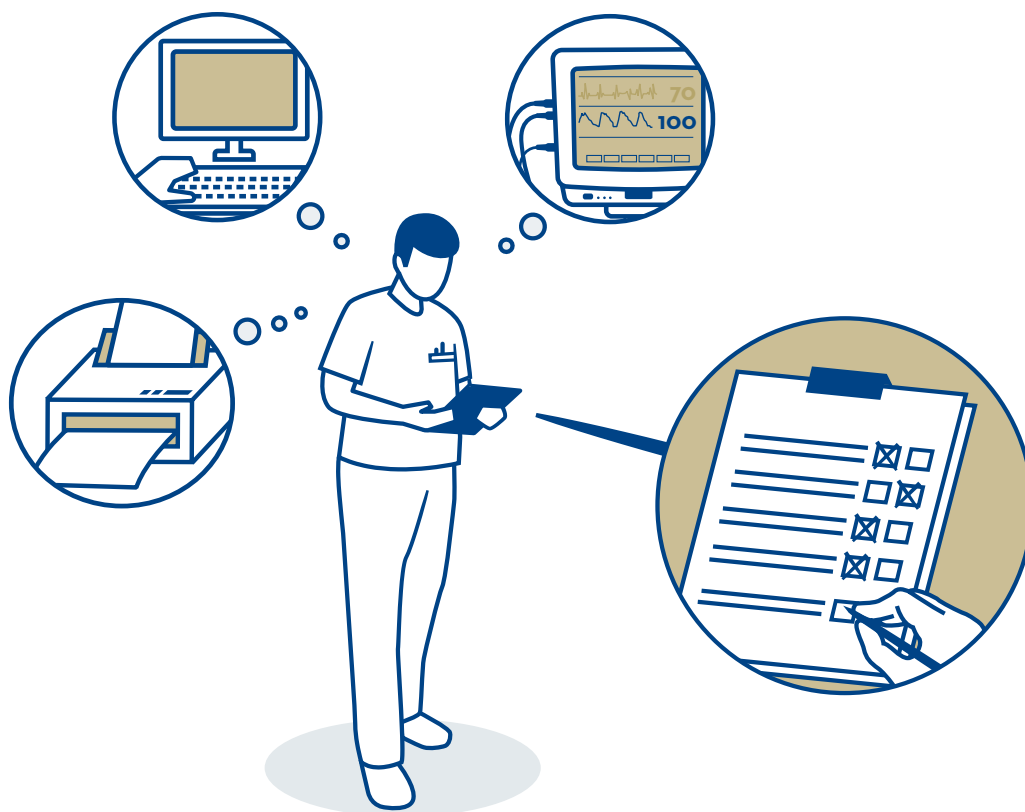
Es ist jährlich zu prüfen, ob die bestehenden Sicherheitsmassnahmen optimiert werden können. Es sollte geprüft werden, ob die Sicherheitsvorgaben (siehe **M-1.02**) aktuell sind, und stichprobenartig ist zu prüfen, ob die technischen Massnahmen greifen.

Sofern Optimierungspotenziale entdeckt werden, sind diese in Abwägung des Aufwandes und des Ertrages zu realisieren und die bestehenden Sicherheitsvorgaben (siehe **M-1.02**) entsprechend anzupassen.

[I-1.01] OPS.1.1.3.A2 Festlegung der Verantwortlichkeiten - Bundesamt für Sicherheit in der Informationstechnik (DE): https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_1_Organisation.html?nn=10137172#doc10095880bodyText15

E2

ICT-Mittel in ein Inventar aufnehmen



Einleitung

Der effektive Schutz von Daten und Informationen bedingt den Einsatz von sicheren ICT-Mitteln. Dabei gilt: Es kann nur geschützt werden, was bekannt ist. Deshalb sind alle schützenswerten ICT-Systeme (beispielsweise Endgeräte und Netzwerke), alle Bestandteile von ICT-Systemen (z.B. Hardware für Netzwerke oder Endgeräte), alle Datenträger, alle medizinischen Geräte (z.B. Laborgeräte, Sterilisierer usw.) sowie alle Anwendungen zu identifizieren, entsprechend der Sensitivität der Daten und Informationen zu klassifizieren und mit zuvor festgelegten Attributen in einer Inventarliste zu dokumentieren.

Zweck/Ziel

Das Inventar der ICT-Mittel dient der Übersicht über die gesamte ICT-Umgebung, die sämtliche in der Praxis verfügbare Hard- und Software umfasst. Die Inventarliste dient als Hilfsmittel bei der Planung von Sicherheitsmassnahmen und verbessert die Reaktionsfähigkeit bei einem Sicherheitsvorfall. Veränderungen, das heisst neue oder ausser Betrieb genommene ICT-Systeme, Hard- und Software sind regelmässig nachzutragen. Das Inventar der ICT-Mittel kann auch als Hilfsmittel zur Planung von ICT-Migrationen und anderen ICT-Projekten herangezogen werden.

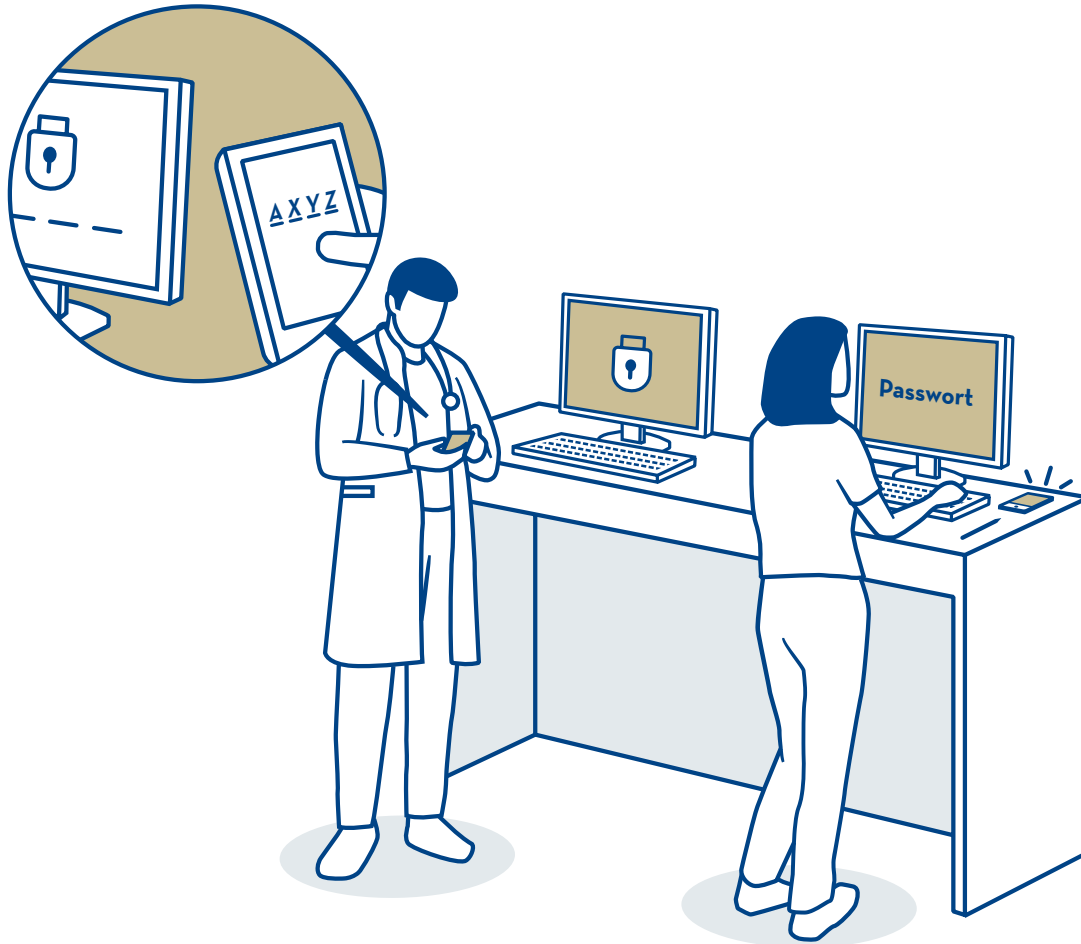
Massnahmen

- M-2.01** Es sind sämtliche ICT-Mittel (siehe Begriffsdefinition Glossar), die in der Arztpraxis eingesetzt oder von ihr zur Verfügung gestellt werden, in einem Inventar, beispielsweise als Excel-Liste, aufzuführen und zu aktualisieren.
- M-2.02** Für sämtliche ICT-Mittel sind mindestens die nachfolgenden Attribute zu dokumentieren:
- Name und Bezeichnung
 - Identifikationsdaten (z.B. System-ID)
 - Verwendungszweck
 - Standort der Hardware
 - Verantwortliche Person
 - Zugriffsrechte auf das ICT-Mittel
 - Adressierungselemente (DNS-Name, IP-Adresse) der Hardware
 - Angaben zur Garantie und Wartung der Hardware
 - Eingesetzte Software-Versionen (Betriebssystem, Antivirus, Applikationen)
 - Ablaufdatum und Aussteller der verwendeten Zertifikate (SSL/TLS-Zertifikate)
- M-2.03** Neue ICT-Mittel sind unmittelbar in das Inventar aufzunehmen und nicht mehr verwendete ICT-Mittel sind umgehend aus dem Inventar zu löschen. Veränderungen an den Attributen **M-2.02** sind im Inventar nachzutragen.
Das Inventar der ICT-Mittel soll mindestens einmal jährlich überprüft und aktualisiert werden.
- M-2.04** Es sind ausschliesslich ICT-Mittel, welche von der Praxis beschafft werden, zu benutzen.
- M-2.05** Bei ausser Betrieb genommenen ICT-Mitteln, insbesondere bei Endgeräten, sind alle Daten unmittelbar nach der Ausserbetriebnahme und vor der Entsorgung vollständig und unwiderruflich zu löschen. Unter der Voraussetzung, dass die Festplattenverschlüsselung **M-7.02** umgesetzt wurde, können die Daten gelöscht oder mit Zufallsdaten überschrieben werden. Andernfalls ist die Massnahme **M-7.02** zuerst umzusetzen.
Die Weitergabe und der Verkauf von ICT-Mitteln sind zu unterlassen.

[I-2.01] ORP.1.A7 Geräteverwaltung - Bundesamt für Sicherheit in der Informationstechnik (DE): https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_1_Organisation.html?nn=10137172#doc10095880bodyText15

E3

Zugriffsschutz regulieren und Benutzerrechte verwalten



Einleitung

Die Verwaltung von Benutzerrechten und Zugriffen umfasst sämtliche Prozesse und Anwendungen, welche der Administration von Zugriffen auf Endgeräte, Applikationen, Daten und Ressourcen dienen. Damit ein Endgerät oder eine Applikation den Zugriff entsprechend der Autorisierung freigibt, müssen sich die Benutzenden authentisieren.

Bei der Authentisierung legen die Benutzenden den Nachweis zur Bestätigung ihrer Identität (Benutzername) vor. Je nach Authentisierungsmethode können die Benutzenden ihre Identität mit der Eingabe einer geheimen Information, die dem Endgerät oder der Applikation bekannt ist (Passwort), oder mit biometrischen Merkmalen, wie zum Beispiel dem Fingerabdruck, dem Gesichts- oder Iris-Scan nachweisen. Im Anschluss daran erfolgt die Prüfung der Identität durch das Endgerät oder die Applikation, dies wird auch Authenti-

fizierung genannt. Die Autorisierung bezieht sich auf die Einräumung der Rechte, die den Benutzenden durch den Dateninhaber gewährt werden.

Zweck/Ziel

Die zentrale Verwaltung und strukturierte Vergabe der Zugriffs- und Benutzerrechte, beispielsweise mittels Active Directory oder alternativen Verzeichnisdiensten, minimiert die Risiken eines unbefugten Zugriffs auf sensiblen Daten durch interne oder externe Parteien. Die regelmässige Wartung der Zugriffs- und Benutzerrechte ermöglicht es, Änderungen durch Ein- und Austritte von Mitarbeitenden zu erfassen und nachzutragen.

Massnahmen

M-3.01 Für den Zugriff auf die medizinischen Daten der Patienten müssen die Praxismitarbeitenden und die Ärzteschaft über ein persönliches Benutzerkonto mit den dazugehörigen Berechtigungen verfügen.

Die Anzahl der Benutzerkonten mit erweiterten Rechten (Administratoren, Poweruser oder ähnliches) sowohl auf den Endgeräten als auch in den Anwendungen sollte möglichst klein gehalten werden.

M-3.02 Die Benutzerrechte sind mindestens für Patienten- und medizinische Daten einzuschränken. Den Benutzenden und den Administratoren sollten nur diejenigen Berechtigungen erteilt werden, die für die tägliche Arbeit notwendig sind (Need-to-Know-Prinzip).

Rolle	Daten			Zuweisung
	Medizinische Daten	Patientendaten	Finanzbuchhaltungsdaten	
User	●	●	×	MPA's
Super User	●	●	●	Praxisinhaber/in oder Chef-MPA
Administratives Personal	×	×	●	Backoffice
Technisches Personal	×	×	×	ICT-Betriebsverantwortliche/r

Abbildung 3
Beispiel Zugriffsmatrix
● uneingeschränkter Zugriff
× kein Zugriff

Die Bewilligung und der Entzug von Zugriffen und Benutzerrechten sollten durch die Praxisinhaberin oder den Praxisinhaber erfolgen, die Vergabe und die Löschung von Benutzerrechten durch die DSDS-Verantwortliche.

M-3.03 Für den Zugriff auf das praxisinterne Netzwerk über das Internet (VPN-Zugang) sind persönliche Benutzerkonten zu verwenden, und zwar mit vorgängiger starker Authentifizierung (zwei unabhängige Faktoren, z.B. Passwort und Token).

M-3.04 Die Benutzerrechte und die Zugriffe sind nach Eintritten und Austritten umgehend anzupassen. Es empfiehlt sich, einmal jährlich alle Benutzerrechte und Zugriffe auf ihre Aktualität und Berechtigung hin zu überprüfen.

M-3.05 Die Fernzugriffe für Wartungszwecke durch externe ICT-Dienstleister haben über separate, persönliche Benutzerkonten zu erfolgen.

Die Aktivitäten auf den Benutzerkonten, wie zum Beispiel Login- und Logout-Versuche, sind zur Erkennung von atypischem Verhalten und zur Sicherstellung der Nachvollziehbarkeit aufzuzeichnen und zu überwachen. Der Zeitpunkt des Fernzugriffs durch externe ICT-Dienstleister sollte vorgängig kommuniziert werden.

M-3.06 Alle Passwörter müssen einmal im Jahr geändert werden. Der Passwortwechsel sollte nach Möglichkeit (beispielsweise für Benutzerkonten) technisch forciert werden. Andernfalls ist der Passwortwechsel organisatorisch sicherzustellen.

M-3.07 Verwendete Passwörter und PINs müssen:

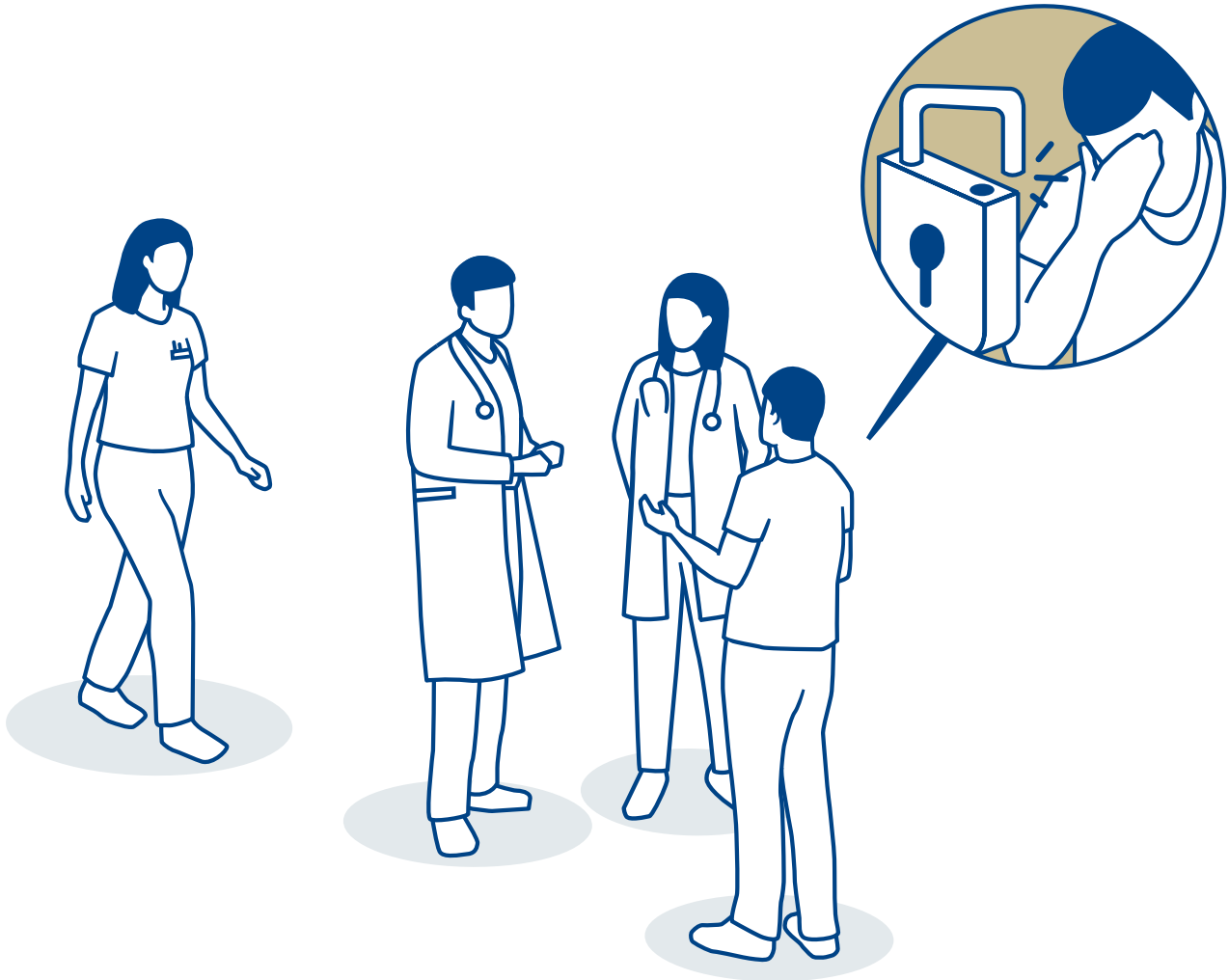
- mindestens 10 Zeichen haben,
- aus Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen zusammengesetzt sein,
- entsprechend weder Buchstaben- noch Zahlenfolgen aufweisen,
- keine Vor- oder Nachnamen, Geburtstage oder Wohnorte enthalten,
- pro Benutzerkonto unterschiedlich sein,
- nur einmal verwendet werden und
- geheim sein.

- M-3.08** Beim Einsatz von biometrischen Verfahren, wie zum Beispiel Fingerabdruck- oder Gesichtserkennung, für Endgeräte, welche von der Praxis zur Verfügung gestellt werden, ist zu beachten, dass neben dem biometrischen Verfahren immer eine PIN oder ein Passwort eingesetzt wird, sodass jedes Endgerät zwei Entsperrungs- und Sperrungsmöglichkeiten hat (siehe **E3: Zugriffsschutz regulieren und Benutzerrechte verwalten**).
- M-3.09** Passwörter sollten in einem Programm zur Passwortverwaltung sicher abgelegt werden und den berechtigten Personen zur Verfügung gestellt werden.
- M-3.10** Das Endgerät ist beim Verlassen des Arbeitsplatzes oder der Arbeitsstation entweder zu sperren oder der Benutzer hat sich abzumelden.

[I-3.01] Factsheet Sichere Passwörter HIN: https://www.hin.ch/wp-content/uploads/2018/08/Checkliste_sichere-Passwoerter.pdf

E4

Praxismitarbeitende für Datensicherheit sensibilisieren



Einleitung

Die Sensibilisierung der Praxismitarbeitenden und der Ärzteschaft umfasst die Aufklärung zum Thema Datenschutz und Datensicherheit sowie die Vermittlung von Vorgaben und Handlungsanweisungen im Falle von Sicherheitsvorfällen. Dabei kann die Sensibilisierung über verschiedene Kanäle, beispielsweise Schulungen, Merkblätter, Ereigniskommunikation oder Weiterbildung, erfolgen.

Zweck/Ziel

Die Mitarbeitenden einer Arztpraxis sind ein beliebtes Angriffsziel für kriminelle Hacker, weshalb Angreifer oftmals versuchen, sich mittels Social-Engineering-Attacken Zugang zur ICT-Umgebung und zu Daten zu verschaffen. Um dies zu verhindern, ist die Sensibilisierung der Praxisverantwortlichen und der Praxismitarbeitenden sowie der Ärzteschaft von zentraler Bedeutung

Die Sensibilisierung bezweckt die gesteigerte Aufmerksamkeit für mögliche Angriffe/Angriffsziele und fördert den sicheren Umgang mit ICT-Mitteln und den bewussten Umgang mit sensiblen Daten.

Massnahmen

- M-4.01** Zur Sensibilisierung der Praxisverantwortlichen und der Mitarbeitenden der Praxis sind Kommunikationskanäle, Themenbereiche sowie der Zeitpunkt der Sensibilisierung festzulegen.
- Es sollte mindestens zu den Sicherheitsvorgaben der **M-1.02** sensibilisiert werden (siehe **E1: Verantwortlichkeiten bestimmen und Vorgaben erlassen**).
- Gefahren
 - Passwörtern und PINs
 - Klassifizierung von Daten und Umgang mit den verschiedenen Klassifizierungen
 - Umgang mit ICT-Mitteln
 - Umgang und Austausch von Daten
 - Vorgehen bei Sicherheitsvorfällen
- M-4.02** Die Praxismitarbeitenden und die Ärzteschaft müssen sowohl beim Eintritt in die Praxis als auch während der Anstellung regelmässig bezüglich der Themen der **M-4.01** sensibilisiert werden, sodass die Aufmerksamkeit für das Thema Datensicherheit und Datenschutz sowie der bewusste Umgang mit Daten nachhaltig gefördert werden. Neu eintretende Mitarbeitende haben zusätzlich zu den Schulungen mittels unterschriebener Einverständniserklärung zu bestätigen, dass sie die praxisinternen Sicherheitsvorgaben verstehen und sie entsprechend einhalten werden.
- M-4.03** Der Bereich Datenschutz und Datensicherheit, insbesondere die in **M-4.01** erwähnten Punkte, sind mindestens zweimal jährlich zu thematisieren, beispielsweise an Teammeetings.
- M-4.04** Zu den Themen von **M-4.01** sollte ein Merkblatt mit Tipps erarbeitet und den Mitarbeitenden ausgehändigt oder an gut sichtbaren Orten, beispielsweise am Arbeitsplatz oder beim Telefon, platziert werden. Das Merkblatt könnte folgendermassen aussehen:

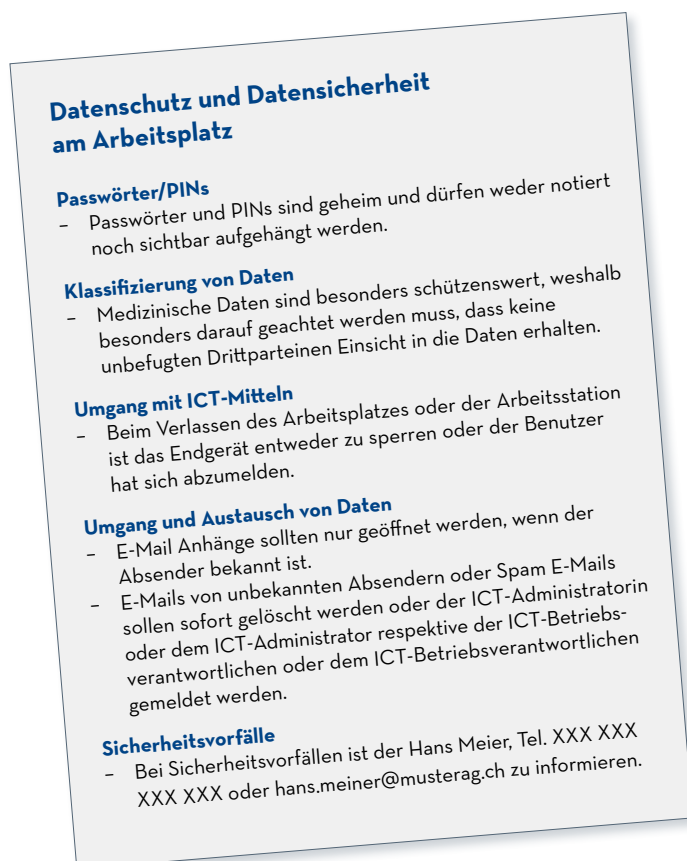


Abbildung 4
Beispiel eines Merkblattes

- M-4.05** Sämtliche Mitarbeitenden sind über sicherheitsrelevante Ereignisse und daraus folgende Konsequenzen sowie eventuelle Anpassungen der Sicherheitsvorgaben (siehe **M-4.01**) zu informieren. Die Kommunikation sollte nach Möglichkeit zeitnah erfolgen, beispielsweise an Teammeetings.
- M-4.06** E-Mail-Anhänge können Schadsoftware enthalten und sollten, wenn der Absender unbekannt ist, nicht geöffnet und das E-Mail sollte gelöscht werden.
Phishing- oder Spam-Mails sollten, ohne auf Verlinkungen oder Anhänge zu klicken und ohne zu antworten, gelöscht werden.
Bei Unsicherheit, ob es sich um eine Phishing- oder Spam-Mail handelt, kann der DSDS-Verantwortliche kontaktiert werden.
- M-4.07** Die private Nutzung der von der Praxis zur Verfügung gestellten ICT-Mittel sollte klar geregelt werden. Die private Nutzung der ICT-Mittel für den Zugriff auf sensitive Daten sollte nicht möglich sein.
Geräte, die sowohl zu geschäftlichen als auch zu privaten Zwecken genutzt werden, sollte zwei Benutzerkonten haben, sodass kein Zugriff vom privaten Benutzerkonto auf die geschäftlichen Daten möglich ist.
Die Nutzung des Internets am Arbeitsplatz mit von der Praxis zur Verfügung gestellten Endgeräten für private Zwecke, beispielsweise für den Zugriff auf private Mailkonten oder das Surfen im Internet, sollte unterlassen oder auf ein Minimum beschränkt werden. Die Beschränkung kann mittels einer hinterlegten Liste von geschäftlich relevanten Internetseiten technisch umgesetzt werden (Whitelisting).

[I-4.01] Verhaltensregeln - Wie schütze ich mich - Melde- und Analysestelle Informationssicherung (MELANI): <https://www.melani.admin.ch/melani/de/home/schuetzen/verhaltensregeln.html>

[I-4.02] HIN Awareness Portal - <https://www.hin.ch/awareness-portal/>

E5

Endgeräte vor Schadsoftware schützen



Einleitung

Schadsoftware bezeichnet Computerprogramme, welche mit dem Zweck erstellt wurden, Daten auf fremden Endgeräten zu stehlen, zu manipulieren oder zu vernichten. Je nach Zweck der Schadsoftware sind Bezeichnungen wie Viren, Würmer oder (Verschlüsselungs-) Trojaner üblich. Solche Schadsoftware wird häufig über E-Mail-Anhänge, Links auf Webseiten oder über Datenträger wie USB-Sticks verteilt.

Zweck/Ziel

Endgeräte wie Smartphones oder Laptops können leicht mit Schadsoftware infiziert werden. Um das Risiko einer Infektion zu reduzieren, müssen alle Endgeräte über ein aktives Virenschutzprogramme verfügen. Diese Programme sollten so konfiguriert sein, dass alle Daten beim Zugriff anhand von bekannten Mustern überprüft werden sowie das Schadsoftware erkannt und deren Ausführung blockieren wird. Mit diesen Massnahmen lässt sich das Risiko von Schadsoftware stark reduzieren. Es gilt jedoch zu beachten, dass Virenschutzprogramme nur bekannte Schadsoftware erkennen. Ein vollständiger Schutz ist damit nicht gewährleistet und ein sensibilisierter Umgang mit potenziellen Gefahren, insbesondere bei der Bearbeitung von E-Mails, Anhängen und Links, bleibt von zentraler Bedeutung (siehe auch E4: Praxismitarbeitende für Datensicherheit sensibilisieren).

Massnahmen

- M-5.01** Alle Endgeräte sind mit einem installierten und aktuellen Virenschutzprogramm auszustatten. Dieses ist so zu konfigurieren, dass alle Dateien beim Zugriff überprüft werden. Zudem müssen die Virensignaturen vom Hersteller mindestens täglich aktualisiert werden. Die Benutzenden dürfen keine Möglichkeit haben, das Antivirusprogramm zu deaktivieren.
Bei der Verwendung von Windows Defender als Antivirenschutzprogramm auf dem Betriebssystem Windows 10 kann der Schutz vor Ransomware als zusätzliche Sicherheitsfunktion aktiviert werden.
- M-5.02** Auf den Endgeräten sollte einmal pro Woche ein vollständiger Scan (Fullscan) durch das Virenschutzprogramm durchgeführt werden. Alarmiert das Virenschutzprogramm, ist dies umgehend der DSDS-V und der ICT-Betriebsverantwortlichen zu melden. Es sollte nach Möglichkeit eine automatische Meldung an die verantwortliche Stelle erfolgen.
- M-5.03** Endgeräte mit Netzwerkanschluss, die von der Praxis zur Verfügung gestellt werden, haben das aktuellste Betriebssystem installiert (siehe auch **M-7.01**). Ausnahmen können genehmigt werden, sofern für das Betriebssystem Sicherheitsupdates zur Verfügung gestellt werden. Applikationen und Apps sind ausschliesslich vom Hersteller oder von offiziellen Stores zu beziehen.
- M-5.04** Der E-Mail-Server ist so zu konfigurieren, dass er die Anhänge von E-Mails auf mögliche Schadsoftware hin überprüft.
- M-5.05** Bei der Verwendung von USB-Sticks ist darauf zu achten, dass keine privaten, unbekannt oder gefundenen USB-Sticks oder solche, die bereits anderorts eingesetzt wurden, mit den Endgeräten, welche von der Praxis zur Verfügung gestellt werden, verbunden werden.
- M-5.06** Die praxisinternen Endgeräte sollten nicht für private Zwecke verwendet werden. Der persönliche Gebrauch kann erlaubt werden, sofern zwei getrennte Benutzerkonten, eines für private und eines für geschäftliche Zwecke, eingesetzt werden (siehe auch **M-4.07**). Für das Surfen im Internet sind die Massnahmen der **E4: Praxismitarbeitende für Datensicherheit sensibilisieren**.
- M-5.07** Endgeräte sind mit einem Zugriffsschutz, das heisst mit einem Passwort zu versehen. Dabei sind die Vorgaben der **E3: Zugriffsschutz regulieren und Benutzerrechte verwalten**.
- M-5.08** Endgeräte, welche die empfohlenen Massnahmen (**M-5.01** bis **M-5.03**) nicht erfüllen, sollten nicht an Endgeräten, welche von der Praxis zur Verfügung gestellt werden, oder am Netzwerk angeschlossen werden.

[I-5.01] Factsheet Schadsoftware HIN: Was tun gegen Viren, Trojaner und Würmer? https://www.hin.ch/wp-content/uploads/2015/10/Factsheet_Schadsoftware.pdf

[I-5.02] HIN Endpoint Security: <https://www.hin.ch/endpoint/>

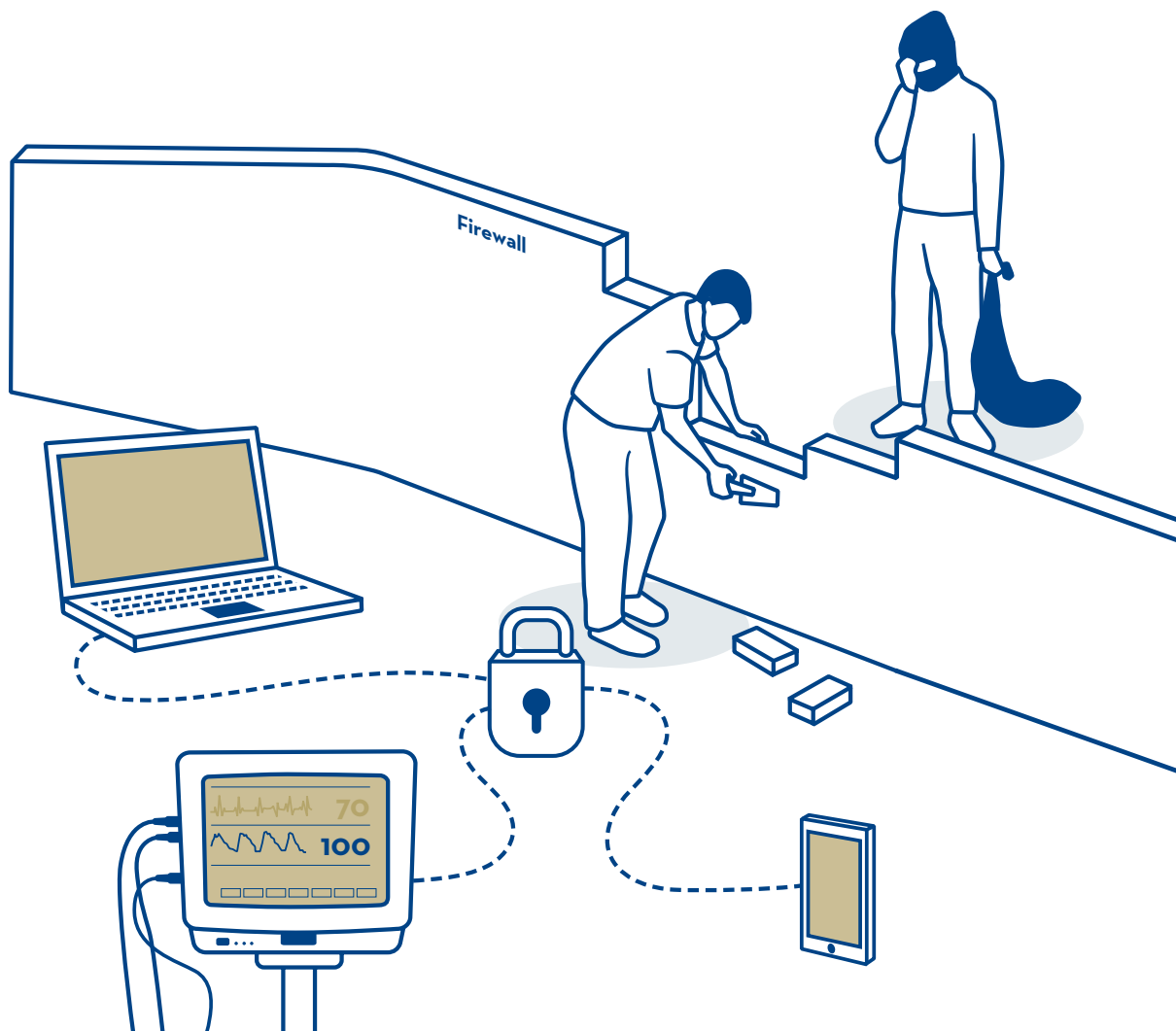
[I-5.03] Microsoft: Aktivieren des kontrollierten Ordnerzugriffs: <https://docs.microsoft.com/de-de/windows/security/threat-protection/windows-defender-exploit-guard/enable-controlled-folders-exploit-guard>

[I-5.04] Microsoft: Häufig gestellte Fragen zum Antispamschutz: <https://docs.microsoft.com/de-de/office365/securitycompliance/anti-spam-protection-faq>

[I-5.05] HIN: Häufige Fragen bei Viren, Schadsoftware und Spam: <https://www.hin.ch/support/schutz-vor-virenschadsoftware-und-spam/>

E6

Netzwerk schützen



Einleitung

Bleibt der Zugriff auf das Computernetzwerk einer Arztpraxis ungeschützt, können sich unberechtigte Dritte (beispielsweise kriminelle Hacker) Zugang zum Netzwerk verschaffen, die Kommunikation abhören oder Daten entwenden. Schnittstellen zu einem Netzwerk sind die physischen Netzwerkanschlüsse, welche per Kabel direkt zu einem Router oder einer Netzwerkdose an der Wand führen, sowie drahtlose Verbindungen (Wi-Fi/WLAN). Gegenüber dem Internet ist das Computernetzwerk der Arztpraxis soweit betrieblich möglich abzuschotten. Dabei sind nur notwendige Verbindungen zu erlauben.

Zweck/Ziel

Um den unberechtigten Zugriff auf das Netzwerk einer Arztpraxis zu schützen, müssen bei der Einrichtung des Netzwerks gewisse Sicherheitsvorkehrungen bei der Schnittstelle zum Internet sowie bei den Anschlüssen im lokalen Netzwerk (kabelgebunden oder kabellos) beachtet werden.

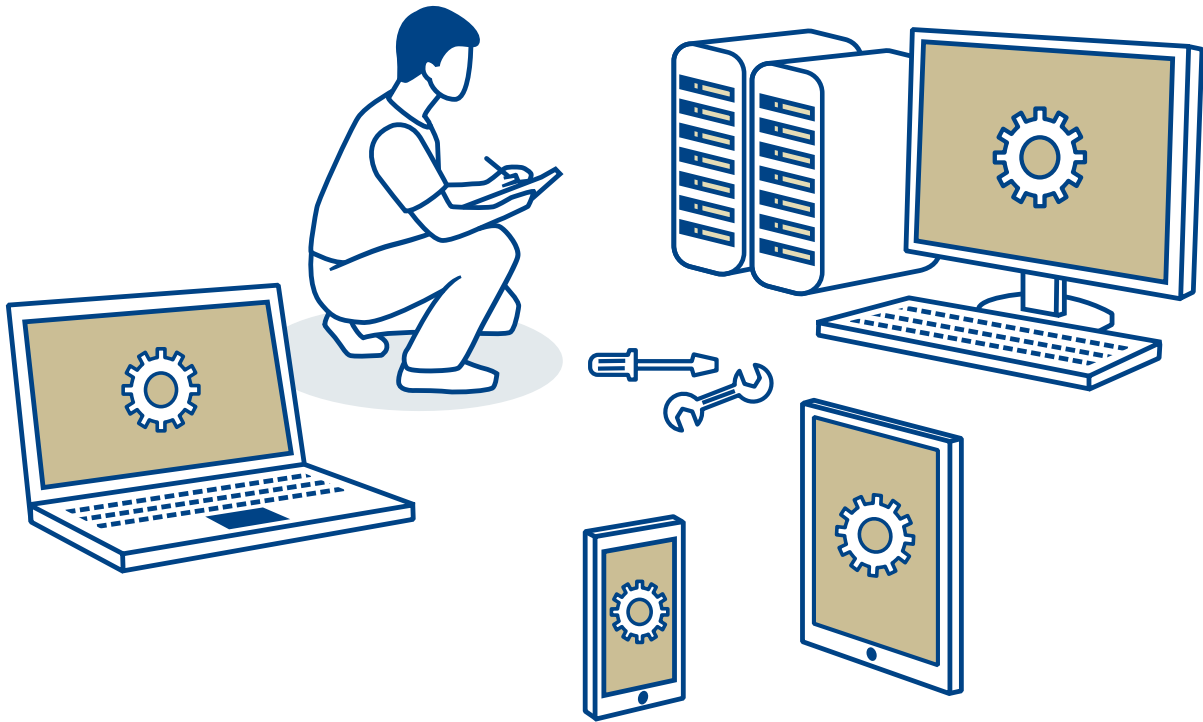
Massnahmen

- M-6.01** Um den unberechtigten Zugriff auf das praxisinterne Netzwerk zu verhindern, müssen Sicherheitsvorkehrungen bei den Schnittstellen zum Internet (Netzwerkübergang Computernetzwerk Arztpraxis zum Internet) getroffen werden, d.h. das praxisinterne Netzwerk muss mit einer Firewall geschützt werden. Dabei sind eingehend nur die betrieblich notwendigen Verbindungen zu erlauben. Für ausgehende Verbindungen wird ebenfalls eine Einschränkung empfohlen. Bei der Produktwahl sollte darauf geachtet werden, dass die Firewall über zusätzliche Sicherheitsfunktionalitäten wie Virens Scanner auf Netzwerkebene, Angriffserkennung (Intrusion Detection/Prevention) sowie Spamfilter für eingehende E-Mails – sofern ein solcher nicht bereits im Mailserver integriert ist – verfügt. Mindestens einmal pro Quartal sollte geprüft werden, ob Aktualisierungen der Software vorliegen. Zudem sollte das Firewall-Regelwerk mindestens jährlich geprüft und sofern notwendig angepasst werden.
- M-6.02** Der Zugriff auf das Praxisnetzwerk über eine kabellose Verbindung sollte nur eingerichtet werden, wenn das absolut notwendig ist. Wird eine WiFi-Verbindung verwendet, so ist der Zugang mit einem Passwort (siehe **E3: Zugriffsschutz regulieren und Benutzerrechte verwalten**) zu schützen und nur berechtigten Benutzenden zur Verfügung zu stellen. Das Kennwort ist einmal jährlich zu wechseln.
- M-6.03** Ungebrauchte Netzwerkdosen sollten versiegelt und nicht an das Netzwerk angeschlossen werden, da sich ansonsten unberechtigte Personen am Netzwerk anschliessen können. Dies gilt insbesondere in öffentlich zugänglichen Bereichen, wie beispielsweise in einem Warteraum.
- M-6.04** Wird eine grössere Informatikinfrastruktur mit mehreren Servern betrieben oder ein Gäste-WLAN angeboten, so sollte das Netzwerk in mehrere Teile aufgeteilt, sogenannte «segmentiert» werden. Damit wird sichergestellt, dass die Benutzenden, welche sich im öffentlichen WLAN befinden, keine Zugriffe auf das interne Netzwerk erhalten.
Der Zugang zum Gäste-WLAN ist mit einem Passwort zu schützen.

[I-6.01] NET.3.1.A1 Sichere Grundkonfiguration eines Routers oder Switches – Bundesamt für Sicherheit in der Informationstechnik (DE): https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_3_1_Router_und_Switches.html

E7

ICT-Umgebung konfigurieren und warten



Einleitung

Durch eine sichere Konfiguration der Systeme und Netzwerkkomponenten können die Angriffsfläche und damit die Wahrscheinlichkeit und die Auswirkungen eines Cyberangriffs verringert werden. Die Umsetzung von sicherheitsrelevanten Konfigurationen wird «härten» genannt. Das Härten eines ICT-Systems ist vor der produktiven Verwendung durchzuführen. Auf ICT-Systeme, beispielsweise Laborgeräte, die vollständig von Drittanbietern geliefert werden, kann infolge vertraglicher und technischer Hürden kein oder kaum Einfluss genommen werden. Solche ICT-Systeme sollten gesondert behandelt und beispielsweise in eine eigene Netzwerkzone verschoben werden, da auf ihnen meistens keine Updates installiert oder keine sicherheitsrelevanten Konfigurationen («härten») vorgenommen werden können.

Zweck/Ziel

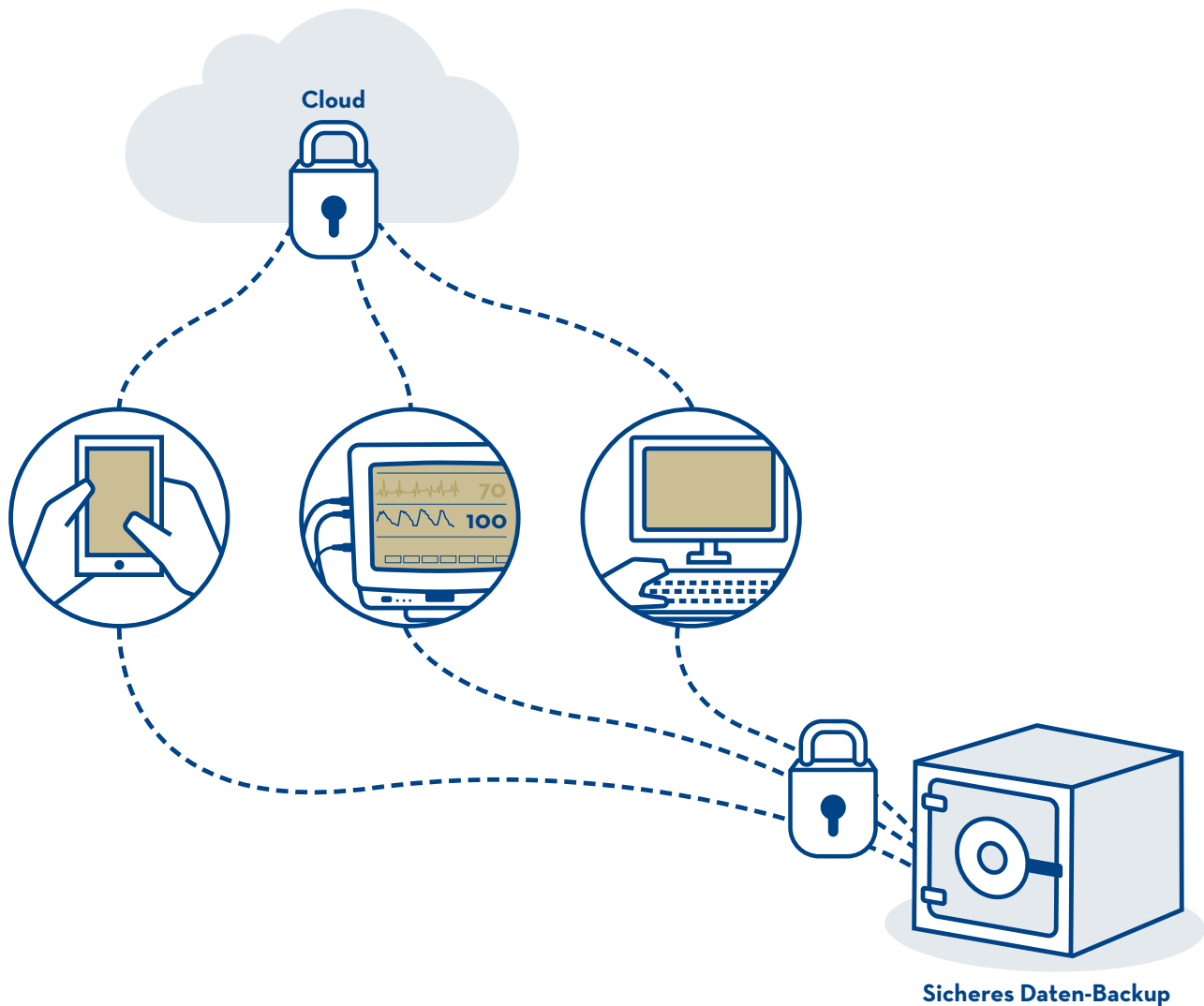
Mit einer sicheren Konfiguration von ICT-Systemen und Netzwerkkomponenten können die Angriffsfläche und somit die Wahrscheinlichkeit und die Auswirkungen eines Cyberangriffes verringert werden.

Massnahmen

- M-7.01** ICT-Systeme, insbesondere Computer, Laptops und Smartphones sowie Netzwerkkomponenten, sind so zu konfigurieren, dass die zeitnahe oder automatische Installation von Aktualisierungen für Betriebssysteme, installierte Anwendungen sowie Sicherheitsupdates unterstützt wird.
- ICT-Systeme und Anwendungen, welche vom Hersteller nicht mehr unterstützt werden, sind für den Einsatz in einer sensitiven Umgebung nicht geeignet und darum zu ersetzen. Ausnahmen sind möglich, sofern durch den Hersteller Sicherheitsupdates für die Anwendung und für die ICT-Systeme zur Verfügung gestellt werden.
- M-7.02** Die ICT-Systeme sind durch die nachfolgenden Massnahmen soweit möglich zu «härten»:
- Nicht benötigte Software, Dienste und Benutzerkonten sind von den Systemen zu entfernen.
 - Die Benutzerkonten sollten persönlich sein und dürfen nur die für die Arbeit notwendigen Berechtigungen haben. Das unpersönliche Administratorenkonto sollte nur für das erstmalige Erstellen von persönlichen Administratorenkontos verwendet werden. Der Gast-Benutzer ist zu deaktivieren.
 - Alle Benutzerkontos, insbesondere solche mit erweiterten Rechten, sind mit sicheren Passwörtern zu versehen (siehe **E3: Zugriffsschutz regulieren und Benutzerrechte verwalten**).
 - Die Festplatten-Verschlüsselung ist zu aktivieren, damit jemand mit direktem Zugriff auf die Festplatte, beispielsweise nach einem Diebstahl, keinen Zugriff auf die Daten selbst erhält.
 - Das BIOS/UEFI, welches für das Starten des Betriebssystems zuständig ist, sollte mit einem Kennwort abgesichert werden. Zudem sollte das BIOS/UEFI so konfiguriert werden, dass das Starten eines Betriebssystems von einem externen Datenträger nicht möglich ist.
 - Der automatische Start für externe Laufwerke, wie zum Beispiel das CD-Laufwerk, ist zu deaktivieren.
- M-7.03** ICT-Systeme mit nur wenigen oder ohne Konfigurationsmöglichkeiten, beispielsweise medizinische Geräte (z.B. Laborgeräte, Sterilisierer usw.), sollten in eine eigene Netzwerkzone verschoben oder ganz vom Netzwerk getrennt werden (siehe **E6: Netzwerk schützen**). Die Netzwerkzone mit den medizinischen Geräten ist so zu konfigurieren, dass nur die für den Betrieb notwendigen ein- und ausgehenden Verbindungen möglich sind.
- M-7.04** ICT-Systeme und Applikationen sind nach Möglichkeit so zu konfigurieren, dass sicherheitsrelevante Aktivitäten wie Login-Versuche, Login, Logout und Mutationen an Daten sowie System- oder Anwendungsabstürze protokolliert werden.
- Die Protokolle sollten zentral gesammelt und aufbewahrt werden und nur mit eingeschränkten Benutzerrechten einsehbar sein.
- Die Protokolldaten sollten mindestens drei Monate aufbewahrt und bei Bedarf (z.B. Verdacht auf Sicherheitsvorfall) für Auswertungen zugänglich gemacht werden.
- M-7.05** Zur betrieblichen Überwachung sollten ICT-Systeme und eingesetzte Applikationen die Aktivität der Benutzenden aufzeichnen und auswerten sowie bei einem Ausfall eines ICT-Systems eine Alarmierung auslösen.
- M-7.06** Für betriebskritische Endgeräte sollten eine Herstellergarantie mit definierten Ersatzfristen vorhanden oder entsprechende Ersatzgeräte vor Ort verfügbar sein.

E8

Digitale Daten sicher ablegen



Einleitung

Auf ICT-Systemen oder Datenträgern gespeicherte Daten können versehentlich von Mitarbeitenden, von fehlerhafter Hardware oder von Schadsoftware gelöscht werden. Zu weit gefasste Zugriffsrechte oder unverschlüsselte Daten können die Vertraulichkeit, Integrität und Verfügbarkeit der Daten gefährden.

Zweck/Ziel

Um dem Risiko eines Datenverlustes entgegenzuwirken, ist es wichtig, eine regelmässige Datensicherung aller Daten vorzunehmen (Backup). Damit die Vertraulichkeit und die Integrität dieser Daten nicht verloren gehen, müssen die Zugriffs- und Benutzerrechte der ursprünglichen Daten ebenfalls gesichert werden.

Massnahmen

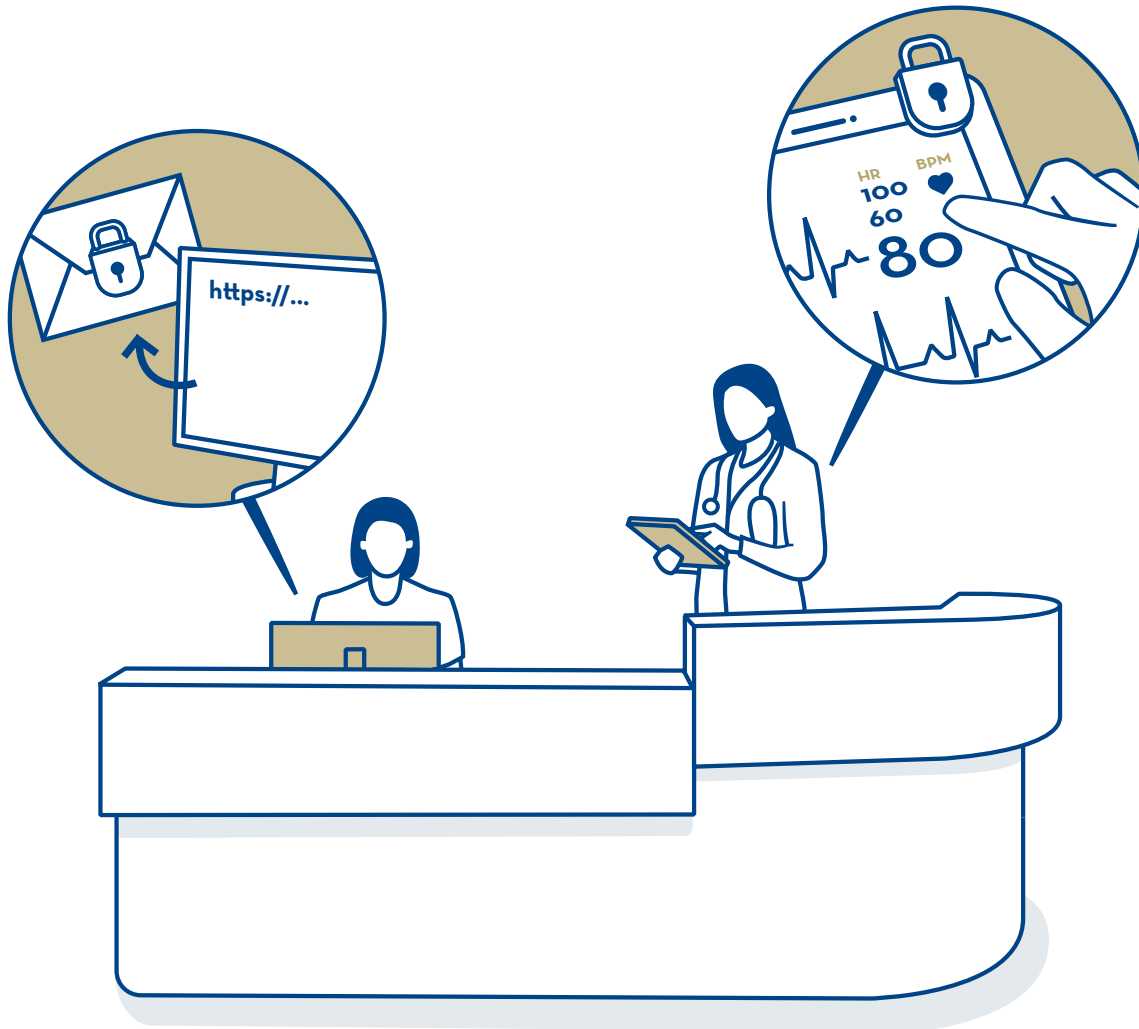
- M-8.01** Es ist zu bestimmen, welche Daten von der Datensicherung erfasst und in welchen Zyklen sie gesichert werden. Mindestens eine Sicherungskopie muss dabei ausserhalb der Praxisräumlichkeiten aufbewahrt werden.
- M-8.02** Das Backup muss ausserhalb der Praxisräumlichkeiten aufbewahrt werden. Die Ablage der Backups ist zu dokumentieren, sodass diese von allen zugehörigen gespeicherten Daten bekannt ist.
- M-8.03** Die eingesetzte Backup-Software soll wie folgt konfiguriert werden:
- Backups sollten verschlüsselt abgelegt werden.
 - Das Verschlüsselungspasswort sollte nur dem Praxisinhaber bekannt sein und in einem Tresor oder Schliessfach hinterlegt werden.
 - Es sind mindestens täglich inkrementelle Backups und mindestens einmal pro Woche ein vollständiges Backup der Daten zu machen. Die Backups sind auf einem separaten Datenträger oder einem ausgelagerten Datenspeicher (z.B. Cloud-Dienst) zu speichern. Beim inkrementellen Backup werden diejenigen Daten gespeichert, die sich seit dem letzten Backup verändert haben, so dass beispielsweise das Backup am Dienstag nur diejenigen Daten enthält, die sich seit dem Backup vom Montag verändert haben.
 - Eine Versionierung der Dateien sollte möglich sein, so dass auf eine gewisse Anzahl früherer Dateiversionen zugegriffen werden kann.
 - Die Zugriffsrechte auf die Dateien in der Datensicherung sollten entsprechend den ursprünglichen Rechten beibehalten werden.
 - Lokale Datenträger sollten täglich gewechselt werden, um den Zugriff durch Schadprogramme, aber auch physische Beschädigungen zu verhindern.
 - Gesicherten Daten sind mindestens einmal wöchentlich an einem externen gesicherten Ort zu platzieren, beispielsweise in einem abgeschlossenen Raum ausserhalb der Praxis.
- M-8.04** Die Wiederherstellung von Daten aus dem Backup ist mindestens einmal jährlich zu testen.
- M-8.05** Die Sicherung von primären Daten und des Backups in der Cloud unterliegt strengen Vorschriften. Ausserdem müssen die gesetzlichen Anforderungen des Datenschutzgesetzes und der beruflichen Geheimhaltungspflicht eingehalten werden.
- Das heisst, medizinische und Patientendaten sind vor der unbefugten Bearbeitung zu schützen.
- Es sind ausschliesslich Cloud-Anbieter zulässig,
- welche die Daten geografisch in der Schweiz, in der EU oder im EWR halten
 - die vertraglich zusichern, dass bei der Bearbeitung von Nutzerdaten ausserhalb der Schweiz in jedem Fall die geltenden Schweizer Gesetze eingehalten werden,
 - die eine Geheimhaltungsvereinbarung unterzeichnen,
 - die eine verschlüsselte Übertragung gewährleisten und
 - die die Daten verschlüsselt ablegen.
- Sofern die Möglichkeit besteht, sollte darauf geachtet werden, dass die Verschlüsselung der Daten in der Cloud diese auch vor der Einsicht durch den Cloud-Anbieter schützt. Die Anforderungen an die Leistungsvereinbarung sind der **E11: Externe Dienstleister beauftragen und überwachen**.
- Bei der Nutzung von Cloud-Lösungen sollte die Patientin oder der Patient über die erhobenen Daten und deren Verwendung sowie die Nutzung von Cloud-Lösungen informiert werden.

[I-8.01] Aufbewahrung von Patientenakten in einer Cloud – Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter: <https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/22--taetigkeitsbericht-2014-2015/aufbewahrung-von-patientenakten-in-einer-cloud.html>

[I-8.02] Rahmenvertrag der FMH für Cloud-Services

E9

Digitale Daten sicher austauschen



Einleitung

Sensible Daten sollten zum Schutz vor Zugriff durch Unbefugte verschlüsselt werden. Dadurch wird sichergestellt, dass die Daten beim Austausch via E-Mail, Fax oder Messaging-Dienste nur von Personen eingesehen, gelöscht oder verändert werden können, die dazu auch befugt sind. Ausserdem wird so verhindert, dass Daten unbemerkt verändert werden.

Zweck/Ziel

Verschlüsselungsverfahren dienen dazu, Informationen, Daten und die Kommunikation vor Einsicht und Manipulation zu schützen. Die Ziele des sicheren Datenaustausches sind der Schutz

der Vertraulichkeit und Echtheit der Nachricht und der Absenderin.

Die Vertraulichkeit einer Nachricht wird durch das Verschlüsseln derselben und den Umstand, dass nur eine Person den passenden Schlüssel zur Entschlüsselung besitzt, geschützt.

Der Einsatz von Verschlüsselungsverfahren macht Veränderungen an der Nachricht sichtbar, so dass die Unveränderbarkeit der ausgetauschten verschlüsselten Nachricht gewährleistet wird.

Durch eine digitale Signatur kann die Echtheit nachgewiesen werden, da nur der Absender den entsprechenden Schlüssel zum Signieren besitzt.

Massnahmen

- M-9.01** Der Zugriff auf Anwendungen über das Internet darf nur über einen verschlüsselten Kanal, beispielsweise mittels HTTPS, erfolgen. Medizinische Daten sowie Authentifikationsmerkmale, wie beispielsweise Passwörter, dürfen nie unverschlüsselt übermittelt werden.
- M-9.02** Werden Patientendaten via E-Mail ausgetauscht, so müssen diese verschlüsselt sein. Dazu ist eine Verschlüsselungslösung zu wählen, welche für die Kommunikation zwischen den Akteuren der Gesundheitsbranche eingesetzt wird. Dazu können beispielsweise die Produkte der HIN eingesetzt werden.
- M-9.03** Anrufer sollten vor der Auskunft über medizinische Daten und Patientendaten identifiziert werden, um einen Social-Engineering-Angriff auszuschliessen.
- M-9.04** Der Austausch via Fax erfolgt unverschlüsselt und sollte auf ein Minimum beschränkt werden. Fax-Geräte sind so zu positionieren, dass eingehende Nachrichten nicht von unberechtigten Personen eingesehen werden können.

[I-9.01] HIN Mail schützt die E-Mail-Kommunikation unter HIN-Teilnehmenden:
<https://www.hin.ch/services/hin-mail/>

EIO

Vorkehrungen für die Behandlung von Sicherheitsvorfällen treffen



Einleitung

Sicherheitsvorfälle sind Ereignisse, welche die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Daten beeinträchtigen. Phishing-Angriffe, die Ausnutzung einer Schwachstelle, der Befall des Endgerätes mit Schadsoftware (Viren, Würmer oder Trojaner) oder der unberechtigte Zugang zu kryptografischen Schlüsseln sind Beispiele für Sicherheitsvorfälle, die eine erhebliche Auswirkung auf den Betrieb einer Arztpraxis haben können.

Die Sicherheitsvorfälle können sich im Bereich der physischen Sicherheit, der vorhandenen ICT-Umgebung, der Benutzer- und Anspruchsgruppen sowie der Applikationen und Endgeräte ereignen.

Je nachdem muss nach einem Sicherheitsvorfall die ICT-Umgebung wiederhergestellt werden, um die operativen Tätigkeiten wieder aufnehmen zu können. Das grundlegende Vorgehen, die Zuständigkeiten in einem solchen Fall sowie die Kontaktdaten der involvierten Personen und Firmen sollten vorgängig erarbeitet und den Praxismitarbeitenden, der Ärzteschaft und den Verantwortlichen zur Verfügung gestellt werden.

Zweck/Ziel

Mittels adäquater Massnahmen in den Bereichen Technologie, Infrastruktur und Personal können Arztpraxen präventiv vor schädlichen Ereignissen geschützt werden. Die vollständige Reduktion der Gefahr eines Sicherheitsvorfalles ist jedoch nicht möglich. Zur zeitnahen und effizienten Erkennung und Behandlung von Sicherheitsvorfällen werden organisatorische und technische Verfahren sowie zugehörige Hilfsmittel eingesetzt. Ziel ist es, das Schadensausmass möglichst gering zu halten.

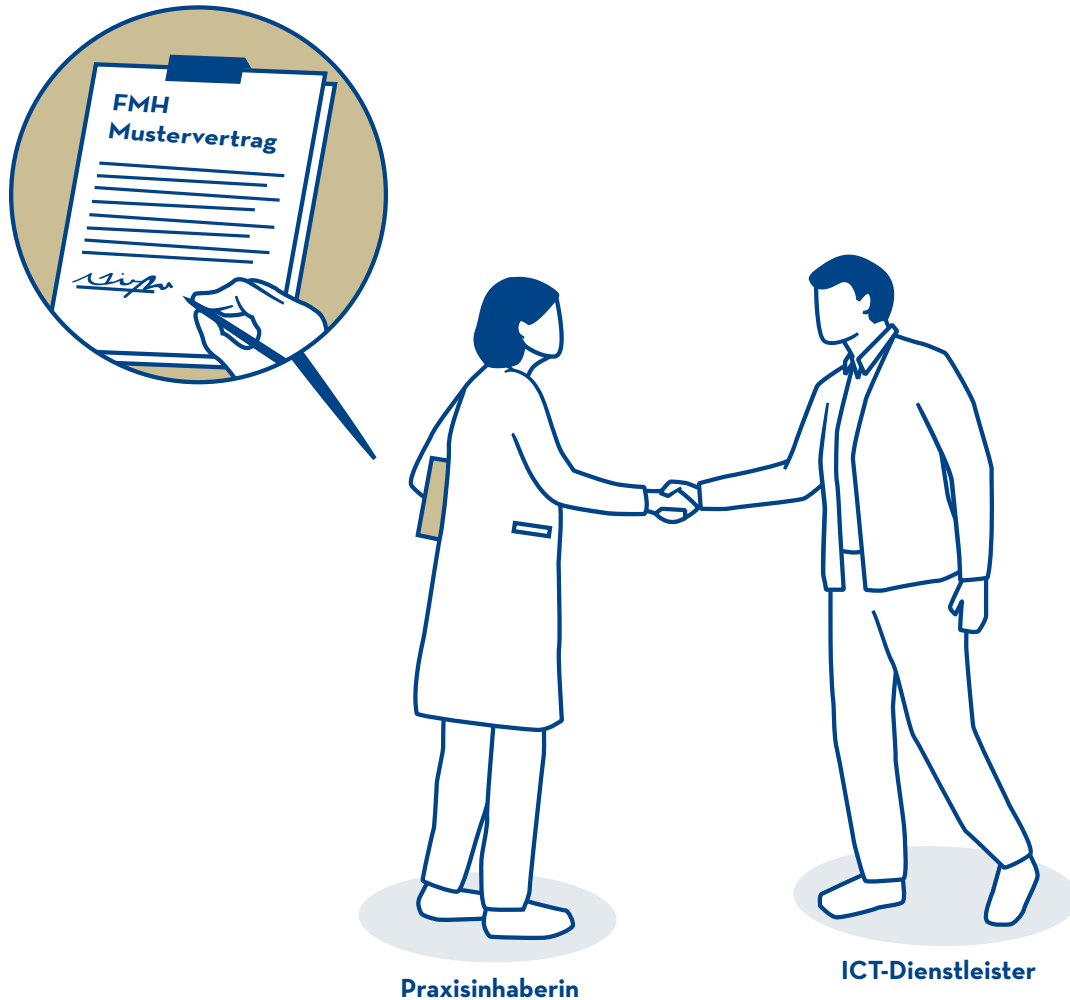
Massnahmen

- M-10.01** Es ist eine Kontaktperson für die Meldung von Sicherheitsvorfällen sowie eine Stellvertretung festzulegen. Die Praxismitarbeitenden, die Ärzteschaft und die Verantwortlichen müssen die Erreichbarkeit der Meldestelle und die entsprechenden Kontaktdaten kennen.
- M-10.02** Merkblätter zur Vorgehensweise sowie zur Analyse eines Sicherheitsvorfalls sollten erarbeitet und die Praxismitarbeitenden sowie die Ärzteschaft davon in Kenntnis gesetzt werden. Das besagte Merkblatt sollte mindestens die nachfolgenden Themen enthalten:
- Definition und Beispiele von Sicherheitsvorfällen
 - Checkliste zur Meldung, Analyse und Bearbeitung von Vorfällen (Handlungsanweisungen)
 - Kontaktangaben der zu informierenden Personen
 - Vorgaben für die interne und externe Kommunikation
- M-10.03** Zur Analyse eines Sicherheitsvorfalls sind mindestens folgende Fragestellungen zu beantworten (Checkliste für die Analyse eines Sicherheitsvorfalls):
- Welche Elemente sind von dem Sicherheitsvorfall betroffen?
 - Wer hat den Vorfall bemerkt und gemeldet?
 - Welcher Nutzerkreis/welche Daten sind von dem Sicherheitsvorfall betroffen (Grösse, Kritikalität usw.)
 - Welche Elemente könnten von dem Sicherheitsvorfall zusätzlich betroffen sein?
 - Wodurch wurde der Sicherheitsvorfall ausgelöst (durch Unachtsamkeit, einen Angreifer, Ausfall der Sicherheitsinfrastruktur usw.)?
 - Sind durch den Sicherheitsvorfall nur interne Personen oder auch Patienten betroffen?
- M-10.04** Wurden infolge des Sicherheitsvorfall medizinische oder Patientendaten entwendet oder gelöscht, sind Sofortmassnahmen, wie zum Beispiel die Isolierung oder Ausserbetriebnahme von einzelnen Diensten oder Endgeräten, umzusetzen. Gemäss dem Entwurf des neuen Schweizerischen Datenschutzgesetzes muss eine Verletzung der Datensicherheit so rasch als möglich dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemeldet werden, es sei denn, der Vorfall führe voraussichtlich zu keinem hohen Risiko für die Persönlichkeits- oder Grundrechte der betroffenen Person.
- M-10.05** Sämtliche Personen, die durch den Vorfall einem hohen Risiko ihrer Persönlichkeits- oder Grundrechte ausgesetzt sind, müssen so rasch als möglich benachrichtigt werden.
- M-10.06** Erkenntnisse aus Sicherheitsvorfällen sind zeitnah an die Mitarbeitenden zu kommunizieren, beispielsweise an den Teammeetings. Müssen nach **M-10.04** und/oder **M-10.05** der EDÖB oder die Betroffenen informiert werden, dann sollten gleichzeitig auch die Mitarbeitenden über den Vorfall informiert werden.
- M-10.07** Erkenntnisse aus Sicherheitsvorfällen sollten in die internen Sicherheitsvorgaben von **M-1.02** einfließen und die Änderungen entsprechend kommuniziert werden. Beispielsweise sollte die Vorgehensweise bei Sicherheitsvorfällen angepasst werden, sofern Optimierungspotenziale einen effizienteren Umgang mit Sicherheitsvorfällen ermöglichen.

[I-10.01] M 6.130 Erkennen und Erfassen von Sicherheitsvorfällen – Bundesamt für Sicherheit in der Informationstechnik (DE): https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/DER/DER_2_1_Behandlung_von_Sicherheitsvorfall%20C3%A4llen.html

E11

Externe Dienstleister beauftragen und überwachen



Einleitung

Externe Dienstleisterinnen und -dienstleister sind je nach Vertragsvereinbarung für den Aufbau, den Betrieb, den Unterhalt und die Wartung der ICT-Umgebung verantwortlich. Die Auswahl des bestpassenden Angebots bedingt eine solide Evaluation des Dienstleistungsangebots, beispielsweise beim Bezug von Cloud-Diensten.

Zweck/Ziel

Die Evaluation der Dienstleister ermöglicht es, eine Anbieterin zu finden, die in Bezug auf Datenschutz und Datensicherheit die entsprechenden Voraussetzungen erfüllt.

Folgende Aspekte sollten überprüft werden:

- Anforderungserfüllung
- Einschränkung aufgrund des Arztgeheimnisses und des Datenschutzes betreffend die Übertragung von Aufgaben und Daten
- Bedeutung des Geschäftsbereichs
- Geografische Datenablage und -verarbeitung
- Anwendbares Recht und Gerichtsstand
- Referenzen
- Unabhängige Beurteilungen durch Dritte

Massnahmen

- M-11.01** Für die Leistungsvereinbarung mit externen ICT-Dienstleistern gilt die aktuellste Ausgabe der allgemeinen Geschäftsbedingungen der Schweizerischen Informatik-Konferenz (SIK) für ICT-Dienstleistungen. Zusätzlich sollte die Leistungsvereinbarung im Bereich Datenschutz und Datensicherheit mindestens folgende Kriterien abdecken:
- Datenbearbeitung und -haltung erfolgen nur nach Vorgaben und zum Zwecke des Auftraggebers und geschehen in dokumentierter Weise
 - Einhaltung von rechtlichen und regulatorischen Anforderungen, insbesondere in Bezug auf das DSG und das Arztgeheimnis
 - Mithilfe bei der Einhaltung von regulatorischen Vorgaben seitens des Auftragnehmers
 - Zusicherung, dass die zur Bearbeitung befugten Personen zur Verschwiegenheit verpflichtet sind
 - Sofortige Meldung von Sicherheitszwischenfällen, die zu einem Risiko für die Betroffenen oder die Arztpraxis führen können
 - Benennung der Unterlieferanten/Subunternehmer und vorherige Bekanntgabe beim Einsetzen von neuen Unterlieferanten/Subunternehmern, mit einem entsprechenden Sonderkündigungsrecht bei begründbarem Zweifel
 - Regeln bei Verletzung der Datensicherheit und des Datenschutzes (Verpflichtung auf Anpassungen und/oder Kündigungsrecht)
 - Weitergabe der eigenen Pflichten an die Subunternehmen
 - Auditrecht oder mindestens Recht auf Auditberichte
 - Kommunikations- und Eskalationswege
 - Kontaktstelle und Vorgehen für Sicherheitsvorfälle
 - Notfallvorsorge
 - Haftung und Konventionalstrafe
 - Vertragsende (vor allem Datenexport/Rückgabe und Löschung von Daten)
 - Migrationsmithilfe
 - Verfügbarkeitswerte (Messwerte)
- M-11.02** Externe ICT-Dienstleister sollten mindestens einmal monatlich oder bei Bedarf jederzeit auf Verlangen folgende Angaben bereitstellen:
- Angaben über den Erfüllungsgrad der definierten Verfügbarkeitswerte (Messwerte)
 - Angaben über Ereignisse wie Ausfälle oder Sicherheitsvorfälle in der Berichtsperiode
 - Angaben über geplante Änderungen (z.B. Wartung)
- M-11.03** Für die Leistungsvereinbarung mit Cloud-Anbietern gilt die aktuellste Ausgabe des Rahmenvertrages der FMH für Cloud-Services.
- Zusätzlich sollte die Leistungsvereinbarung mit dem Cloud-Anbieter mindestens nachfolgende Kriterien festhalten:
- Bereitstellung eines jährlichen Berichts zum Erfüllungsgrad der Verfügbarkeit, zu Sicherheitsvorfällen in der Berichtsperiode und Angaben zu geplanten Aktivitäten
 - Angaben zur technischen und organisatorischen Umsetzung der Datensicherheit sowie Nachweise (z.B. Zertifikat ISO/IEC 27001)
 - Vertragliche Zusicherung, dass die Datenbearbeitung und -haltung in der Schweiz, in der EU oder im EWR erfolgt

- M-11.04** Die Zusammenarbeit mit den Sicherheitsverantwortlichen von externen ICT-Dienstleistern sollte entsprechend koordiniert werden. Das bedeutet,
- dass der externen ICT-Dienstleisterin die vorliegenden Empfehlungen zugänglich gemacht werden,
 - dass der externen ICT-Dienstleisterin die praxisinternen Sicherheitsvorgaben (siehe **M-1.02**) zugänglich gemacht werden,
 - dass vertraglich festgehalten wird, welche Nachweise die externe ICT-Dienstleisterin zur Überwachung der Umsetzung der Sicherheitsvorgaben (**M-1.03**) zu liefern hat und
 - dass die externen ICT-Dienstleister die Sicherheitsvorgaben umzusetzen und einzuhalten haben.

[I-11.01] Für die Leistungsvereinbarung mit externen ICT-Dienstleistern gelten die Allgemeinen Geschäftsbedingungen der Schweizerischen Informatik-Konferenz (SIK) für ICT-Dienstleistungen, Ausgabe Januar 2015.

[I-11.02] Für die Leistungsvereinbarung mit Cloud-Anbietern gilt der Rahmenvertrag der FMH für Cloud-Services.

Anhang

Bearbeitungsverlauf

Die Themenbereiche wurden vorgängig mit den Anspruchsgruppen festgelegt und erweitert. Bei der Festlegung und Erweiterung der Themenbereiche waren folgende Personen und Organisationen involviert:

- Dr. Reinhold Sojer, Foederatio Medicorum Helveticorum (FMH)
- Angela Jakob, Foederatio Medicorum Helveticorum (FMH), Projektassistentin
- Liliane Mollet, insecor GmbH, Datenschutzverantwortliche der FMH
- Lucas Schult, Health Info Net AG (HIN), Leiter IT (CIO), 8304 Wallisellen
- Alexander Hermann, Redguard AG, 3003 Bern

Folgende Ärzteschaft hat sich für die Bereitstellung von Informationen bezüglich ihrer ICT-Umgebung zur Verfügung gestellt und damit zur Plausibilitätsprüfung der empfohlenen Massnahmen beigetragen:

- Dr. med. Steinacher Alex, Ärztezentrum Müllheim, 8555 Müllheim
- Dr. med. Koller Raphael, Herzteam Wil, 9500 Will SG
- Dr. med. Schlagenhauß Bettina, Dermacenter AG, 6403 Küssnacht am Rigi
- Dr. med. Dürrenmatt Urs, Praxis Dr. U. Dürrenmatt, 3600 Thun
- Dr. med. Maurer Susanne, Zentrum für Adipositas- und Stoffwechselmedizin Winterthur GmbH, 8400 Winterthur
- Dr. med. Bürki Pius, Kinderzentrum Lindenviertel AG, 6340 Baar

Verwendete Hilfsmittel und Referenzen

Zur Ausarbeitung der Empfehlungen wurden die in der Tabelle aufgelisteten Dokumente und gesetzlichen Grundlagen verwendet sowie Interviews mit der Zielgruppe geführt, um die inhaltlichen Schwerpunkte festzulegen und die aktuellen Herausforderungen abzuholen.

Nr. Dokumentname → Quelle

[1] SR 235.1 Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 (Stand am 1. März 2019)
→ <https://www.admin.ch/opc/de/classified-compilation/19920153/201903010000/235.1.pdf>

[2] SR235.11 Verordnung Bundesgesetz über den Datenschutz (VDSG) vom 14. Juni 1993 (Stand am 16. Oktober 2012)
→ <https://www.admin.ch/opc/de/classified-compilation/19930159/201210160000/235.11.pdf>

[3] SR 816.111 Anhang 2 der Verordnung des EDI vom 22. März 2017 über das elektronische Patientendossier (Stand am 15. Juli 2019)
→ <https://www.admin.ch/opc/de/classified-compilation/20163257/201907150000/816.111.pdf>

[4] Minimalstandard zur Verbesserung der IKT-Resilienz
→ https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html

-
- [5] Umsetzungshilfe Datenschutz und Datensicherheit im EPD
→ https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/2017/D/170627_Umsetzungshilfe_Datenschutz-Datensicherheit_d.pdf
-
- [6] Mehr Informationssicherheit für Klein- und Mittelbetriebe (KMU)
→ <https://www.iktech.ch/images/10-Punkte.pdf>
-
- [7] Technische und organisatorische Massnahmen des Datenschutzes
→ <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden/technische-und-organisatorische-massnahmen-des-datenschutzes.html>
-
- [8] Erläuterungen des EDOEB zum Datenschutz in der Arztpraxis
→ <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/gesundheit/erlaeuterungen-zum-datenschutz-in-der-arztpraxis.html>
-
- [9] Empfehlungen Eidgenössisches Departement für Daten- und Öffentlichkeitschutz
- Erläuterungen zum Datenschutz in der Arztpraxis
→ <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/gesundheit/erlaeuterungen-zum-datenschutz-in-der-arztpraxis.html>
 - Aufbewahrung von Patientenakten in einer Cloud
→ <https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/aeltere-berichte/22--taetigkeitsbericht-2014-2015/aufbewahrung-von-patientenakten-in-einer-cloud.html>
 - Datensicherheit in der Arztpraxis
→ <https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/aeltere-berichte/13--taetigkeitsbericht-2005-2006/datensicherheit-in-der-arztpraxis.html>
-
- [10] Empfehlungen HIN
- Sichere Passwörter
→ https://www.hin.ch/wp-content/uploads/2018/08/Checkliste_sichere-Passwoerter.pdf
 - Schadsoftware
→ https://www.hin.ch/wp-content/uploads/2015/10/Factsheet_Schadsoftware.pdf
 - Spambekämpfung
→ https://www.hin.ch/wp-content/uploads/2018/01/hin_quickguide_Spam_A4_de.pdf
 - Cyberkriminalität
→ https://www.hin.ch/wp-content/uploads/2018/01/hin_factsheet_cyberkriminalitaet_a4_d_web.pdf
-
- [11] Empfehlung FMH
→ https://www.fmh.ch/files/pdf21/FAQ_DSGVO.pdf
-

Glossar

Backoffice Das Backoffice ist derjenige Teil eines Unternehmens, der nicht originärer Teil des Kerngeschäftes ist, sondern zu dessen Aufrechterhaltung dient.

BIOS/UEFI Basic Input/Output System ist ein Programm, welches vor dem Betriebssystem gestartet und benötigt wird, um das Betriebssystem eines Computers zu starten.

Cookies / Flash Cookie Cookies speichern Benutzerdaten zu Webseiten auf der Festplatte des Endgerätes ab, welche für verschiedene Funktionen der besuchten Internetseite benötigt werden. Dies können Informationen zum Seitenbesuch wie Dauer, Login-Daten, Benutzereingaben oder ähnliches sein.

Cyber Security Cyber Security umfasst den Schutz von Systemen inklusive Hardware, Software und Daten vor Cyber-Attacken.

Datensicherheit Datensicherheit befasst sich mit der Sicherheit sämtlicher Daten. Der Kernpunkt der Datensicherheit sind Massnahmen, um den Schutz der Daten vor Missbrauch, Verfälschung, Verlust und unberechtigten Zugriffen auf technischer, organisatorischer und personeller Ebene zu gewährleisten.

Endgerät Endgeräte inkludieren sämtliche Geräte, die Daten verarbeiten und/oder Daten temporär oder permanent speichern. Dazu zählen Computer, Laptops, Server, Smartphones, Tablets, Drucker und Fax.

Hardware Hardware ist der Oberbegriff für physische Komponenten von datenverarbeitenden Systemen, beispielsweise Endgeräte.

HTTPS (Hyper Text Transfer Protocol Secure) HTTPS ist eine Variante des http-Protokolls, das eine Sicherungsschicht für die Daten während der Übertragung durch TLS bietet. HTTPS ermöglicht so zum Beispiel eine verschlüsselte Kommunikation und damit eine sichere Verbindung zwischen einem entfernten Benutzer und einem Webserver.

ICT-Mittel ICT-Mittel umfasst sämtliche hardware- und softwarebasierte Technik im Bereich der Kommunikation und Information. Dies inkludiert ICT-Systeme, wie zum Beispiel Endgeräte mit und ohne VPN-Zugang, Netzwerke oder medizinische Geräte (z.B. Laborgeräte, Sterilisierer usw.), Hardware wie zum Beispiel Endgerätkomponenten, Server- oder Netzwerkkomponenten, Datenträger und eingesetzte Software.

ICT-System Systeme sind allgemein definiert als eine Gesamtheit von Elementen, die zusammengesetzt ein Ganzes ergeben. In der Informations- und Kommunikationstechnologie umfasst der Begriff System jegliche Art elektronischer datenverarbeitender Systeme. Darunter fallen Computer, Mobiltelefone, Serversysteme, Cloud Computing, Netzwerke, Datenbanksysteme, Informationssysteme, Videokonferenzsysteme oder Kommunikationssysteme. Medizinische Geräte (z.B. Laborgeräte, Sterilisierer usw.), die einen Netzwerkanschluss haben, zählen auch zu den ICT-Systemen.

ICT-Umgebung ICT steht für Information Communication Technology. Die ICT-Umgebung beschreibt die Gesamtheit aller ICT-Mittel im Zusammenspiel.

IP-Adresse (Internetprotokolladresse) Die IP-Adresse wird für das Senden und Empfangen in der Internetkommunikation benötigt.

Medizinische Daten Medizinische Daten inkludieren sämtliche Gesundheitsdaten von Patienten.

Netzwerk Netzwerke verbinden verschiedene Endgeräte miteinander, um einen Datenaustausch zwischen ihnen zu ermöglichen, zum Beispiel ein internes Netzwerk oder das Internet.

Netzwerkinfrastruktur Die Netzwerkinfrastruktur beschreibt die Gesamtheit aller eingesetzten Softwareanwendungen und Hardwarekomponenten, um die Geräte miteinander zu verbinden.

Patientendaten Patientendaten inkludieren sämtliche Informationen zu Patienten wie Personalien oder Krankenkassennummer.

Peripheriegeräte Peripheriegeräte umfasst alle Geräte, die sich ausserhalb der Zentraleinheit befinden, wie zum Beispiel Tastatur, Computermaus, Monitor, interne oder externe Festplatten, Webcam, Touchpad, Lautsprecher oder Mikrofon.

Sicherheitsvorfall Ein Sicherheitsvorfall beschreibt ein Ereignis, welches die Datensicherheit, das heisst die Vertraulichkeit, die Verfügbarkeit oder die Integrität der zu schützenden Daten tangiert.

Social Engineering Social Engineering sind Angriffe mit dem Ziel, durch die Beeinflussung auf zwischenmenschlicher Ebene bestimmte Verhaltensweisen hervorzurufen, wie zum Beispiel die Bekanntgabe von vertraulichen Informationen. Dazu zählen unter anderem Phishing- und Spoofing-Angriffe per Mail oder Telefon.

SSL/ TLS (Secure Sockets Layer/Transport Layer Security)

SSL/TLS ein Protokoll zur Verschlüsselung von Datenübertragungen im Internet. Es wird unter anderem für die Protokollerweiterung HTTPS verwendet, um die Verbindung zwischen einem Client und einem Server zu verschlüsseln, um die Integrität und die Vertraulichkeit der Daten während der Datenübertragung gewährleisten.

VPN (Virtual Private Network) Das Virtual Private Network bezeichnet ein virtuelles privates Kommunikationsnetz, das ohne physische Verbindung, sondern durch einen logischen und verschlüsselten Kommunikationskanal zwischen den Kommunikationspartnern aufgebaut wird. Es können nur die Kommunikationspartner, die zu diesem privaten Netzwerk gehören, kommunizieren sowie Informationen und Daten austauschen. Organisationen nutzen das VPN zur Herstellung einer Kommunikationsverbindung vom Wohnort eines Mitarbeitenden zum organisationsinternen Netzwerk, um den Zugriff auf organisationsinterne Ressourcen, Daten und Informationen zu ermöglichen.

WiFi (Wireless Fidelity) WiFi ist eine Kennzeichnung und ein Markenname für Geräte, die fähig sind, eine kabellose Verbindung herzustellen.

WLAN (Wireless Local Area Network) Wireless Local Area Network ist der Name für eine kabellose Verbindung zum Internet. Endgeräte können per WLAN, das heißt ohne Kabel, mit dem Internet verbunden werden.

Impressum

Herausgeberin: FMH - Verbindung der Schweizer Ärztinnen und Ärzte, Bern

Text: Redguard AG, Bern

Grafikdesign/Illustration: Hahn+Zimmermann, Bern

Publikation: Dezember 2019

www.fmh.ch

