Pharmazeutische Gehaltskasse für Österreich

Das Sozial- und Wirtschaftsinstitut der österreichischen Apotheker

IT-Sicherheit in der Apotheke

Rechnen Sie mit uns!

2024

INHALTSVERZEICHNIS

Sehr geehrte Frau Kollegin,
sehr geehrter Herr Kollege,

wir leben in einer Zeit mit rasanten Veränderungen und völlig neuen Anforderungen. Die Corona-Pandemie hat uns die Bedeutung und die Vorteile bzw. auch Nachteile der Digitalisierung aufgezeigt. IT-Unterstützung ist praktisch in allen Lebensbereichen selbstverständlich geworden und in der Apotheke ist das Arbeiten ohne technische Unterstützung nicht mehr vorstellbar. Durch die steigende Internetkriminalität betrifft Daten- und Informationssicherheit besonders auch Sie in der Apotheke. Nutzen Sie die Möglichkeit der neuen Technologien, bleiben Sie aber gleichzeitig kritisch und schützen Sie Ihre Daten und Informationen.

Für uns stehen Sie als Mitglied der Pharmazeutischen Gehaltskasse im Zentrum unserer Entscheidungen und Sie können mit uns rechnen! Einerseits in Hinblick auf die Sicherheit Ihrer Daten, die bei uns verarbeitet werden und andererseits durch diese Informationsbroschüre, die Ihnen relevante IT-Themen für den Apothekenalltag übersichtlich und leicht lesbar darstellt.
Unser Ziel ist es, erfahrene und weniger erfahrene Computerbenutzer in der Apotheke zu erreichen. Für detailliertes Fachwissen können wir Ihnen die Literatur aus der Quellenangabe empfehlen. Diese Informationsbroschüre kann Ihnen auch als Nachschlagewerk dienen, aber erhebt nicht den Anspruch auf Vollständigkeit.
Die aktuelle Version können Sie jederzeit auf unserer Homepage www.gehaltskasse.at/broschüren downloaden.

Erste Obfrau
Mag.pharm. Irina Schwabegger-Wagner e. h.

Zweiter Obmann
Mag.pharm. Georg Fischill e. h.

Das Thema Sicherheit beschäftigt uns in vielen Bereichen, sei es nun im beruflichen oder im privaten Bereich. Sicherheit ist immer ein subjektives Empfinden und wird von jeder Person unterschiedlich wahrgenommen und gelebt.

Informationstechnologie (IT) ist als Oberbegriff für die I**nformations- und Datenverarbeitung**, sowie die dafür benötigte Software und Hardware, zu verstehen.
Die **IT-Sicherheit** bezieht sich auf **elektronisch gespeicherte Informationen und IT-Systeme**, mit dem Ziel, die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen und Informationstechnik zu gewährleisten. Alle technischen und auch nicht technischen **Maßnahmen zur Verringerung der Risiken, Schwachstellen bzw. Bedrohungen** der Informationstechnologie fallen unter dem Begriff IT-Sicherheit.
Wenn wir von **EDV-Sicherheit** sprechen, geht es prinzipiell um den **Schutz von Daten**. Der Begriff EDV (Elektronische Datenverarbeitung) steht für die Erfassung und Bearbeitung von Daten durch elektronische Geräte.

Der Umfang an persönlichen und sensiblen Daten steigt laufend und deren Schutz muss oberste Priorität haben. Jede/Jeder Einzelne von uns kann seinen Beitrag dazu leisten. Trotz höchster Sicherheitsmaßnahmen lauern die Gefahren sowohl auf virtueller, elektronischer, physischer und personeller Ebene. Zum Beispiel müssen auch die elektronischen Geräte, mit denen Sie arbeiten, sowie die Räumlichkeiten, in denen sie sich befinden, geschützt werden. Oft sind es nur simple Maßnahmen, die eine große Wirkung zeigen. Vergessen Sie nicht darauf Ihr Team in der Apotheke auf sicherheitsrelevante Themen zu sensibilisieren.
Seien Sie sich der Gefahren, die unsere elektronische Welt birgt, bewusst. Die Schwierigkeit besteht sicher darin, das richtige Ausmaß an technischen Sicherheitseinrichtungen zu ermitteln.

⚠ Wir alle bemühen uns um höchste Sicherheitsvorkehrungen, aber in der Informationssicherheit gibt es keine 100%ige Sicherheit!

Sie leben Sicherheit schon in vielen Bereichen, z.B. haben Sie in Ihrem Auto Airbags, ABS und Sicherheitsgurte oder Sicherheitstüren und Alarmanlagen in Ihren Häusern und Wohnungen.

Betreiben Sie in der Apotheke keine „Vogel-Strauß-Politik“ nach dem Motto: „Mir ist noch nie etwas passiert“.

1. Datenschutz in der Apotheke

In der Apotheke begegnen Ihnen viele verschiedene Arten von Daten, angefangen von den Kundendaten auf Rezepten und Karteien, den Rezeptabrechnungsdaten, den Geschäfts- und Wirtschaftsdaten, bis hin zu Ihren persönlichen Zugangsdaten. Es ist selbstverständlich, dass Datenschutz einen hohen Stellenwert in Ihren Tätigkeiten einnimmt und Sie sensibel mit diesem Thema umgehen.

Grundsätzlich beschäftigen Sie sich als Apotheker*in schon sehr lange mit dem Thema **Datenschutz**. Mitunter durch den § 19 der Apothekenbetriebsordnung[1] , in dem das Thema „Verschwiegenheit" behandelt wird.

Durch das Inkrafttreten der EU-Datenschutzgrundverordnung im Mai 2018 erhielt das Thema Datenschutz und die Wahrung der Persönlichkeitsrechte eine neue Bedeutung und Akzeptanz. Der Umgang mit personenbezogenen Daten ist im privaten wie auch im geschäftlichen Umfeld bewusster geworden. Für Unternehmen mitunter auch durch die Befürchtung finanzieller bzw. strafrechtliche Konsequenzen. Sollten personenbezogene Daten in falsche Hände geraten, so kann man das nicht mehr rückgängig machen! Durch die Medienpräsenz dieses Themas sind die Bürger*innen informiert und auf das Thema Datenschutz sensibilisiert.

Datenschutz hat heute zunehmend mit **Datensicherheit** zu tun. Datensicherheit beinhaltet alle digitalen **Datenschutzmaßnahmen,** die angewendet werden, um den unzulässigen Zugriff auf Computer, Datenbanken und Websites zu verhindern. Auch einer Beschädigung von Daten wird mit einem sorgsamen Umgang der neuen Technologien vorgebeugt.

Die gängigsten **Datensicherheitstechnologien** sind Backups, Datenmaskierung und Datenlöschung. Auch die **Verschlüsselung** ist eine wesentliche Maßnahme der Datensicherheitstechnologie, um digitale Daten, Software, Hardware und Festplatten für Hacker unlesbar zu machen. **Authentifizierungen** dienen ebenso der Datensicherheit. Überall wo Daten gesammelt werden, besteht auch die Gefahr des Datenmissbrauchs. Ein gesundes Misstrauen, bei der Überlassung von personenbezogenen Daten ist durchaus gerechtfertigt.

[1] ABO §19: „Alle in der Apotheke tätigen Personen sind - sofern nicht Durchbrechungen der Verschwiegenheit gesetzlich vorgesehen sind - verpflichtet, alle ihnen ausschließlich aus ihrer Tätigkeit bekannt gewordenen betriebs- und kundenbezogenen Daten sowohl während ihrer Apothekentätigkeit als auch nach deren Ende geheim zu halten. Die Entscheidung über die Übermittlung derartiger Daten liegt beim Apothekenleiter/bei der Apothekenleiterin".

Datenschutzgrundsätze

Die EU - Datenschutzgrundverordnung[2] ist seit 25. Mai 2018 in allen Mitgliedstaaten wirksam und vereinheitlicht die Regeln für die Verarbeitung personenbezogener Daten, die Rechte der Betroffenen und die Pflichten der Verantwortlichen. Die Verordnung enthält zahlreiche Öffnungsklauseln und lässt dem nationalen Gesetzgeber gewisse Spielräume. In Österreich wurde das Datenschutz-Anpassungsgesetz 2018, eine Novelle des DSG 2000 (jetzt nur DSG) beschlossen. Das Gesetz wurde im BGBl Nr. 120/2017 kundgemacht und trat am 25.05.2018 in Kraft[3]. Ab diesem Zeitpunkt gelten sowohl die Regelungen aus der Datenschutz-Grundverordnung (DSGVO), als auch aus dem österreichischen Datenschutzgesetz idF des Datenschutz-Anpassungsgesetzes 2018 (Datenschutzgesetz - DSG) und der Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV) [4].

Jedes Unternehmen ist verpflichtet **Verarbeitungsverzeichnisse** der Datenverarbeitungen zu führen und diese Verarbeitungstätigkeiten innerhalb eines Risikomanagements in Bezug auf IT-Sicherheit und Datenschutz-Folgenabschätzungen zu bewerten. Innerhalb der Verarbeitungsverzeichnisse wird der Zweck und die Rechtsgrundlage bzw. die Empfänger und Datenkategorie der Datenverarbeitungen dokumentiert, sowie der Speicherort der personenbezogenen Daten.

Das Verfahrensverzeichnis in der Apotheke sollte z. B. die Rezeptverrechnung, Kundenkarteien, Korrespondenz, Videoüberwachung oder Wareneinkauf umfassen. Videoüberwachung in der Apotheke ist grundsätzlich zulässig, aber nie zum Zweck der Kontrolle von Mitarbeiter*innen (außer diese haben zugestimmt). Jeder Verarbeitungsvorgang muss protokolliert (außer Echtzeitüberwachung) werden und eine Speicherung ist grundsätzlich für maximal 72 Stunden vorgesehen.[5]

Die **Pflichten der Verantwortlichen** wurden stark ausgeweitet. Jede Apotheke hat dafür Sorge zu tragen, dass die Zweckbindung der Datenverarbeitung, die Datensparsamkeit, die Begrenzung von Zugriffsrechten, die Transparenz von Zugriffen und die Richtigkeit und Vollständigkeit von Daten gewährleistet ist. Innerhalb der Datenschutzgrundverordnung spricht man von geeigneten technischen und organisatorischen Maßnahmen. Diese Maßnahmen müssen auch evaluiert und gegebenenfalls angepasst werden. Achten Sie darauf, Einwilligungserklärungen für Stammkund*innen einzuholen und, sollten Dienstleister in Ihrem Auftrag Daten verarbeiten, ist ein Auftragsdatenverarbeitungsvertrag mit diesen abzuschließen.

Datenschutz-Folgenabschätzungen sind für besonders risikoreiche Datenverarbeitungen vorzunehmen. Die Datenschutzbehörde führt „Black und White-Lists“ zur Orientierung. Unternehmen, welche besonders sensible Daten verarbeiten, bekommen die Auflage einen Datenschutzbeauftragten zu bestellen. Ob in Apotheken die Notwendigkeit für die Bestellung eines Datenschutzbeauftragten besteht beantwortet Ihnen die Österreichische Apothekerkammer.

Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht und hat einen großen Stellenwert. Die **Betroffenenrechte und Informationspflichten** wurden innerhalb der neuen Datenschutzgesetze ausgeweitet und

[2] https://www.dsb.gv.at/rechtentscheidungen/gesetze-in-oesterreich.html (31.01.2024)

[3] https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdf (31.01.2024)

[4] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010206 (31.01.2024)

[5] Quelle zur Videoüberwachung im Login Bereich auf der Homepage der Apothekerkammer https://www.apothekerkammer.at/geschuetzt/rechtliche-informationen/rechtsbereiche/datenschutzrecht/videoueberwachung-in-der-apotheke#c3455 (31.01.2024)

gestärkt. Jede Person hat ein Auskunftsrecht bzw. ein Recht auf Berichtigung über die gespeicherten Daten. Zusätzlich besteht mit der neuen Datenschutzgrundverordnung das Recht auf Löschung, das Recht auf eingeschränkte Verarbeitung, das Recht auf Datenübertragbarkeit bzw. ein Widerspruchsrecht. Im Falle eines Datenschutzvorfalles sind die betroffenen Personen innerhalb von 72 Stunden zu verständigen. Vor der Meldung an die Datenschutzbehörde sollte das Datenleck nach Möglichkeit beseitigt werden, um weitere Schäden zu verhindern. Prüfen Sie, ob ein „hohes Risiko" für die Betroffenengruppe vorliegt, da in diesem Fall auch die betroffenen Personen zu informieren sind.

Zu bedenken ist auch, dass im Falle von Verstößen zusätzlich zu einer Verwaltungsstrafe auch Schadensersatzforderungen jener Person drohen, deren Daten verletzt wurden. Diese Verwaltungsstrafen können sehr hoch ausfallen! Vergessen Sie nicht, Ihre Mitarbeiter*innen in der Apotheke regelmäßig zu schulen und auf das Thema Datenschutz zu sensibilisieren.

Die Österreichische Apothekerkammer unterstützt Sie bei der Umsetzung der Datenschutzgesetze in Ihrer Apotheke!
Alle notwendigen Unterlagen finden Sie im geschützten Login Bereich unter https://www.apothekerkammer.at/geschuetzt/rechtliche-informationen/rechtsbereiche/datenschutzrecht

Authentifizierung und Passwortmanagement

Es gibt zwar nicht nur die eine Maßnahme, um Cyberkriminelle aufzuhalten und die Daten in der Apotheke zu schützen, aber eine der wichtigsten Maßnahmen für die Datensicherheit und den Schutz vor Manipulation ist definitiv eine gute Authentifizierung. Die Authentifizierung bestimmt und prüft die Gültigkeit Ihrer Identität. Es gibt verschiedene Möglichkeiten der Authentifizierung:

- **Passwort** – ist etwas, das möglichst nur Sie selbst wissen sollten! Passwörter beweisen wer Sie sind, weil Sie etwas wissen. Die Gefahr bei Passwörtern besteht darin, dass sie einen zentralen Ausfallpunkt darstellen.
- **Smartcard** – ist eine Plastikkarte mit eingebautem Chip, wie etwa die e-Card oder Bankomatkarte und somit etwas, das Sie haben und auf das Sie gut aufpassen sollten! In Kombination mit dem PIN-Code (z.B. Bankomatkarte) ist es eine Form der Zwei-Faktor-Authentifizierung.
- **Biometrie** – bedient sich eines bestimmten Merkmals von Ihnen, wie etwa dem Fingerabdruck oder Iris Scan.

Die häufigste Authentifizierung bzw. Anmeldung ist jene mittels Benutzername und Passwort, aber auch die am wenigsten sichere Methode. Je stärker das Passwort allerdings ist, desto sicherer/stärker wird diese Methode. Sicherer sind biometrische Merkmale und die Verwendung von Smartcards oder die Authentifizierung mittels digitaler Signatur.

Wenn Sie mehr als eine Authentifizierungsmethode verwenden, fügen Sie eine zusätzliche Ebene des Schutzes vor Cyberkriminellen hinzu. Die zusätzliche Nutzung eines zweiten Faktors zur Authentifizierung ist somit weitaus die sicherste Lösung.
Bei der Zwei-Faktor-Authentifizierung (manchmal auch 2FA, Zwei-Schritt-Verifizierung oder Multi-Faktor-Authentifizierung genannt) werden nicht nur eine, sondern zwei verschiedene Methoden zur Authentifizierung benötigt. Auf diese Weise ist Ihr Konto auch dann geschützt, wenn Ihr Passwort kompromittiert wird.

Tipps für gute Passwörter

Passwörter sind im digitalen Leben ein notwendiges Übel und für den sicheren Umgang braucht es Strategien. Vermehrt wird Ihnen der Begriff Passwort begegnen. Kennwort, Zugangscode, Keyword oder etwa PIN sind durchaus auch üblich und im Sinne des hier beschriebenen Begriffes Passwort zu verstehen. Folgende Ratschläge haben wir für Sie zusammengestellt:

- Vermeiden Sie Name, Geburtsdatum, Tastaturmuster und verwenden Sie auch keine Wörter, die in einem Wörterbuch zu finden sind.
- Verwenden Sie stattdessen Passwortphrasen – am besten in Kombination mit Zahlen und Sonderzeichen! Empfehlenswert sind Sätze oder zufällige Wörter, die man sich leicht merken kann. Z.B.: „!Die!Titanik!ist!1912!gesunken!“
- Je länger das Passwort ist, desto sicherer! Besonders wichtige Benutzerkonten sollten Sie mit mindestens 20 Zeichen langen Passwörtern schützen und auch regelmäßig ändern. Für weniger wichtige Zugänge, wie etwa Online-Zeitungen, können Sie auch weniger starke Kennwörter benutzen. Wenn Sie wissen wollen, wie sicher das gewählte Passwort ist, dann können Sie es testen[6] .
- Verwenden Sie für jedes Benutzerkonto ein anderes Passwort! Sollte ein Passwort doch einmal geknackt werden, bleiben andere Zugänge dennoch geschützt.

[6] https://de.pc112.eu/passwort-test-check-it-sicherheit-staerke (31.01.2024)
http://www.wiesicheristmein-passwort.de/ (31.01.2024)

Tipps zur Passwortverwaltung

Am besten wäre es natürlich, sich alle **Passwörter** zu **merken**. Aber bei der Fülle von Kennwörtern tun wir uns oft schwer den Überblick zu behalten bzw. grenzt es an Unmöglichkeit sich alle zu merken.

Wenn Sie sich Passwörter aufschreiben, bewahren Sie sie auf jeden Fall an einem sicheren Ort, wie etwa in einem mechanischen oder auch elektronischen Datensafe, auf. Eine Textdatei, die Passwörter enthält, sollte auf keinen Fall als ungeschütztes Dokument am PC abgelegt werden. Eine ausgedruckte Passwortliste, die in der Geldbörse mitgenommen wird, ist ebenso nicht empfehlenswert!

Eine gute Möglichkeit ist es sich eines **Passwort-Managers**[7] zu bedienen. Das sind Programme, die Benutzernamen und Passwörter verwalten. Mittels Verschlüsselung und eines komplexen Masterpasswortes verwahren Passwort-Manager die Passwörter sicher. Der Vorteil ist, dass, anstatt von vielen verschiedenen Passwörtern nur mehr eines zu merken ist (Masterpasswort). Je nach Wahl des Programmes werden die Passwörter entweder lokal auf dem Gerät oder zwecks Synchronisierung auf verschiedenen Systemen (oft cloudbasiert) gespeichert. Es gibt eine Fülle verschiedener Anbieter.[8]

[7] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Passwort-Manager/passwort-manager_node.html (31.01.2024)

[8] https://www.chip.de/artikel/Test-Die-besten-Passwort-Manager_182620837.html (31.01.2024)

Sichere digitale Identität

Sichere digitale Identitäten sind zum Beispiel die ID Austria, eAusweise oder persönliche Datensafes. Im e-Banking Bereich, bei e-Formularen der Pharmazeutischen Gehaltskasse oder bei e-Business Anwendungen werden sichere digitale Identitäten eingesetzt. Um digitale Amtswege sicher und nachvollziehbar durchführen zu können, müssen Behörden die Identität von Personen zweifelsfrei feststellen können. Dazu bedarf es eines elektronischen Werkzeugs, die Personen eindeutig ausweist: **die ID Austria**.

Mittlerweile können viele Amtswege online erledigt werden (https://www.oesterreich.gv.at). BriefButler, zum Beispiel, ist eine Plattform, auf der man PDF-Dokumente signieren bzw. Dokumente eingeschrieben versenden kann. Sie können hier Kuverts oder Briefmarken sparen. Plattformen, um diverse Online-Kündigungen einfach durchzuführen sind auch sehr praktisch und zeitsparend (www.online-kuendigen.at).

Ein e-Tresor bietet die Möglichkeit, Dokumente und Verträge elektronisch abzulegen, um diese dann weltweit wieder abrufen zu können. Sie bieten höchsten Schutz vor Diebstahl, bzw. können die darin abgespeicherten Dateien extra mit einem Passwort gesichert werden. Neben dem sicheren Online-Speicherplatz bieten sie eine Plattform, um Dokumente elektronisch zu signieren bzw. signierte Dokumente zu prüfen und zu versenden.

Bedenken Sie, dass ein **Identitätsdiebstah**l großen Schaden anrichten kann, sei es nun finanziell oder durch einen persönlichen Imageschaden. Ein Diebstahl der Identität bedeutet, dass mit dem eigenen Namen und persönlichen Daten eine dritte Person ihr Unwesen treibt (z. B. Warenbestellungen oder Namensmissbrauch auf Blogs, Kredite können aufgenommen werden, usw.). Wer im Internet sicher unterwegs sein möchte, braucht einen digitalen Personalausweis!

Die digitale Signatur

Eine digitale Signatur stellt sicher, dass ein Dokument oder eine Nachricht von der Person kommt, die ihre Unterschrift gegeben hat. Zur Umsetzung wird ein asymmetrisches Verschlüsselungsverfahren verwendet, wobei der Sender seine Nachricht mit dem öffentlichen Schlüssel[9] des Empfängers signiert und verschlüsselt, und der Empfänger die Unterschrift mittels seines privaten Schlüssels[10] bestätigt und die Datei entschlüsselt. Es handelt sich hier um einen **Identitätsnachweis auf höchster Sicherheitsstufe.**

Zum Beispiel fangen Trojaner[11] eingegebene Transaktionsnummern (TAN) ab und missbrauchen sie für eigene Zwecke. Der Einsatz einer digitalen Signatur kann vor derartigen Angriffen wirkungsvoll schützen.

Mit der ID Austria können Sie sich modern, sicher und digital identifizieren.

[9] Ein öffentlicher Schlüssel ist jedem Gerät im Netzwerk und im Internet bekannt.

[10] Ein privater Schlüssel ist nur einer Person (dem Empfänger) bekannt.

[11] Trojaner Programme sind in der Lage Hintertüren, durch die der Angreifer den PC, Smartphone, etc. fernsteuern kann, zu öffnen. Haben sie erst einmal die Kontrolle, können sie Daten löschen oder ändern, Nachrichten versenden, Informationen und Passwörter ausspionieren und noch vieles mehr.

ID Austria

Immer mehr Menschen benutzen die **ID Austria**. Damit können Sie sich sicher online ausweisen und diverse digitale Services nutzen. Sei es als **Ausweis** bei Behörden oder als **rechtsgültige elektronische Unterschrift**. Diese Form der Online-Unterschrift ist gesetzlich der eigenhändigen Unterschrift auf Papier gleichgestellt. Sie können daher Verträge abschließen und rechtsgültig elektronisch unterschreiben. Informationen rund um die ID Austria finden Sie auf www.oesterreich.gv.at.

Eine kostenlose Aktivierung der ID Austria ist bei Behörden möglich und gewährleistet die Vollfunktion. Bei der Freischaltung wird die Personenbindung zwischen der Person und dem verwendeten Handy herbeigeführt. Die jeweilige Handynummer bildet den Benutzernamen und gegen Missbrauch ist man durch die Festlegung des Passwortes („Signaturpasswort") abgesichert.

In der jeweiligen Anmeldung meldet man sich mit dem Benutzernamen und dem Signaturpasswort an. Für den Signaturvorgang wird eine SMS mit einem TAN auf das registrierte Handy geschickt. Mit diesem TAN unterschreiben Sie dann in der jeweiligen Anwendung rechtsgültig.

Im Dezember 2023 hat der Umstieg von der Handy-Signatur auf die ID Austria stattgefunden. Ein Umstieg von der Handy-Signatur, welche von der Pharmazeutischen Gehaltskasse registriert wurde, lässt die Basisfunktionen der ID Austria zu.
Die ID Austria Basisfunktionen sind für die e-Service Anwendungen der Gehaltskasse ausreichend. Für unsere Nutzer*innen bedeutet das keine Änderung. Sie behalten alle Funktionen und Ihre Anmeldedaten (https://www.gehaltskasse.at/id-austria).
Die Pharmazeutische Gehaltskasse bietet diverse e-Formulare bzw. die Anmeldung in das e-Service Portal der Pharmazeutischen Gehaltskasse über die Signierung mittels ID Austria an. Die Informationen dazu finden Sie im Kapitel „Digitale Dienste".

Da die ID Austria über ihr Smartphone funktioniert, sollten Sie nicht darauf vergessen Ihr **mobiles Gerät vor unbefugten Zugriffen** zu **schützen**. Informationen zum Schutz von mobilen Geräten haben wir für Sie im Kapitel „Technische und Organisatorische Schutzmaßnahmen" zusammengestellt.

Sicherheitsmaßnahmen zum Datenschutz

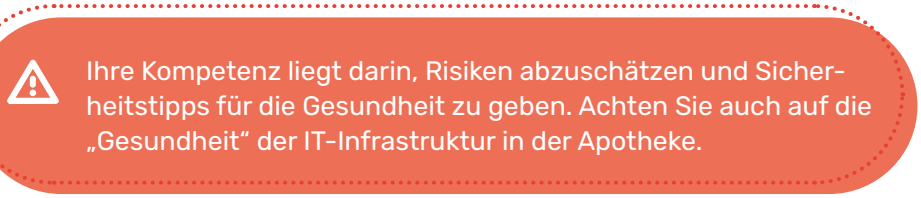
- Überlegen Sie sich, wer Zugriff auf die unterschiedlichsten Daten in der Apotheke haben soll, und schränken Sie den Zugriff gegebenenfalls ein. Sie können Benutzerprofile einrichten, mit denen Sie den Mitarbeiter*innen unterschiedliche Rechte vergeben können. Je nach Größe Ihrer Apotheke ist ein Zugriffsplan praktisch, da Sie auf einen Blick sehen können, wer welche Berechtigungen hat.
- Wichtige Unterlagen sollen nicht offen am Schreibtisch oder elektronisch am PC/Server für alle griffbereit liegen. Versperren Sie diese oder sichern Sie Ordner mit einem Passwort.
- Bedenken Sie dies auch bei der Entsorgung von Datenmaterial. Wichtig ist, dass firmen- oder personenbezogene Ausdrucke im Dokumentenvernichter landen und Daten auf Datenträgern fachgerecht zerstört werden.
- Um vorzusorgen, dass keine Firmendaten heruntergeladen werden können, könnte man die Schnittstellen, wie USB oder Card Reader, deaktivieren und nur dort Ausdrucke zulassen, wo man sie auch benötigt.
- Verwenden Sie im privaten und beruflichen Bereich keine gleichen Passwörter.
- Passwörter, PIN-Codes, Apothekerausweis, sowie auch Schlüssel stellen einen besonderen Wert dar – gehen Sie vorsichtig damit um. Ändern Sie Ihre Passwörter regelmäßig, geben Sie diese nicht weiter und wenn Sie das Gefühl haben, dass ein Dritter Ihre Passwörter kennt – ändern Sie sie.
- Aktivieren Sie die ID Austria für einen sicheren Zugang in das e-Service Portal der Pharmazeutischen Gehaltskasse.
- Social-Engineering ist eine nicht-technische Methode, die menschliche Charaktereigenschaften (z.B. Gutgläubigkeit) ausnützt, um so an vertrauliche Informationen zu gelangen und ist oft schwer erkennbar. Sie sollten Ihre Mitarbeiter*innen aber daraufhin sensibilisieren. Auch Lieferanten oder Handwerker könnten aus reiner Neugier an Informationen gelangen, die nicht für sie bestimmt sind.
- Denken Sie immer daran, dass Sie hoch sensible Daten in Ihrer Apotheke verwalten und verarbeiten. Lassen Sie nur Personen, denen Sie wirklich vertrauen an Ihre technischen Geräte und in Ihre Räumlichkeiten. Unzureichend geschulte Mitarbeiter*innen oder selbst ernannte „Hobbytechniker“ sollten in Ihrer Apotheke keinen Platz haben.
- Informieren Sie sich regelmäßig zur aktuellen Gesetzeslage im Datenschutz und benutzen Sie die bereitgestellten Informationen auf der Homepage der Österreichischen Apothekerkammer und der Pharmazeutischen Gehaltskasse.

2. Die Apothekeninfrastruktur

Für Sie als Apotheker*in ist es wichtig, dass Sie Ihren täglichen Arbeiten in der Apotheke störungsfrei nachgehen können. Dazu muss allerdings die Technik funktionieren. Die Verfügbarkeit der Informationstechnologie und der diversen technischen Systeme und Werkzeuge ist essenziell für den Betrieb in der Apotheke.
Ohne IT-Unterstützung ist der Arbeitsablauf, so wie er heute funktioniert, kaum mehr vorstellbar. Es ist meist selbstverständlich, dass Sie ein POS-System im Einsatz haben, dass Sie Bankomaten und Lagerautomaten ansteuern, Lagerbewirtschaftung, Rezeptverrechnung und das Rechnungswesen mittels Computerunterstützung durchführen, sowie im Internet recherchieren.

Vor einigen Jahren wurde an der Tara noch mit dem Warenverzeichnis in Papierformat und Registrierkassen gearbeitet. Wenn man den Lagerstand wissen wollte, wurde einfach in der Lade nachgeschaut. Die Bestellung wurde mit Minikarten über Apodat telefonisch durchgeführt. Jedes Rezept musste taxiert und nummeriert werden und die Sammelaufstellung wurde per Hand geschrieben. Gefühlt ist das noch gar nicht so lang her.

Die technische Entwicklung in der Apotheke ist in den letzten Jahren rasant vorangeschritten. Viele Abläufe wurden erleichtert und viele neue Herausforderungen sind im Zuge der Digitalisierung dazugekommen.



Durch die Vorschriften in der Apothekenbetriebsordnung haben Apotheken eine weitgehend vorgeschriebene Struktur, trotzdem hat jeder Betrieb unterschiedliche Ansprüche und individuelle Gegebenheiten.

Eine klare Trennung der Infrastruktur für den privaten und geschäftlichen Bereich sollte angestrebt werden. Nur mit einer klaren Trennung des Netzwerkes können Sie sicherstellen, dass geschäftliche und private Belange nicht miteinander vermischt werden. Sie können so auch separate Einstellungen, wie z.B. spezielle Internetseiten sperren, speziell für Ihren Betrieb vornehmen.

Technische IT-Infrastruktur

Die IT-Infrastruktur ist das zentrale Steuerungselement aller digitalen Prozesse in Ihrer Apotheke. Aus diesem Grund sollten Sie diese immer aktuell halten, hegen und pflegen. Unter IT-Infrastruktur versteht man die Komponenten, die für die Ausführung und Verwaltung unternehmensfähiger IT-Umgebungen notwendig sind. Dazu zählt Hardware, wie Server, PCs, Router, haustechnische Anlagen sowie Software und Netzwerkkomponenten für die Verbindung innerhalb und außerhalb der Apotheke. Diese Komponenten können in unternehmenseigenen Strukturen oder innerhalb von Cloud Systemen umgesetzt werden.

Apothekenhardware

Das Herzstück jeder IT ist der **Server**, auf dem alle gemeinsam genutzten Ressourcen, wie Programme, Laufwerke, Drucker und Daten, zentral gespeichert und zur Verfügung gestellt werden können. Der Apotheken Server sammelt dabei alle Ihre Daten an einer zentralen Stelle und bildet somit das Gehirn Ihrer Apotheke.

Arbeiten Sie nicht direkt am Server. Dieser soll die Dienste für Ihre PCs zur Verfügung stellen. Bedenken Sie, dass z.B. im Falle eines Programmfehlers am Server oder wenn Daten irrtümlich gelöscht werden, Ihr gesamtes IT- System betroffen ist und Sie nicht mehr auf Ressourcen und Daten zugreifen können. Im schlimmsten Fall hätten Sie einen kompletten Ausfall ihrer IT.

Server sind für gewöhnlich die leistungsstärksten Geräte im Netzwerk und technisch so ausgestattet, dass sie möglichst nie ausfallen. Das ist auch der wesentliche Vorteil gegenüber einem Computer - die Ausfallsicherheit. Achten Sie aber immer auf ein aktuelles Betriebssystem, für das es auch Sicherheitsupdates gibt.

Um die **Ausfallsicherheit** des Servers weiter zu erhöhen, können z.B. RAID-Systeme eingesetzt werden. Darunter versteht man einen Zusammenschluss von mehreren Festplatten. Fällt eine Festplatte aus, kann eine andere deren Funktion übernehmen und der laufende Betrieb wird nicht gestört. Sollte eine Festplatte ausfallen, wird meist eine Fehlermeldung über eine „Monitoring Software“ ausgegeben und Sie können die defekte Festplatte während des Apothekenbetriebes tauschen lassen. Monitoring Systeme können auch weitere kritische Prozesse, wie Temperatur, Speicherkapazität, Update-Status, Datenbank und/oder Datensicherung überwachen.

Ein Server läuft rund um die Uhr und sollte am besten geschützt in einem **Serverschrank** aufgestellt werden. Einerseits um das Gerät vor Staub und Schmutz zu schützen und andererseits, um vorzubeugen, dass das Gerät irrtümlich beschädigt oder ausgeschaltet werden kann. Auch andere wichtige Netzwerkkomponenten wie Switches, Router, die Telefonanlage und dergleichen sind im Serverschrank gut aufgehoben.

Meistens werden die **Daten** auf dem Server abgelegt. Die auf dem Server gesammelten und gespeicherten Daten sollten bei der täglichen Datensicherung an einem separaten

Ort abgelegt werden.

Es gibt aber auch die Möglichkeit, die Daten außerhalb Ihres Servers, auf externen Speichermedien oder auf einem Cloud System, zu speichern. Der Vorteil solcher Systeme besteht darin, dass hier umfangreiche Datenmengen bewältigt werden können und diese für eine höhere Ausfallsicherheit redundant ausgelegt werden können. Der Nachteil eines Cloud Systems besteht darin, dass Sie nicht die alleinige Hoheit über Ihre Daten haben.

Für den täglichen Arbeitsablauf an der Tara haben Sie **Tara PCs** und Barcodescanner im Einsatz. Tara PCs sind meist Touch-PCs und sind über ein kabelgebundenes Netzwerk mit dem Server verbunden.

Wenn Sie Daten auf den PCs lokal speichern, müssen Sie bedenken, dass nicht alle Mitarbeiter*innen auf den gleichen Datenbestand zugreifen können bzw., ob diese Daten auch regelmäßig gesichert werden.

Wenn Sie **hochwertige Komponenten** einsetzen, dann sind Sie gut für die Zukunft gerüstet. Achten Sie auch auf das Alter Ihrer eingesetzten Hardware. Nach fünf Jahren haben PCs ihr Systemalter erreicht und sind nicht mehr leicht zu optimieren. Ein Kollege hat diesbezüglich einmal einen Vergleich gebracht: „*Wenn man versucht einen alten PC zu optimieren, dann ist das so, als ob man eine gebrechliche Person jeden Tag zur Physiotherapie schickt, damit sie einen Marathon laufen kann.*“

Wenn Sie die wichtigsten Komponenten redundant auslegen, für eine unterbrechungsfreie Stromversorgung und für eine regelmäßige Datensicherung sorgen, dann haben Sie gut vorgesorgt. Lassen Sie alle Schutzmaßnahmen von einem Profi planen!

Apothekensoftware

Eine Software ist nichts anderes als ein Computerprogramm. Sie brauchen Software auf den elektronischen Geräten, um effizient arbeiten zu können.

In erster Linie werden Sie eine Apothekensoftware im Einsatz haben, mit deren Hilfe Sie Ihren täglichen Ablauf in der Apotheke steuern können. Gewöhnlich ist Software kostenpflichtig, es gibt aber auch Freeware und Testversionen, die Sie gratis verwenden können. Achten Sie hier besonders darauf, dass sie frei von Viren und sonstiger Malware ist.

Im Allgemeinen wichtig für Software ist, dass sie korrekt lizenziert ist. Das kann Ihnen unter Umständen viel Ärger ersparen. Für jedes lizenzpflichtige eingesetzte Programm müssen Sie eine entsprechende Lizenz nachweisen, ansonsten handelt es sich um eine Urheberrechtsverletzung. Lassen Sie sich die Lizenzen aushändigen und allfällige Lizenzfreiheit von Ihrem Softwarebetreuer bestätigen. Im Falle einer Unsicherheit können Sie ein Lizenzverfahren anstreben und von Ihrem Betreuer eruieren lassen, ob alles korrekt ist.

Vermeiden Sie Softwaremüll! Prüfen Sie genau, ob Sie ein kostenloses Programm wirklich brauchen und laden Sie Programme nur von bekannten Webseiten herunter!

Ein weiterer wichtiger Punkt in Bezug auf die Software bzw. das Betriebssystem ist eine regelmäßige Aktualisierung. Die Hersteller stellen in regelmäßigen Abständen kostenlose Updates, mit denen Sicherheitslücken im System behoben werden, zur Verfügung.

Lesen Sie alle Meldungen bzw. auch Fehlermeldungen Ihres PCs genau durch und setzen Sie nicht unbedacht ein „Hakerl“ oder klicken Sie nicht einfach auf „ok“.

Apotheken-Netzwerk

Das **Apotheken-Netzwerk** bildet die Nervenbahnen Ihrer Apotheke und ist ein sehr wichtiger Bestandteil Ihrer Kommunikation. Das Netzwerk erhält eine öffentliche Nummer (IP-Adresse) über welche die elektronischen Geräte erreichbar sind. Die kabelgebundenen Verbindungen werden LAN (Local Area Network) genannt und die Funkverbindungen WLAN (Wireless Local Area Network). Für die Verbindung in das Internet braucht es eine Internetverbindung zu einem Internet-Provider. Auch ein getrenntes Netzwerk für E-Mail oder für Ihre Mitarbeiter*innen könnte aufbaut werden.
Setzen Sie für die interne Kommunikation immer auf verschlüsselte Verbindungen und zentrale Laufwerke, um geschäftliche Dokumente auszutauschen. Benutzen Sie hierfür keine USB-Sticks und private Notebooks.

Um Internet, Anwendungen und Ressourcen auf allen Computern gemeinsam zu benützen, braucht man ein lokales Netzwerk. Über den Server können Sie Dienste und Programme gemeinsam nutzen und auf die gleichen Datenbestände zugreifen – kurz gesagt, alle elektronischen Aktivitäten werden über das Apotheken-Netzwerk gesteuert. Sie können auch Hintergrundmusik oder elektronische Werbetafeln über Ihr Netzwerk steuern.

In einigen Apotheken sind Kommissionierautomaten im Einsatz. Die Steuerung erfolgt auch über das interne Apotheken-Netzwerk. Es gibt vollautomatische Systeme oder das klassische Automatensystem. Wichtig ist, ein ausgereiftes Programm zu verwenden, Spitzenkomponenten einzusetzen, für eine regelmäßige Wartung und für eine unterbrechungsfreie Stromversorgung zu sorgen.

Die **Firewall** in Ihrem Netzwerk ist wie ein Türsteher, welcher nur autorisierte Verbindungen/Gespräche zulässt und dafür sorgt, dass von außen niemand direkt mit dem Netzwerk spricht. Nutzen Sie professionelle Lösungen, um Ihr Netzwerk maximal zu schützen.

⚠ Sobald Sie Ihren „persönlichen Computer“ in einem Netzwerk haben, ist es aus mit der „Persönlichkeit“. Überlegen Sie, wem Sie Zugriff auf Ihre Daten gestatten, setzen Sie Benutzerkennung und gute Passwörter ein. Vertrauliche Daten sollen auch vertraulich bleiben.

VPN-Verbindung

Über eine **VPN-Verbindung** (Virtuelles Privates Netzwerk) können Sie, unabhängig vom Standort, eine sichere Verbindung vom Apotheken-Netzwerk zu einem externen Netzwerk aufbauen.

Wenn Sie neben Ihrer Hauptapotheke eine **Filialapotheke** betreiben, dann sollten Sie in Bezug zur Kommunikation auf maximale Sicherheit setzen und auf eine VPN-Verbindung Wert legen. Eine VPN-Verbindung stellt über Zertifikate sicher, dass die Gegenstelle weiß, es handelt sich um eine autorisierte Verbindung. Außerdem sind die Übertragungen verschlüsselt und können von Kriminellen zwar abgefangen, aber nicht gelesen werden.

Die ist auch nötig, wenn Sie zum Beispiel von zu Hause auf Ihre Apothekendaten zugreifen wollen oder wenn Sie einem Fachmann erlauben Ihr System mittels VPN-Zugang zu administrieren.

Internetanbindung

Eine Trennung von Apotheken-Netzwerk und Internetzugang ist heute nicht mehr möglich. Sie expedieren Arzneimittel, bestellen die Ware über das Internet, schicken die Rezeptdaten zur Pharmazeutischen Gehaltskasse, machen Internetbanking, steuern Bankomaten an, usw.

Für welche **Internetanbindung** Sie sich entscheiden, wird sich nach dem jeweiligen Bedarf in der Apotheke richten. Hinterfragen Sie aber Ihre Providerzugänge mit den jeweiligen Konditionen regelmäßig. Wählen Sie die Bandbreite nach Ihrem Datentransfervolumen.

Drahtgebundene Netzwerke müssen mit einem Kabel verbunden werden. WLAN (Wireless Local Area Network) bzw. Bluetooth und auch Infrarot funktionieren über Funk. Kabelloses WLAN bringt einen großen Komfort, man muss sich allerdings bewusst sein, dass sich die Funkwolke bis auf die Nebengebäude und Straße ausbreiten kann. Wichtig ist, das Funknetz mit dem höchstmöglichen Verschlüsselungssystem abzusichern.
Die Internetverbindung ist für viele Prozesse in der Apotheke essenziell, deshalb empfiehlt sich auf jeden Fall eine Backup-Lösung. Möglich wäre beispielsweise ein LTE-Router, der bei Ausfall der stationären Internetverbindung über eine SIM-Karte eine Verbindung mit dem Mobilfunknetz herstellt.

Cloud Computing

Cloud Computing ist ein Konzept, das die Nutzung von skalierbaren virtualisierten IT-Infrastrukturen, Plattformen und Anwendungen ermöglicht, die über das Internet bezogen und nutzerabhängig abgerechnet werden. Auch Cloud-Dienste sind Server, welche in einem Rechenzentrum stehen. Hier werden unter anderem Datenspeicherdienste angeboten, d.h. Sie kaufen sich Festplattenkapazität in einem Rechenzentrum ein und lagern dort Ihre Daten. Es werden immer mehr Anwendungen in der Cloud angeboten. Beispiele dafür sind der Zugriff auf E-Mails in Microsoft Office 365, das Teilen von Dateien über Dropbox oder das Speichern von Bildern in der Apple iCloud. Der Vorteil liegt darin, dass Pflege und Wartung von professionellen IT-Mitarbeiter*innen durchgeführt werden.

Sie können Server, Systeme, Datenspeicher oder auch das Netzwerk virtualisieren. Sie müssen nur bedenken, dass Sie dann nicht mehr die alleinige Kontrolle über Ihre Systeme und Daten haben bzw. oft auch gar nicht lokalisierbar ist, wo die Daten verarbeitet werden. Die Anbieter geben meist Zusagen, haften aber nicht. Wobei man sagen muss, dass das Informationssicherheitsniveau bei namhaften Cloud-Anbietern hoch ist. Der Vertrag kommt zu den Konditionen des Anbieters zustande und meist nach Recht des Staates, in dem der Anbieter seine Niederlassung hat (z.B. gilt bei US-Servern das US-Recht). Nach dem Datenschutzrecht muss der Auftraggeber für die IT-Sicherheit sorgen und sich von der Sicherheit beim Dienstleister überzeugen.

Cloud-Dienste sind weder gut noch böse. Sie sind Werkzeuge, um Dinge zu erledigen. Wenn Sie diese Dienste nutzen, übergeben Sie Ihre Daten an Fremde und erwarten, dass diese sie sicher und verfügbar halten. Bei der Auswahl der Cloud Anbieter sollten Sie mit Bedacht vorgehen.

Als Tipps können wir Ihnen folgende Überlegungen mitgeben:

- Vertrauen – Handelt es sich um ein bekanntes öffentliches Unternehmen, dessen Dienste schon von Millionen von Menschen genutzt werden?
- Kundendienst – Ist es einfach Hilfe und Antworten auf Fragen zu bekommen bzw. gibt es überhaupt einen Support?
- Einfachheit – Wie einfach ist es den Dienst zu nutzen? Je komplizierter, desto wahrscheinlicher ist es, dass Sie Fehler machen und versehentlich Daten preisgeben oder verlieren. Verwenden Sie einen Cloud Anbieter, der für Sie einfach zu verstehen, zu konfigurieren und zu nutzen ist.
- Sicherheit – Ist die Übertragung in die Cloud verschlüsselt und wenn ja wer kennt den Schlüssel? Wie werden die Daten gespeichert?
- Kompatibilität - Unterstützt der Cloud Anbieter alle Geräte und Betriebssysteme, die Sie verwenden oder planen zu verwenden?

- Nutzerbedingungen - Nach welchen Gesetzen arbeitet der Diensteanbieter? Achten Sie auf die Rechte, die Sie an Diensteanbieter abtreten.

Relevant ist auch, dass Sie Ihre Cloud-Dienste richtig nutzen. Die Art und Weise, wie Sie auf Ihre Daten zugreifen und sie freigeben kann oft einen weitaus größeren Einfluss auf die Sicherheit Ihrer Daten haben als alles andere.

Einige wichtige Maßnahmen die Sie durchführen sollten:

- Verwenden Sie ein starkes, einzigartiges Passwort, um Ihr Cloud-Konto zu schützen. Nutzen Sie die Zwei-Faktor-Authentifizierung.
- Schützen Sie Ihre Daten, indem Sie nur bestimmten Personen oder Personengruppen, welche den Zugriff auch benötigen, Zugriff auf bestimmte Daten und Ordner einräumen. Sie sollten einfach nachverfolgen können, wer auf die Daten und Ordner Zugriff hat. Es muss verhindert werden, dass Daten versehentlich öffentlich freigegeben werden.
- Machen Sie sich mit den Sicherheitseinstellungen des Cloud Anbieters vertraut.
- Vergessen Sie nicht auch die Laufzeit der Verträge zu erneuern, sonst könnten Sie den Zugriff auf Daten verlieren.

Cloud Computing ist ein großer Trend, weil es einfach praktisch ist, Daten abzulegen und von jedem Rechner darauf zugreifen zu können. Bei Gratisanbieter gibt es meist keine Garantie auf Verfügbarkeit. Wenn Sie relevante Dokumente speichern wollen oder eine Cloud aus organisatorischen Gründen notwendig ist, dann setzt man besser auf lokale Anbieter mit guter Security und hoher Verfügbarkeitsgarantie. Auf der sicheren Seite ist man Anbieter zu wählen, welche zumindest aus der EU stammen und die Server auf europäischem Boden betreiben. Noch besser ist es auf österreichische Anbieter zu setzen, damit Daten und Datenschutz im eigenen Land bleiben. Bevor Sie allerdings persönliche Daten in die Cloud laden, gehören diese aus Sicherheits- und Privatsphärengründen verschlüsselt.

Gefahren für die IT-Infrastruktur

Viele Gefährdungen könnte man für die IT-Infrastruktur in Apotheken aufzählen. Neben der Gefahr vor Einbruch, Feuer, Wasser oder Strom- bzw. Netzwerkausfall liegt der Schwerpunkt in diesem Kapitel auf der Cyberkriminalität.

Gefahren für die IT-Infrastruktur sind zum einen Personen, die überdurchschnittliche Fachkenntnisse aufweisen und Computersoftware bzw. auch Hardware bauen oder verändern. Zum Beispiel wollten Hacker in das Netzwerk eindringen und möglichst viele Ihrer Informationen und persönlichen Daten sammeln.
Im Visier der Datenjäger stehen auch Dokumente in Cloud Speichern, E-Mails, Chats, oder in „Sozialen Netzwerken". Kreditkarten, Bankomatkarten und Smartphones sind ebenso gute Quellen für Spionage.

Zum anderen ist es Malware, welche als Überbegriff für bösartige Software, wie Spam, Viren, Würmer, usw., steht. Das sind Programme, die unerwünschte Funktionen auf Ihrem PC ausführen und Ihre Dateien schädigen. Mittlerweile sind rund 800 Millionen Schadprogramme im Umlauf und es werden immer mehr. Die Schäden, welche diese Schadprogramme und Hackerangriffe verursachen gehen in die Milliarden Euro. Häufig gelangen diese über fehlerhaftes Nutzerverhalten in die Apotheken-Netzwerke.
Die meisten Schadprogramme finden ihren Weg über E-Mail-Links sowie E-Mail Anhänge und da insbesondere durch Erpressungstrojaner sehr viel Geld erwirtschaftet werden kann, werden Kriminelle hier immer kreativer.

Ransomware spielte im vergangenen Jahr und wohl auch in der Zukunft eine große Rolle und ist mittlerweile zu einer richtigen Plage geworden. Firmen werden gezielt ausgewählt und mit Schadsoftware angegriffen, die den Zugriff auf Daten und Systeme einschränken oder unterbinden. Zunächst verhalten sich die Schadprogramme bzw. Hacker unauffällig, sammeln Informationen über die Beschaffenheit der IT-Infrastruktur und wertvolle Daten. Dadurch sind sie auch schwer von den Alarmsystemen zu identifizieren. Oft bleibt diese Schadsoftware wochenlang unbemerkt und kann im Netzwerk verweilen. Entweder sperrt ein solches Schadprogramm den kompletten Zugriff auf das System oder es verschlüsselt bestimmte Nutzerdaten. Für die Freigabe wird dann ein Lösegeld (Ransom) verlangt. Diese Form der digitalen Erpressung ist nicht neu und richtet sich häufig gegen Windows-Rechner. Prinzipiell können aber alle Systeme von Ransomware betroffen sein.
Der Blick muss in Zukunft noch geschärft und kleine verdächtige Verhaltensweisen untersucht werden. Regelmäßige Sicherheitsupdates aller Geräte, Virenschutzprogramme, regelmäßige Datensicherungen und Achtsamkeit bei E-Mails ist eine gute Vorsorge, um dieser digitalen Pandemie zu begegnen.

⚠ Malware kann sich auch auf Medien, wie USB-Sticks verstecken. Überprüfen Sie deshalb neue Medien vor jeder Verwendung und deaktivieren Sie die Autostartfunktion. Beachten Sie auch, dass immer mehr an Spams und Malware über soziale Portale wie Facebook oder Twitter verbreitet werden.

Spams

Der Begriff „Spam-Mail“ oder auch „Junk-Mail“ steht für alle Arten von unerwünschten E-Mails. Spams sind meist unerwünschte Werbungen, welche Ihre Daten nicht gefährden, auf Dauer aber ziemlich lästig werden können und die Speicherkapazität von Mailservern belasten.
Die wohl bekanntesten sind **Phishing-Mails** (Smishing) und Hoax.

Jedes Mail, in dem Sie aufgefordert werden, persönliche Informationen einzugeben, ist mit großer Wahrscheinlichkeit ein Phishing-Mail. Es handelt sich hier um das sogenannte Passwort Phishing und den Versuch an Nutzerdaten zu gelangen. Daher sollte man auf solche Mails nicht antworten. Sie sollen dazu verleitet werden, Ihre Kreditkartendaten bekanntzugeben, einen Account zu aktualisieren, usw. immer mit dem Ziel an persönliche Daten zu gelangen. Häufig spielen Cyberkriminelle mit Emotionen, um Sie zum Handeln zu bewegen, indem sie z.B. ein Gefühl der Dringlichkeit oder Neugierde erzeugen.
Seriöse Unternehmen würden Kontodaten oder andere persönliche Daten niemals per E-Mail verlangen. Wenn Sie von Ihrer Bank eine Mail, in der nach Ihren Kontodaten gefragt wird, bekommen, rufen Sie an und fragen Sie zur Sicherheit nach. In Phishing-Mails wird immer vorgetäuscht jemand anderes zu sein.

Hoax sind keine Viren, aber sie zeigen deutlich, wie allein nur durch Social Engineering eine E-Mail-Lawine losgetreten werden kann. Es handelt sich hierbei immer um Falschmeldungen, die sich über das Internet oder auch per SMS verbreiten. In solchen Mails werden Sie in etwa aufgefordert eine bestimmte Mail an möglichst viele Personen weiterzuleiten oder Sie werden aufgefordert Dateien/Programme auf Ihrem PC zu installieren bzw. zu deinstallieren, oder auch sich ein bestimmtes Programm zu downloaden, usw. Schenken Sie solchen Mails keinen Glauben. Sie können in verschiedenen Hoax–Listen[12] im Internet nachschauen, ob es sich um ein bereits bekanntes Hoax-Mail handelt.

[12] z.B.: http://hoax-info.tubit.tu-berlin.de/hoax/hoaxlist.shtml (31.01.2024)

Viren und Würmer

Viren und Würmer können Ihr gesamtes Netzwerk zerstören.

- **Computerviren** sind Programme die von einem zum anderen Computer, über Netzwerke, USB-Sticks oder anderen Speichermedien, übertragen werden können. Die meisten Viren werden in Dateien über E-Mail Anhänge, Downloads im Internet oder über den Besuch von manchen Webseiten übertragen, zunehmend auch über Instant Messaging. Auf Ihrem Computer wird mittels der Autostartfunktion ein Programm aufgerufen, das sofort beginnt Schaden auf Ihrem Rechner zu verursachen. Ein Virus beginnt sofort andere Programme oder Dateien zu infizieren und sich dadurch zu vervielfältigen. Das macht es nicht nur schwer zu eruieren, welche Programme betroffen sind und welche nicht, es macht auch das Entfernen des Virus sehr schwer. Die Auswirkungen eines Virus gehen von einer einfachen Systemstörung bis hin zu Datenverlust oder sogar Hardware-Defekte.
- Ein **Wurm** gleicht einem Virus, verbreitet sich aber meist durch Sicherheitslücken in der Netzwerksoftware. Ein Wurm ist in der Lage, sich ohne Zutun des Anwenders, es reicht einzig ein vernetzter Computer, zu verbreiten. Des Weiteren ist ein Wurm in der Lage, Ihr E-Mail-Adressbuch auszulesen und sich automatisch an alle darin befindenden Personen weiterzuschicken. Ein Wurm kann Störungen anrichten oder auch ungewollte Änderungen an Ihrem System vornehmen. Sie können es nicht einmal verhindern. Machen Sie deshalb zuverlässig alle Updates Ihres Betriebssystems und Ihrer Software.

Spyware und Trojaner

Spyware und Trojaner dienen zur Spionage. Das heißt, sobald man eines dieser beiden auf dem Computer hat, kann ein anderer Benutzer diese verwenden, um Ihre persönlichen Daten auszuspionieren. Man kann sich diese genau wie Viren über externe Medien (z.B. USB-Sticks) und das Internet downloaden.

- **Trojaner** können als nützliche Programme getarnt sein und spionieren nach der Installation Ihre persönlichen Daten aus. Besonders gefährliche Trojaner sind in der Lage, Hintertüren, durch die der Angreifer den PC fernsteuern kann, zu öffnen. Haben sie erst einmal die Kontrolle, können sie Daten löschen oder ändern, Nachrichten versenden, Informationen und Passwörter ausspionieren und noch vieles mehr. Das Positive daran ist, dass mit dem Löschen des Trojaners keine Spionage mehr durchgeführt werden kann. Ein Trojaner vervielfältigt sich nicht und ist somit durch das Löschen komplett von Ihrem Computer verschwunden.
- **Spyware** kann ungewollt private Daten über das Internet an Dritte senden. Die Art der privaten Informationen, die ausspioniert werden, ist unterschiedlich. So kann zum Beispiel das Surfverhalten aufgezeichnet und analysiert werden, um infolgedessen personalisierte Werbung einzublenden. Es können aber auch persönliche Daten ausgespäht werden, wie beispielsweise Kennwörter oder Kreditkartendaten. Spyware führt als Nebeneffekt auch oft dazu, dass der Rechner langsamer als gewohnt arbeitet.

Botnetz

Unter einem Botnetz versteht man ein Netzwerk aus tausenden infizierten Computern, die von einem Rechner ferngesteuert werden können. Der einzelne PC in so einem Netzwerk wird „Bot" bezeichnet.

Die **Spionageprogramme** installierten sich meist ohne Ihr Wissen. Zum Beispiel können Sie sich durch einen Klick auf einem E-Mail-Anhang oder eine URL, die eine Schwachstelle im Browser ausnutzt, einen Trojaner installieren. Sie als Computerbenutzer merken das gar nicht. Ihr PC wird aber zum „Bot" und eine dritte Person kann durch Befehle im Netzwerk Ihren PC fernsteuern.

Botnetze werden dazu verwendet, um Massen an Spams zu verteilen. Die Spamlawine kann so gut getarnt, über Zwischenstationen, verbreitet werden. Wenn Spams über Bots versendet werden, ist ein Nachverfolgen des Versenders nur unter größten Schwierigkeiten möglich. Daher werden die meisten Spams über solche Netzwerke verschickt.
Nicht selten werden solche Bots auch dafür missbraucht, um dort illegale Dateien auszuspionieren und sie dann im Internet bereitzustellen.
Auch ein großer Teil der betrügerischen Phishing-Seiten wird auf solchen Botnetzen betrieben, da das Entdeckungsrisiko für die Betrüger gering ist. Der direkte Diebstahl von Zugangsdaten oder auch Kreditkartenbetrug, wird so im großen Stil durchgeführt.

Da Botnetze auf Viren, Trojanern und Würmern basieren, sollte eine aktuelle Antiviren-Software die Schadprogramme identifizieren können. Eine gute Firewall sollte zudem in der Lage sein, den verdächtigen Netzwerkverkehr zu melden.

⚠ Der wichtigste Schutzfaktor, für alle oben genannten Gefahren, ist aber immer der Benutzer!
Wenn Sie mit dem nötigen Wissen und der richtigen Dosis an Vorsicht im Internet verweilen und mit Ihren elektronischen Geräten hantieren, werden Sie sicher weniger Probleme haben.

3. Technische und organisatorische Schutzmaßnahmen

Es ist unerlässlich, dass Sie Schutzmaßnahmen ergreifen, um Ihre Daten und kritischen Systeme in der Apotheke zu schützen. Neben den wichtigen technischen und physischen Schutzmaßnahmen sind auch organisatorische Maßnahmen essenziell. Betreiben Sie aktives Sicherheitsmanagement!

Dieses Kapitel soll Ihnen einen Überblick geben, wie die Apothekeninfrastruktur geschützt werden kann und stellt eine Ergänzung zu den vorangegangenen Kapiteln dar.

Technische Schutzmaßnahmen

Zum Schutz vor Cyberangriffen und sämtlicher Schadsoftware brauchen Sie eine **Firewall, Spamfilter und Antivirenprogramme**. Wobei ein gutes Rechtekonzept bzw. eine gute Authentifizierung und Passwortregelung ebenso notwendig sind. Regelmäßige Updates Ihrer IT-Infrastruktur verstehen sich von selbst und ebenso gute Verschlüsselungsmaßnahmen für Hardware und mobile Geräte bzw. Datenträger. Monitoringsysteme sind wesentlich, um über Probleme sofort alarmiert zu werden und können umfangreich eingesetzt werden (USV, Sicherheitsschwachstellen, Probleme mit der Infrastruktur, Klima). Wartungsverträge helfen dabei das Problem wieder rasch in den Griff zu bekommen. Sie sollten auch auf eine gute Dokumentation der Technik achten und eine Übersicht darüber haben, welche Geräte und Software Sie einsetzen. Ein Backup Ihrer Datenbestände in der Apotheke ist selbstverständlich. Nachfolgend wird auf einige Themen näher eingegangen.

Firewall

Zur Absicherung Ihres Systems und zum Schutz vor Angriffen aus dem Internet sollten Sie eine Firewall einsetzen. Sie ist eine Hürde zwischen dem Computer bzw. Server und dem Internet und somit das Herzstück eines jeden guten **Sicherheitssystems.**

Eine Firewall trennt den Datenverkehr. Um festzustellen, welcher Datenverkehr/welches Datenpaket eine Gefahr für Ihren Rechner ist, werden Regeln für die einzelnen Datenpakete festgelegt. Jedes Paket, das in Ihr Netzwerk will, muss die Firewall passieren und wird so geprüft, ob es regelkonform ist. Falls gegen eine der vordefinierten Regeln verstoßen wird, wird das Paket aussortiert. Man unterscheidet hierbei zwischen Hardware-Firewall oder Software-Firewall.

- Eine **Hardware-Firewall** ist ein eigenes Gerät. Spezielle Firewall-Hardware kann auch in Routern oder Switches integriert sein.
- Eine **Software-Firewall** wird auf PCs oder Servern installiert.

Beide Arten von Firewalls decken den Datenverkehr des ganzen Netzwerkes ab. Jeder, der mit dem Netzwerk verbunden ist, unterliegt denselben Regeln.

- Eine Personal-Firewall hingegen, ist direkt an einem Computer installiert, meist schon im Betriebssystem integriert und nur für dieses Gerät zuständig. Zusätzlich zu der normalen Funktion filtert eine Personal-Firewall auch innerhalb des Netzwerkes. Dies ist jedoch nicht nötig, wenn man eine gute Hardware- bzw. Software-Firewall im Einsatz hat.

Wichtig ist, dass Ihre Schutzsysteme immer gut gewartet werden und die Software auf dem neuesten Stand ist. Hier bietet sich an Wartungsverträge abzuschließen. Ganz unabhängig von der Größe Ihrer Apotheke ist es wichtig, dass Sie über Ihre Systeme gut Bescheid wissen. Lassen Sie sich die eingesetzten Sicherheitssysteme von Ihrem technischen Betreuer erklären.

Spamfilter

Spamfilter sind dafür geeignet, unerwünschte Mails abzuhalten. Sie können Nachrichten bestimmter Absender, oder auch Nachrichten von einer ganzen Domäne, blockieren.

Es gibt in einigen E-Mail-Programmen auch einen automatischen Spam-Filter. Dieser durchsucht den Inhalt jeder eingehenden E-Mail auf bestimmte Wörter bzw. den Absender und wenn eines der Wörter auf der „Black List“[13] des Filters steht, dann wird die Mail automatisch in einen Spam-Ordner verschoben. Natürlich können Sie diese „Black List“ bei einigen Spam-Filtern selbst anlegen oder vorgegebene mit von Ihnen ausgewählten Wörtern erweitern. Den Inhalt des Spam-Ordners können Sie jederzeit überprüfen, um so fälschlich als Spam markierte E-Mails zurück in Ihren Posteingang zu schieben.

[13] Black List: Beinhaltet alle in E-Mails verbotenen Wörter und Quellen, die nicht vertrauenswürdig sind.

Wenn Sie eine „White List“[14] hinterlegen, werden all jene Personen bzw. Domänennamen, die dort definiert sind, immer akzeptiert.

[14] White List: Beinhaltet alle vertrauenswürdigen E-Mails, Namen und Quellen.

Es gibt aber viele Möglichkeiten Spamfilter zu integrieren, zum Beispiel können sie von Ihrem Mailprovider bzw. auch über Antivirenschutzprogramme zur Verfügung gestellt werden.

Antivirenprogramme

Ein Antivirenprogramm ist eine Software, die gegen Viren, Würmer und trojanische Pferde schützen soll. Des Weiteren ist sie in der Lage Malware dieser Art von Ihrem Computer zu löschen, wenn Sie sich bereits infiziert haben.
Antivirenprogramme enthalten einen Katalog mit tausenden von Charakteristika bekannter Viren, die sie aufspüren. Die Hersteller solcher Virenschutzprogramme haben ihren Finger am Puls der Virenwelt und veröffentlichen regelmäßige Updates.

Zum **Schutz gegen Malware** hat sich ein Mix von verschiedenen Produkten als sehr wirkungsvoll erwiesen. Verwenden Sie aber nur ein Virenschutzprogramm, da sich mehrere gegenseitig behindern könnten. Auch ein Anti-Spyware-Programm sollten Sie installieren und die Computer regelmäßig nach bekannten Schädlingen durchsuchen. Antiviren- und Anti-Spyware-Programme stören sich nicht gegenseitig und sind meist schon in einem Programm integriert.

Virenschutzprogramme sollten auf jeden Fall folgende Funktionen haben:

- Automatisches Update der Virendefinitionen. Es ist sehr wichtig, dass Sie Ihre Software regelmäßig aktualisieren!
- Scannen von eingehenden und abgehenden Mails samt Anhängen.
- Termingesteuerter Aufruf einer Überprüfung des gesamten Systems. Führen Sie regelmäßig Fullscans Ihres Rechners durch, besonders auch dann, wenn Dritte daran gearbeitet haben.
- Prüfen Sie jedes neue Programm bzw. alle eingehenden Daten von Datenträgern, besonders dann, wenn Sie sie nicht selbst erstellt haben.

Diese Funktionen sollten einen Virus, Trojaner oder Ähnliches erkennen und das infizierte Objekt separieren (Quarantäne). Es kann dann in den meisten Fällen entschieden werden, ob eine Korrektur (Desinfizieren) des Objektes durchgeführt oder es gelöscht werden soll. Im Zweifelsfall sollten Sie sich für das Löschen entscheiden. Falls das nicht funktioniert, nehmen Sie den Computer vom Netzwerk und sprechen Sie mit Ihrem technischen Betreuer.

Datensicherung (Backup)

Daten können durch Hardwaredefekte verloren gehen oder bei Virenbefall manipuliert, beschädigt oder auch unbeabsichtigt gelöscht werden.
Stellen Sie sich vor, jahrelange Aufzeichnungen Ihrer Geschäfts- oder Kundendaten bzw. Lagerbewegungen und dergleichen sind unwiederbringlich verloren. Datensicherungen sind die Eckpfeiler eines jeden Katastrophenplans. Die Verantwortung zur regelmäßigen Datensicherung obliegt der Apotheke.

Daher ist ein durchgeplantes **Datensicherungskonzept** von hoher Relevanz.

Im ersten Schritt müssen Sie entscheiden, **was** Sie **sichern** möchten. Spezielle Daten, die für den Apothekenbetrieb notwendig sind, oder alles, vielleicht einschließlich Ihres gesamten Betriebssystems. Wenn Sie besonders vorsichtig sein wollen, dann sichern sie alles.

Im nächsten Schritt müssen Sie entscheiden, **wie häufig** Sie die Daten **sichern** wollen. Mit Hilfe von integrierter Sicherungsprogramme können automatische Zeitpläne erstellt werden. Übliche Zeitpläne sind stündlich, täglich und wöchentlich, aber es gibt auch Lösungen, die Dateien sofort sichern, wenn sie bearbeitet oder gespeichert werden. Wir empfehlen zumindest automatische tägliche Backups.

Im nächsten Schritt entscheiden Sie, **wie** Sie ihre **Daten sichern** wollen. Es gibt zwei Möglichkeiten: lokale oder cloudbasierte Backups.

Lokale Backups werden auf physischen Geräten durchgeführt, wie etwa auf einem externe USB-Laufwerk, auf Magnetbändern oder über sonstige Geräte, die über das Netzwerk erreichbar sind. Der Vorteil lokaler Backups besteht darin, dass große Daten-

mengen schnell gesichert und auch wiederhergestellt werden können. Der Nachteil ist, dass Schadsoftware auch auf die Backups übergreifen kann und physische Sicherungen auch verloren gehen bzw. gestohlen werden könnten. Stellen Sie sicher, dass Backups an einem sicheren Ort aufbewahrt werden. Um Georedundanz zu erreichen, ist es empfehlenswert, die Datensicherungsmedien außerhalb der Apotheke aufzubewahren, am besten in einem feuerfesten Tresor. Als zusätzliche Sicherheitsmaßnahme können Backups auch verschlüsselt werden.

Cloudbasierte Lösungen sind Onlinedienste, die die Daten über das Internet sichern und speichern. In der Regel installieren Sie eine Anwendung, welche dann automatisch Sicherungskopien der Daten, entweder zu einem festgelegten Zeitpunkt oder bei Änderungen bzw. Speicherung, erstellt. Die Vorteile von Cloud-Lösungen liegen in der Einfachheit, der Automatisierung der Backups und dem Zugriff auf die Dateien von fast jedem Ort aus. Katastrophen, wie Feuer oder Diebstahl haben keine Auswirkung auf diese Backups. Der größte Nachteil ist die Bandbreite, die verbraucht wird. Ob Daten gesichert und wiederhergestellt werden können, hängt von der Menge der zu sichernden Daten und der Geschwindigkeit der Internetverbindung ab.

Beachten Sie einige wichtige Punkte:

- Überprüfen Sie immer, ob die Datensicherung korrekt durchgeführt worden ist. Bei automatischen Sicherungen werden Sie durch Statusmeldungen auf eventuelle Unregelmäßigkeiten aufmerksam gemacht.
- Testen Sie regemäßig, ob Ihre Backups funktionieren, indem Sie eine Datei wiederherstellen.
- Wenn Sie ein System, einschließlich des Betriebssystems, aus der Sicherung wiederherstellen, müssen Sie vorher auch die neuesten Sicherheitspatches und Updates einspielen.
- Wichtig ist, dass zwei Personen (wegen Urlaub, etc.) für die Datensicherung verantwortlich sind und diese dahingehend auch gut eingeschult werden.
- Wenn Sie eine Cloud Lösung verwenden, dann informieren Sie sich über die Sicherheitsoptionen und ob eine zweistufige Verifizierung möglich ist. Achten Sie auch darauf, dass die Lösung leicht zu bedienen ist.
- Sie können auch lokale und cloudbasierte Lösungen parallel einsetzen.

Lassen Sie sich in Bezug auf die Datensicherung, sei es nun das Verfahren oder die Backup Variante von Ihrem Softwarehaus bzw. technischen Betreuer der Apotheke beraten.
Wenn Sie von Zeit zu Zeit eine Rücksicherung der gespeicherten Daten üben, können Sie in einem Notfall sicher und rasch handeln.

Wartungsverträge

Wartungsverträge erhöhen zwar nicht die Sicherheit, tragen aber zu einer rascheren Fehlerbehebung bei. Sie können Wartungsverträge für Ihre Apothekensoftware und Hardwarekomponenten abschließen, wobei bei Hardware oft eine Garantieverlängerung zur gesetzlichen Garantie gekauft werden kann.
Klären Sie bei Abschluss die Gegebenheiten, ob Ersatzteile lagernd sind, ob und wie oft gewartet wird und vor allem, wie schnell auf ein Problem reagiert wird. Meist ist eine kurze Reaktionszeit mit höheren Kosten verbunden. Weiter zu beachten ist auch, ob ein Techniker zu Ihnen in die Apotheke kommt und der Vertrag Material plus der Dienstleistung inkludiert und keine Fahrtkosten extra zu bezahlen sind.
Erfragen Sie auch, ob es durch die Wartung zu Unterbrechungen im laufenden Apothekenbetrieb kommen kann und wie lange die Wartung dauert.

Eine ähnliche Variante ist ein Leasingangebot mit Wartungsvertrag. Zum Beispiel können Drucker geleast werden. Das Gerät wird gewartet, kaputte Teile werden gratis ausgetauscht und um den Tonerkauf müssen Sie sich auch keine Gedanken machen.

Vor einem technischen Gebrechen ist keiner gefeit. Je besser Sie vorsorgen, desto weniger Probleme werden Sie in so einem Fall haben.
Überprüfen Sie Ihre Infrastruktur und Sicherheitsvorkehrungen regelmäßig auf diverse Fehler und lassen Sie Ihre Hardware von Zeit zu Zeit von Fachpersonal überprüfen und optimieren.

Schutzmaßnahmen für mobile Geräte und Apps

Mobile Geräte wie Tablets, Smartphones und/oder Smartwatches sind zu einer wichtigen Technologie geworden, die wir in unserem privaten und beruflichen Leben nutzen. Mobile Geräte sind eine faszinierende und einfache Möglichkeit, mit Freunden zu kommunizieren, online einzukaufen, Bankgeschäfte zu erledigen und für die Signierung mittels ID Austria auf unserer Homepage relevant.

Das Wichtigste, das Sie zum Schutz Ihres Gerätes tun sollten, ist die automatische **Bildschirmsperre** bei Nichtnutzung zu aktivieren. Dadurch wird es für andere Personen wesentlich schwieriger auf Daten zuzugreifen, sollte Ihnen das Gerät verloren gehen oder gestohlen werden. Eine SIM-Sperre verhindert, dass das Telefon ohne Code eingeschaltet werden kann und ist auch zu empfehlen.

Angriffsszenarien bei Smartphones sind vor allem Phishing und Spams. Smishing (ein Kunstwort aus SMS und Phishing) sind Angriffe, bei denen Cyber-Angreifer SMS, Textnachrichten oder ähnliche Messaging-Technologien verwenden, um Sie zu einer Aktion zu verleiten, die Sie nicht durchführen sollten.

Eine automatische **Aktualisierung** des Betriebssystems ist wichtig. Pflegen Sie die Browserdaten regelmäßig und gehen Sie achtsam mit Ihrem Smartphone um. Überlegen Sie sich, eine Sicherheits-Software für mobile Geräte zu installieren.

Wichtig ist, dass Sie keine persönlichen Daten in einem öffentlichen WLAN übertragen. Verwenden Sie stattdessen die Hotspot-Funktion des Smartphones und damit Ihre mobile Datenverbindung.

Sie können auch überlegen eine Software zu installieren, welche Ihnen erlaubt, das mobile Gerät aus der Ferne über das Internet zu orten und/oder aus der Ferne zu sperren. Das kann im Falle einer notwendigen Standortermittlung recht praktisch sein.

Was mobile Geräte so leistungsfähig macht, sind die Tausende von **Apps**, aus denen wir wählen können. Diese Apps ermöglichen uns, produktiver zu sein, mit anderen zu kommunizieren und sich auszutauschen, zu trainieren und sich weiterzubilden oder einfach mehr Spaß zu haben. Als App bezeichnet man eine Software, die auf Smartphones, Tablets und mittlerweile schon auf allen möglichen Geräten heruntergeladen werden kann. Apps müssen genau so, wie auch das Betriebssystem des Computers und die mobilen Geräte aktualisiert werden. Die Entwickler der Apps erstellen und veröffentlichen Updates, um diese Schwachstellen zu beheben und Ihr Gerät zu schützen.

Cyberkriminelle haben es verstanden bösartige Apps zu erstellen und zu verbreiten, die den Anschein erwecken legitim zu sein. Wenn eine dieser Apps installiert wird, können Kriminelle oft die vollständige Kontrolle über das mobiles Gerät oder Ihre Daten übernehmen. Deshalb sollten Sie sicherstellen, dass Sie nur sichere mobile Apps aus vertrauenswürdigen Quellen herunterladen.

Laden Sie deshalb für Apple-Geräte mobile Apps nur aus dem Apple App Store herunter. Für Android-Geräte sollten Sie mobile Apps nur aus dem Google Play Store herunterladen.

Der Vorteil hierbei ist, dass Apple bzw. Google eine Sicherheitsüberprüfung aller mobilen Apps vornehmen, bevor sie den Kund*innen zur Verfügung gestellt werden. Es können zwar nicht alle bösartigen Apps abfangen werden, aber verwaltete App Stores reduzieren das Risiko drastisch.

Sie können bei Android Geräten erlauben mobile Apps auch aus anderen Quellen herunterzuladen. Wir raten dringend davon ab, da jeder Cyberkriminelle leicht bösartige mobile Apps erstellen und so verbreiten kann.

Grundsätzlich ist es wichtig, sich über die Apps zu informieren bevor Sie sie herunterladen und installieren. Je länger ein App öffentlich ist, je mehr Menschen es verwenden und je häufiger der App-Anbieter sie aktualisiert, desto wahrscheinlicher ist es, dass Sie der App vertrauen können.

Achten Sie auch auf Ihre Privatsphäre. Wenn Sie Apps die Berechtigungen geben auf Ihren Standort oder das Mikrofon bzw. auch auf Ihre Kontakte zuzugreifen, dann erlauben Sie dem Ersteller der App möglicherweise auch Sie zu verfolgen oder sogar Informationen an andere weiterzugeben oder zu verkaufen. Wenn Sie eine App nicht mehr verwenden oder sie nicht mehr nützlich finden, dann entfernen Sie sie von Ihrem mobilen Gerät.

Schutz der physischen Infrastruktur

Unterschätzen Sie nicht die physische Sicherheit der Infrastruktur. Achten Sie darauf, dass Ihre technischen Geräte vor Diebstahl geschützt sind. Der Serverschrank bzw. die Datenträgerarchive sollten nicht für jeden zugänglich sein. Wenn möglich sollten keine mobilen Geräte, wie Laptops oder Smartphones unbeaufsichtigt in der Offizin liegen.
Auch Naturkatastrophen, wie zum Beispiel Feuer und Wasser, können großen Schaden anrichten. Für solche Gefahren gibt es die Möglichkeit Versicherungen abzuschließen. Eine gute Planung von Vorsorgemaßnahmen ist aber trotzdem sehr empfehlenswert, da zum Beispiel im Falle eines Brandes viele Unannehmlichkeiten auf Sie zukommen können.

Ihre Rezepte sind ohne Ihr Zutun gegen Feuer, Verlust durch Diebstahl und Vandalismus von der Pharmazeutischen Gehaltskasse automatisch versichert.

Schutzmaßnahmen zur Vermeidung von Einbrüchen gibt es viele, mechanische und elektronische. Es gibt die unterschiedlichsten Arten von Alarmanlagen und die Möglichkeit die Anlage direkt mit einem Sicherheitsdienst oder der Polizei zu vernetzen. Lassen Sie sich zu Ihrer baulichen Absicherung von einem Experten beraten, da immer die Gesamtumstände betrachtet werden müssen.

Vergessen Sie nicht, dass sämtliche Infrastruktur in Gebäuden, wie etwa Strom, Abwasser, Heizung usw., computergesteuert ist. Somit kann der Ausfall der Stromversorgung, der Telefon- bzw. Internetleitung große Probleme mit sich bringen bzw. eine „mittlere“ Katastrophe darstellen.

Vor Stromausfällen bzw. -schwankungen kann eine **USV-Anlage** (unterbrechungsfreie Stromversorgung) schützen. Je nach Größe der USV-Anlage und dem Bedarf in der Apotheke kann sie dazu dienen, alle Kernelemente, wie etwa den Serverschrank, die Tara PCs, Steckdosen an denen relevante Rezepturgeräte angesteckt sind, sowie auch die Steuerung für die Eingangstür, in Ihrem Netzwerk abzusichern.

Personelle Schutzmaßnahmen

Das Apothekenpersonal ist im Fachgebiet sehr gut ausgebildet, aber es ist auch notwendig, dass alle darüber Bescheid wissen, welche Gefahren die digitale Welt birgt. Cyberkriminalität steigt von Jahr zu Jahr und es ist notwendig sehr aufmerksam zu agieren. Alle Mitarbeiter*innen müssen in Richtung IT-Sicherheit sensibilisiert sein und eine gewisse Grundkenntnis über Gefahren haben und wie man diesen begegnen kann.
Wichtig ist, dass Sie klare Verhaltensregeln in Ihrer Apotheke aufstellen.

Dürfen Ihre Angestellten zum Beispiel im Internet surfen, Firmeninventar privat nutzen, private E-Mails über den Apothekenaccount schicken, Software auf einem PC installieren, private Daten speichern, sich mit privaten Geräten in das WLAN der Apotheke einwählen, usw. Jeder einzelne dieser Punkte birgt Risiken und muss individuell überlegt werden.

Untersagen sie z.B. die Nutzung von Datenträgern, wie USB-Sticks, an Ihrer Apotheken-EDV. Immer wieder nutzen Kriminelle die Neugierde aus und verteilen beispielsweise USB-Sticks vor Gebäuden, denn statistisch dauert es nur ca. 30 Minuten bis neugierige Mitarbeiter*innen diesen in einen Firmenrechner stecken.

Unterschätzen Sie auch nicht die Gefahren rund um die sozialen Netzwerke, ChatGPT und Co. Die Offenlegung von Apothekendaten, sei es nun wirtschaftliche und/oder kundenbezogene Daten, über Onlinedienste bzw. soziale Plattformen ist strikt zu untersagen.

Regelmäßige Teammeetings in Bezug auf Sicherheit können ebenso sehr effektiv sein. Unter anderem könnten verschiedene Gefahrenszenarien durchdacht werden, neue Ideen zur Verbesserung der Sicherheit eingebracht werden bzw. Bedienungsanleitungen für Alarmanalagen, Feuerlöscher und dergleichen aufgefrischt werden.

Ein gutes Rechtekonzept ist auch ein wesentlicher Beitrag für die Sicherheit der Apothekeninfrastruktur. Wählen Sie mit Bedacht, wem Sie Zugriff auf Ihre Firmendaten geben. Administrationsrechte sollten den IT-Fachexpert*innen vorbehalten sein.

⚠ Awarenessbildung und IT-Sicherheitsmaßnahmen sind unerlässlich, um einem Cyberangriff zu entkommen.
Betreiben Sie aktives Sicherheitsmanagement in Ihrer Apotheke.

Alltägliche Schritte, mit denen Sie datensparsam im Netz unterwegs sein können, hat Tactical Tech im „Data Detox Kit“ bereitgestellt (https://datadetoxkit.org/de/home/). Nehmen Sie sich dafür Zeit, es lohnt sich.

4. Strategische Schutzmaßnahmen

Qualitäts- und Prozessmanagement

Qualitäts- und Prozessmanagement ist ein interessantes Thema für den Gesundheitsbereich und zunehmend auch für Apotheken. Sie als Apotheker*in sind Manager*in Ihrer Apotheke.

Prozessmanagement ist die grundlegende Voraussetzung für die **Erhaltung oder Verbesserung der Wettbewerbsfähigkeit eines Unternehmens** und sichert seine Existenz. Prozess– und Qualitätsmanagement zielt darauf ab, die Effektivität und Effizienz der Prozesse zu optimieren, sowie Kundenzufriedenheit und Qualität zu erhöhen.

Qualitäts- bzw. Prozessmanagement bezeichnet aufeinander abgestimmte Tätigkeiten zum Leiten, Lenken, Planen, dem Betrieb und der Weiterentwicklung von Arbeitsabläufen und der Qualität in einem Unternehmen.

Ziel eines Prozesses bzw. **Qualitätsmanagementsystems** in der Apotheke kann es sein, die Prozessabläufe in der Apotheke, vor allem auch in Bezug auf Kundenzufriedenheit, regelmäßig zu optimieren und gegebenenfalls zu verbessern.

Bei der Warenübernahme könnte beispielsweise überlegt werden, wie oft geliefert wird, wer die Ware in das System einbucht, wer sie wegräumt, wie mit Fehllieferungen umgegangen wird, ob alle Arbeiten durchgeführt werden oder ob es Doppelgleisigkeiten gibt bzw. kennen alle Mitarbeiter*innen die notwendigen Arbeitsschritte, usw.

Die Abläufe werden analysiert und eventuell verändert. Bedenken Sie, dass die neuen Abläufe gemeinsam mit Mitarbeiter*innen gestaltet werden sollen, damit keine Akzeptanzprobleme von neu gestalteten Prozessen auftreten. Achten Sie darauf, die neuen verbesserten Abläufe auch den Mitarbeiter*innen bekannt zu machen.

Ziel soll es sein, Fehlerquellen und Missverständnisse durch klare Aufgaben bzw. Kompetenzverteilung zu reduzieren und die Arbeitsabläufe effizient und effektiv zu gestalten.
Auch wenn jeder seine Arbeiten kennt und diese auch schon jahrelang macht, kann es doch Verbesserungswünsche und -vorschläge geben.

Informationssicherheitsmanagement

Da in der Apotheke besonders schützenswerte Informationen gespeichert und verarbeitet werden, könnten Sie überlegen ein **IT-Sicherheitshandbuch** zu entwickeln. Ziel ist es, die IT-Sicherheit in der Apotheke zu beschreiben, die Risiken im IT-Bereich aufzuzeigen und zu minimieren, sowie die Mitarbeiter*innen auf Sicherheitsthemen zu sensibilisieren. Wichtig ist, zuerst die Unternehmenswerte zu erheben und zu klassifizieren. Als nächsten Schritt sind die Gefahren und Risiken zu beschreiben, sowie Schätzungen bezüglich Eintrittswahrscheinlichkeiten und Auswirkungen vorzunehmen. Dann kann mit der Planung und Umsetzung von Sicherheitsmaßnahmen begonnen werden. Achten Sie dabei auf rechtliche Vorgaben.

Ein weiterer wichtiger Punkt in Bezug auf die Mitarbeiterführung ist der **Sicherheitsleitfaden**. Unabhängig von der Größe Ihrer Apotheke müssen die Mitarbeiter*innen wissen, was sie dürfen und was nicht.

Gute Richtlinien erklären den Sinn und Zweck der Inhalte.

Die persönliche Sicherheit der Mitarbeiter*innen in der Apotheke steht immer an oberster Stelle!

Informationen dazu können sie dem österreichischen Informationssicherheitshandbuch entnehmen: https://www.sicherheitshandbuch.gv.at (31.01.2024).

Notfallmanagement

Ein gutes Notfallmanagement soll die Kontinuität des Apothekenbetriebes während eines Notfalls sicherstellen. Der Inhaber einer öffentlichen Apotheke ist verpflichtet den Betrieb der Apotheke aufrechtzuerhalten und die Abgabe von Arzneimitteln sicherzustellen (ApoG § 13 Betriebspflicht)[15].

Es empfiehlt sich deshalb Überlegungen dahingehend zu treffen, wie mit Vorfällen verschiedenster Art umgegangen und darauf reagiert werden kann. Dabei sind nicht nur technische Maßnahme zum Wiederanlauf zu beachten, sondern im Notfall müssen auch organisatorische Abläufe gut funktionieren.

In der Apotheke kann es verschiedenste Notfälle geben, sei es, dass ein zentrales IT-System ausfällt und den gesamten IT-Betrieb lahmlegt oder, dass ein Stromausfall eine „mittlere" Katastrophe verursacht, wenn automatische Türen, Kommissionierapparat oder sonstige stromgesteuerte technische Systeme nicht mehr laufen. Auch höhere Gewalt, wie ein Blitzeinschlag oder Hochwasser, können einen Notfall auslösen, oder leider auch vermehrt durch menschliches Zutun, wie etwa durch Ransomware Angriffe.

Cybersicherheit und Notfallvorsorge bedeutet, **Cyber-Security als Ganzes zu Betrachten** und in effektive Sicherheitsmaßnahmen zu investieren. Wichtig ist eine gute und entsprechende Sicherheitsarchitektur. Sie können auch Cyber-Versicherungen abschließen und von bestimmten Versicherungsleistungen profitieren.

Die Folgen von Cyberangriffen sind meist mit erheblichen Kosten für die Datenwiederherstellung und Systemrekonstruktion verbunden. Ein kompromittiertes System ist nicht mehr vertrauenswürdig. Alle Daten und alle Programme könnten manipuliert worden sein. Nach einem solchen Vorfall müssen zwingende Maßnahmen durchgeführt werden. Dazu gehören die vollständige Trennung des IT-Systems vom Netzwerk, die Neuinstallation des Betriebssystems, das Einspielen der Backups, die Änderung von allen Passwörtern, das Scannen des Systems auf mögliche Schadsoftware, der Austausch von bestimmten Hardwarekomponenten wie Datenträgern, die Analyse von Dateien, die nicht wiederhergestellt werden können, sowie das Einspielen von sicherheitsrelevanten Patches und Updates.

Es kann auch zu Schadensersatzanforderungen bzw. zu einem Reputationsverlust kommen. Wenn Apotheken gesperrt werden müssen, wie etwa nach Hacker Angriffen, müssen die Kosten für Beweissicherung, Analyse, Spurensuche und Schadensbegrenzung meist selbst getragen werden, sowie auch Anwalts- und/oder Prozesskosten.

Wichtig ist, dass verdächtiges Verhalten erkannt wird. In der Regel sind folgende Informationen für die Bewertung eines Vorfalles wichtig:

- Beschreibung des Problems
- mögliche Ursache (Technische Ausfälle, Umweltfaktoren)
- welche Bereiche und Systeme sind betroffen

[15] Apothekengesetz § 13: „Der Inhaber einer öffentlichen Apotheke sowie der verantwortliche Leiter einer solchen ist verpflichtet, den Betrieb der Apotheke ununterbrochen aufrecht zu erhalten; ebenso darf bei der Übernahme einer Apotheke durch einen Dritten in deren Betriebe keine Unterbrechung eintreten."

- handelt es sich um eine Datenschutzverletzung
- könnten Daten unbefugt manipuliert worden sein
- welche Schritte wurden bereits gesetzt und wer wurde informiert

Wichtig ist, dass Sofortmaßnahmen eingeleitet werden und intern wie auch extern verantwortliche Personen informiert werden. Bei Betriebsunterbrechungen muss eine Meldung an die Gesundheitsbehörde bzw. an die Apothekerkammer gemacht werden. Um Sofortmaßnahmen setzten zu können, empfiehlt es sich Handlungsanweisungen für spezielle Ereignisse zu definieren und sich den Themen rund um die Abwicklung der Tätigkeiten in der Apotheke zu widmen.

Für folgende Bereiche sollten Sie sich über Sofortmaßnahmen Gedanken machen:

- Einkauf (Telefon, Warenwirtschaft, E-Mail und Lieferungen)
- Lagerhaltung (Kommissionierautomat, Kühlschrank, Sicherheitsschränke)
- Herstellung (elektronische Geräte und Waagen)
- Abgabe (Kommissionierautomat, Kasse, e-card Infrastruktur, Türen)
- Büro (Rezeptverrechnung, Lohnverrechnung, Buchhaltung, Telefon, Bank, Zeiterfassung)

In Notfällen sind klare Pläne und Anweisungen eine große Hilfe, um die Ruhe zu bewahren und die richtigen Schritte zu setzen. In Bezug zu den oben genannten sensiblen Bereichen können Sie sich folgende Fragen stellen:

- Wie könnte ein Notbetrieb funktionieren?
- Welcher manueller Ersatzprozesse könnten Sie sich bedienen?
- Stehen Ihnen Hilfsmittel wie Batterien und Lampen bereit?
- Haben Sie ein Warenverzeichnis in Papier?
- Haben Sie Wartungsverträge oder spezielle Vereinbarungen mit externen Dienstleistern?
- Haben Sie eine Möglichkeit stromgesteuerte Systeme zu umgehen?
- Haben Sie interne oder externe Ausweichmöglichkeiten?
- Haben Sie Verhaltensregeln für das Apothekenpersonal?
- Haben Sie eine Beschreibung der eingesetzten Komponenten?
- Haben Sie Alarmierungspläne?

- Brauchen Sie spezielle Personen im Notfall und spezifische Kompetenzen?
- Wohin wenden Sie sich, wenn es zu einem Angriff gekommen ist?
- Überlegungen dahingehend, wie Sie mit Ransomware Angriffen umgehen. Besteht die Bereitschaft Lösegeld zu zahlen und wenn ja, lässt sich das auch umsetzen?

Rund um das Thema Notfall- und Katastrophenmanagement lässt sich viel schreiben. Dieses Kapitel soll Ihnen einen Anreiz geben, um sich mit dem Thema intensiver auseinanderzusetzen. Wir empfehlen, sich dazu weiterführend zu informieren.

Allgemeine Informationen zum Notfallmanagement stellt das Bundesamt für Sicherheit in der Informations-technik (BSI) in einem Standard bereit: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=1 (31.01.2024)

Lesen Sie dazu auch die Seiten des Bundesministeriums für Inneres zum Krisen – und Katastrophenschutz (https://www.bmi.gv.at/204/start.aspx 31.01.2024) bzw. die Seiten des österreichischen digitalen Amtes: https://www.oesterreich.gv.at/themen/gesundheit_und_notfaelle/katastrophenfaelle.html (31.01.2024)

Die Österreichische Apothekerkammer hat ein Krisenvorsorgekonzept für Apothekenbetriebe entwickelt. Informieren Sie sich über das Projekt auf der Apothekerkammer-Homepage.
https://www.apothekerkammer.at/fileadmin/Bundeslaender/Steiermark/Krisen_-_Blackout/20201108_Krisenvorsorge_Morawetz.pdf

5. Elektronische Kommunikation in der Apotheke

Surfen im Internet, E-Mails empfangen und versenden, Chatten, Social Network und vieles mehr zeichnet die elektronische Welt, ohne die wir nicht mehr auskommen möchten, aus.

Absolute Sicherheit in der virtuellen Welt ist nicht möglich. Wenn Sie aber einige Grundverhaltensregeln einhalten, wird es all jenen, die versuchen unbefugt an Ihre Informationen zu gelangen, erschwert diese zu bekommen. Auf den nachfolgenden Seiten sind

wertvolle Informationen und Tipps für Sie zusammengefasst.

Internet

Das Internet ist das größte offene Computernetzwerk der Welt; hat eine globale Verbreitung und bietet eine Fülle von digitalen Informationen, die sich mit erstaunlicher Geschwindigkeit ändern und verbreiten. Das Internet ist eine Kommunikationstechnologie, die unser Leben beeinflusst und aus unserem Alltag nicht mehr wegzudenken ist. Vor 33 Jahren (06.08.1991) ging die erste Website online und heute besteht das WWW aus rund 1,1 Milliarden Internetseiten. Eine Website ist ein Ort, an dem ein Betreiber Inhalte hostet mit denen andere Personen interagieren. Jede Interaktion mit einer Website wird über das Internet übertragen.

Browser sind die Grundlage einer jeden Suchanfrage im Internet. Pflegen Sie deshalb Ihre Browserdaten! Löschen Sie regelmäßig den Internetverlauf, die temporären Internetdaten, sowie im Browser gespeicherte Kennwörter und Cookies. Welche Informationen der eigene Browser übermittelt, kann unter der URL https://coveryourtracks.eff.org (31.01.2024) überprüft werden.

Das Internet ist auch der größte Bazar der Welt. Es gibt nichts, was Sie im Internet nicht finden. Aber achten Sie darauf, dass Sie keine Urheberrechte verletzen. Oft bewegt man sich in einer gesetzlichen Grauzone, wie etwa beim Streamen[16] von Musik. Prüfen und hinterfragen Sie jedes Angebot im Internet und überlegen Sie, welche Dienste Sie über das Internet wirklich nutzen wollen. Viele angebotene Dienste sind einfach zu handhaben und kosten auch kein Geld, aber die Währung ist meist jede Menge Daten! Grundsätzlich sollten immer nur Mindestangaben, die für den jeweiligen Dienst notwendig sind, gemacht werden.

[16] Streamen: Während dem Vorladen der Datei kann man sie schon abspielen und nach Beendigung des Browsers ist die Datei nicht mehr auf Ihrem Rechner.

Verwenden Sie Pseudonyme (Nick Name) dort, wo keine Urkunden unterfertigt werden müssen. Online werden, außer bei der digitalen Signatur, niemals Verträge geschlossen, sondern bloß Willenserklärungen zum Abschluss eines Vertrages abgegeben.
Sobald Sie sich mit dem Internet verbinden, sind Sie Gefahren ausgesetzt. Es gibt keine Privatsphäre im Internet und es ist bei weitem nicht so anonym, wie Sie vielleicht glauben!

Wenn Sie im Internet recherchieren, einkaufen oder einen Flug buchen wollen, werden **Cookies** verwendet.

Cookies sind kleine Dateien, die auf dem PC gespeichert werden. Sie enthalten die Ad-

resse der Website und Identitätscodes, aber keine persönlichen Daten und sind normalerweise nützlich. Die Idee hinter einem Cookie ist, das Interneterlebnis für die Benutzer zu verbessern (z.B. bestimmte Angaben müssen nicht mehr gemacht werden und sind schon vorbelegt) und war ursprünglich als etwas Positives gedacht.

Sie können aber auch zur Datensammlung missbraucht werden und benötigen viel Speicherplatz, deshalb sollte man sie von Zeit zu Zeit auch löschen.

Das **Domain Name System (DNS)** ist das **Adressbuch des Internets**. Sobald ein Benutzer eine Anfrage an eine Website stellt, fragt der Browser einen DNS-Resolver nach der IP-Adresse der angefragten Seite. Diese Anfragen sind meist ungeschützt und so können die angesteuerten Webseiten und Domains einfach manipuliert und nachverfolgt werden. Die Angriff Szenarien rund um das DNS-Thema bezeichnet man als Spoofing: In der DNS-Namensauflösung wird die IP-Adresse der Ziel-Domain manipuliert und das Endgerät greift auf eine gefälschte IP-Adresse zu. So kann das Endgerät mit Malware infiziert werden und auf vertrauliche Daten zugegriffen werden.

Internetkriminalität ist im Vormarsch. Eine KPMG[17] -Studie hat aufgezeigt, dass bereits 60% der österreichischen Unternehmen mittlerweile Opfer eines Cyberangriffs gewesen sind. Malware und Phishing sind die häufigsten Angriffsarten. Aber jedes System ist nur so sicher, wie sein schwächstes Glied und es werden menschliche Schwächen ausgenutzt, um an vertrauliche Daten zu gelangen. Diese Methode ist als Social Hacking oder Social Engineering bekannt. Das Eindringen in ein Computernetz ist nicht offensichtlich und wird auch oft nicht gleich bemerkt. Wird ein ungeschützter PC an das Internet angeschlossen, ist er im schlechtesten Fall in wenigen Minuten mit Malware infiziert! Je stärker die Welt vernetzt ist, desto größer ist die Gefahr Ziel von Cyberattacken zu werden.

[17] KPMG Austria GmbH; Wirtschaftsprüfungs- und Steuerberatungsgesellschaft https://kpmg.com/at/de/home/insights/2023/05/cybersecurity-studie-2023.html (31.01.2024)

Es gibt viele Wege die Sicherheit im Internet zu erhöhen. Informieren Sie sich gut und lassen Sie sich von Fachpersonal beraten!

Wichtig ist, dass der eingehende und ausgehende Datenverkehr im Netzwerk gut überwacht wird, damit Cyberkriminalität keine Chance hat.

Übertragungsprotokolle und Verschlüsselung

Um sich vor Cyberkriminalität zu schützen, sollte man grundsätzlich vermeiden, private bzw. persönliche Daten im Internet zu verbreiten. Vertrauenswürdige Seiten erkennt man durch https://, dem obligaten Schloss-Symbol oder dem digitalen Zertifikat. SSL ist ein Verschlüsselungsprotokoll für die sichere Datenübertragung.
Jeder Webbrowser kommuniziert mittels eines **Übertragungsprotokolls**[18] mit dem Webserver.

[18] Übertragungsprotokoll: Legt die Regeln für eine Übertragung zwischen zwei Geräten fest.

- **http:** ungesicherte Übertragungstechnik
- **https:** gesicherte Übertragungstechnik

Der sichere https-Standard hat sich heute durchgesetzt. Die verschlüsselte Verbindung zwischen Webserver und Browser mit Hilfe von SSL/TLS Zertifikation ist nicht mehr wegzudenken. Diese Entwicklung ist eine der größten Veränderungen der Sicherheit in den letzten 30 Jahren und ein Beispiel dafür, wie Schwachstellen aus den Anfangszeiten nachhaltig behoben werden konnten.

Verschlüsselung ist ein Verfahren, welches aus einem Klartext mittels eines Schlüssels und eines kryptographischen Verfahrens einen verschlüsselten Text erzeugt.
Bei asymmetrischen Verfahren müssen diese zwei Schlüssel unterschiedlich sein. Dieses hat sich unter dem Namen Public-Key-Verfahren durchgesetzt. Es beruht auf einem Schlüsselpaar, das sich in einen öffentlichen und einen privaten Schlüssel teilt. Verschlüsselte Daten können nur vom Empfänger, der den passenden Schlüssel zur Entschlüsselung hat, entschlüsselt werden.

Digitale Zertifikate sind digitale Ausweise im Internet. Sie bestätigen, dass eine bestimmte Person oder Organisation eine bestimmte Signatur (privaten Schlüssel) benutzt. Sie werden von Zertifizierungsstellen, die eine Identitätsprüfung der Person durchführen und sicherstellen, dass der Unterzeichner den privaten Schlüssel korrekt verwendet, ausgegeben.

QR-Codes

Nun kennen wir alle die **Barcodes**, welche sich auf der Verpackung eines nahezu jeden Produktes befinden, das man kaufen kann. Ein solcher Barcode, auch Strichcode genannt, enthält parallele Striche unterschiedlicher Breite. Darin verschlüsselt sind Information, also Daten, die durch optische Lesegeräte wie Scanner entschlüsselt und in Klartext übertragen werden können. Bis hierher also nichts Neues, denn Sie alle kennen diese Codes von den Arzneimittelverpackungen, die Sie tagtäglich über ihr Kassensystem abscannen.

Ein anderer Typ des 2D-Codes, der **Quick Response-Code (QR)** ist längst zu einem alltäglichen und bequemen Kommunikationsmittel geworden. Die Eigenschaften der Codes machen sie typisch für die Digitalisierung. Und die Entwicklung geht immer weiter, denn nicht nur Zahlen lassen sich als Information hinterlegen. Mit den Codes können im Gesundheitswesen Patienten- und Verordnungsdaten verschlüsselt abgefragt werden.

Der **QR-Code** (Quick-Response-Code) ist ein maschinenlesbarer Code, der aus einer quadratischen Matrix, die mit kleinen schwarzen und weißen Quadraten gefüllt ist, besteht. Diese Quadrate können mit QR-Code-Generatoren leicht erstellt werden und dienen zur Codierung von Informationen wie Webseiten-URLs, E-Mail-Kontaktinformationen oder anderen Datentypen. Die kodierten Daten werden binär dargestellt. Auffällig beim QR-Code ist die spezielle Markierung in drei der vier Ecken des Quadrats. Diese drei Kästchen dienen der Orientierung, da sich das Lesegerät oder die Kamera anhand des fehlenden Musters in der vierten Ecke orientieren kann und somit weiß, wo oben und unten ist. Der QR-Code gilt als besonders benutzerfreundlich, weil er Daten durch einen fehlerkorrigierenden Code ergänzt. Hierdurch kann der Verlust von bis zu 30 Prozent der Daten, zum Beispiel bei schlechtem Druckbild, ausgeglichen und der Code auch dann noch entschlüsselt werden. Aufgrund der hohen Fehlertoleranz ist der QR-Code beim Endverbraucher-Marketing das Mittel der Wahl. Es können Markenlogos oder Bild- und Farbveränderungen spielerisch in den Code integriert werden.

ABER VORSICHT! QR-Codes können von Menschen nur schwer interpretiert werden, was es Cyber-Angreifern erleichtert, Informationen zu verschlüsseln, die bösartig sind oder Schaden anrichten können. Ein QR-Code kann Sie beispielsweise auf eine bösartige Webseite leiten, die versucht, Ihre persönlichen Daten wie Passwörter oder Kreditkartennummern abzufangen bzw. versucht Malware auf Ihrem Gerät zu installieren. Der QR-Code selbst ist nicht die Bedrohung, wohl aber die Informationen oder Aktionen, die er auslöst.

Künstliche Intelligenz

Künstliche Intelligenz bezeichnet Systeme mit „intelligentem" Verhalten, die Ihre Umgebung analysieren und zu einem gewissen Grad autonom handeln. KI-basierte Systeme sind etwa Sprachassistenten, Bildanalysesoftware, Suchmaschinen oder Sprach- und Gesichtserkennungssysteme. KI-Systeme sind Softwareprogramme, die die Funktionsweise des menschlichen Gehirns nachahmen. Suchmaschinen schaffen über KI-Algorithmen Ordnung in das unstrukturierte Informationschaos im Internet. Künstliche Intelligenz ist hervorragend geeignet, um kognitive Fähigkeiten zu erlernen, aber koordinatorische und sensomotorische Fähigkeiten fehlen.

Machine Learning ist ein Teilgebiet der künstlichen Intelligenz und entwickelt das künstliche Wissen aus Erfahrung. Sein Herzstück sind Algorithmen und die Fähigkeit große Mengen an strukturierten Daten zu verarbeiten und miteinander zu verknüpfen. Machine Learning wird in der IT-Sicherheit, im Gesundheitswesen, bei der Wettervorhersage, in der Verwaltung, im Verkehr und der Mobilität, im Marketing und vielen anderen Bereichen eingesetzt.

Chat GPT ist eine innovative KI-Plattform, die natürliche Sprache versteht und Textantworten generieren kann. ChatGPT basiert auf einem OpenAI Modell, und dieses Modell wurde auf riesige Mengen an Textdateien aus dem Intranet trainiert. Die Informationen, die ChatGPT verwendet, stammen aus diesen Textdateien.

ChatGPT ist ein Online-Chatbot mit KI und eine der ersten öffentlich verfügbaren Lösungen, die in der Lage ist, wie ein echter Mensch zu agieren und den sogenannten Turing-Test bestanden hat. Bei diesem Test wird die Fähigkeit einer Maschine, intelligentes

Verhalten zu zeigen, ermittelt, indem ein echter Mensch mit der Maschine über einen textbasierten Chat-Kanal interagiert. Wenn der Mensch nicht unterscheiden kann, ob er mit einer Maschine oder einem Menschen interagiert, hat die Maschine den Test bestanden. Onlineunterhaltungen sind jedoch nur der Anfang dessen, was KI leisten kann. Inzwischen gibt es KI-Lösungen, die ein Video von einer Person erstellen können, die eine Klasse in einer beliebigen Sprache unterrichtet, die Gesundheitsdaten analysieren und schnell feststellen können, wer höchstwahrscheinlich an Krebs erkrankt ist, die Nachrichtenartikel oder Aufsätze zu einem Thema ihrer Wahl erstellen, Bilder für Kinderbücher generieren oder Codes für neue Computerprogramme erstellen.[19]

[19] https://www.sans.org/newsletters/ouch/

Auch wenn KI nicht unbedingt etwas ist, das man fürchten muss, gibt es doch einige Gefahren, derer man sich bewusst sein sollte. Achten Sie auf Deep Fakes, falsche Informationen und auf Ihre Privatsphäre. Geben Sie keine Daten in ChatGPT ein, die Sie als sensibel, persönlich oder vertraulich betrachten. Ja, wir sind in der Science-Fiction-Welt angekommen.

Unter **Internet der Dinge (IoT)** versteht man „smarte", also intelligente Geräte wie beispielsweise Kameras, Beleuchtungen oder Lautsprecher, welche über das Internet mit einem Server des Herstellers verbunden und dann meist über eine App am Smartphone zugänglich gemacht werden. Da diese Geräte häufig ein großes Sicherheitsrisiko für Ihr Netzwerk darstellen, sollten Sie diese idealerweise in einem separaten Netzwerk betreiben und vom Netzwerk der Warenwirtschaft trennen

Tipps zur Internetnutzung

- Vertrauliche oder persönliche Daten sollten ausschließlich über verschlüsselte Seiten bekannt gegeben werden. Die Übertragung ist sicherer, wenn die Internetadresse in der Browserleiste mit https:// beginnt.
- Nutzen Sie die sicheren Browsereinstellungen: Abschalten von Cookie-Diensten bzw. nur Cookies akzeptieren, die vom selben Server kommen wie die Website.
- Löschen Sie (in den Internetoptionen) Cookies, Dateien und den Internetverlauf, um so die Spuren, die beim täglichen Surfen entstehen, zu vernichten.
- Aktivierung von Blocking-Diensten: Moderne Browser bieten Pop-Up-Blocker[20] oder Phishing-Site-Blocker an.
- Aktivierung von Privacy-Profilen: Der sogenannte P3P[21] Standard prüft automatisiert, ob die Datenschutzerklärung der Website mit den Datenschutzerwartungen des Internetbenutzers übereinstimmt.
- Reduktion von Plug-ins[22]: Überprüfen Sie, ob Sie wirklich alle Plug-ins brauchen (Flash Player, Adobe Reader, Shockwave Player, etc.).
- Überprüfen Sie regelmäßig Kreditkarten- und/oder Bankkonto Auszüge.
- Vorsicht beim Verbinden mit einem ungeschützten WLAN!

[20] Popup Fenster sind Browserfenster, die sich ohne Ihre Erlaubnis öffnen, meist um damit Werbung zu betreiben. Manche Browser enthalten Popup-Blocker. Werden Popups komplett blockiert funktionieren allerdings manche Webseiten, wie zum Beispiel e-Banking, nicht mehr.

[21] P3P ist eine technische Plattform zum Austausch von Datenschutzinformationen.

[22] Sie können den Funktionsumfang von Browsern mit Plug-ins erweitern. Das sind Zusatzprogramme, die sich in den Browser einklinken und zusätzliche Funktionen liefern.

- Achten Sie auf die Verschlüsselung im Web, besonders bei kritischen Vorgängen!
- Achtung auf gefälschte Webshops. Seien Sie misstrauisch bei Werbeanzeigen oder Sonderangeboten, die zu gut klingen, um wahr zu sein.
- Scannen Sie QR-Codes nur von vertrauenswürdigen Quellen und nehmen Sie sich Zeit die Aufforderung zum Handeln oder den Link zu prüfen.
- Überlegen Sie es sich zweimal, bevor Sie vertrauliche oder persönliche Daten auf einer Webseite eingeben, die Sie über einen QR-Code aufgerufen haben.

E-Mail

Die elektronische Post ist der Weg, über den die geschäftliche Kommunikation zwischen Unternehmen und Kund*innen läuft. Auch im Austausch zwischen der Apotheke und der Pharmazeutischen Gehaltskasse ist E-Mail ein Medium zur Informationsweitergabe. E-Mail bietet nur wenige Möglichkeiten die Privatsphäre zu schützen. Ihre E-Mail kann von jedem gelesen werden der Zugang zu ihr hat bzw. dann auch an Dritte weitergeleitet werden.

Wenn Sie mehrere **E-Mailadressen** verwenden, sollten Sie unterschiedliche Benutzernamen und Passwörter verwenden. So können Sie nicht so leicht rückverfolgt werden. Mehrere E-Mailadressen lassen sich auch auf einem Programm gemeinsam verwalten, so brauchen Sie nicht auf jeden Account extra zugreifen.

Benutzen Sie keine E-Mailadresse mit mehreren Personen gemeinsam, außer es ist so von Ihnen gewünscht!

Jeder kann in Ihrem Namen eine E-Mail an andere Personen weiterleiten. Auch E-Mails unterliegen dem Briefgeheimnis.

E-Mail Adressfelder:

- Verwenden Sie **An**, wenn Ihre E-Mail nur einen Adressaten hat oder die Empfänger einer E-Mail allen anderen bekannt sind. Die Einträge im An-Feld werden bei allen Adressaten angezeigt.
- Verwenden Sie **Cc** (Carbon Copy), wenn Sie Kopien an einen oder mehrere Empfänger schicken wollen. Adressaten, die im Cc-Feld stehen, wissen, wer der Hauptempfänger ist und wer lediglich eine Kopie bekommen hat.
- Verwenden Sie **Bcc** (Blind Carbon Copy) immer, wenn sich einige oder gar alle Adressaten nicht kennen. Alle, die in Bcc stehen, erscheinen in der E-Mail nicht als Empfänger. So werden Sie nicht zum Adressenlieferanten.

Tipps zum E-Mailverkehr

- Klicken Sie keine Links in Mails an, von denen Sie nicht wissen, wo sie hinführen!
- Geben Sie unter keinen Umständen Kennwörter, Kreditkartennummern oder persönliche Daten auf einer Website ein, wenn Sie vorher auf einen Link in einem Mail geklickt haben.
- Die Pharmazeutische Gehaltskasse schickt Ihnen nie E-Mails, in denen Sie aufgefordert werden, persönliche Daten bekannt zu geben! Fragen Sie bei uns nach, wenn Sie ungewöhnliche Nachrichten von uns erhalten.
- Kein Internetanbieter pflegt Kundenkontakt über Instant Message und keiner fragt mittels Mail nach persönlichen Daten.
- Erweckt die Nachricht ein starkes Gefühl der Dringlichkeit oder klingt die Botschaft zu gut, um wahr zu sein, dann seien Sie vorsichtig.
- Öffnen Sie keine ZIP oder RAR Datei in E-Mails, wenn Sie den Absender nicht kennen. Hier können sich ganze Schadprogramme verstecken. Diese Dateien sind komprimiert und auf eine spezielle Art codiert, deshalb brauchen sie wenig Platz und können nur mit dem entsprechenden Programm wieder decodiert werden.
- Versenden Sie keine sensiblen Daten unverschlüsselt per Mail!
- Die Autovervollständigung von E-Mail-Empfängern ist eine gängige Funktion. Überprüfen Sie immer den Namen und die E-Mail-Adresse bevor Sie auf Senden klicken.
- Vorsicht bei der Weitergabe der E-Mailadresse oder bei der Eintragung der Daten in Internetformulare. Man sollte immer davon ausgehen, dass die Daten missbräuchlich verwendet werden könnten.
- Öffnen Sie keine Mails, Anhänge und Programme, wenn Sie den Absender nicht kennen bzw. die Mails Inhalte enthalten, die Sie niemals von dem Absender erwarten würden (z.B. schickt Ihnen kein Geschäftspartner Urlaubsfotos).
- Werden Sie als Apotheker*in nicht zum Spamer! Bedenken Sie, dass die Versendung von Massenmails, ohne Einwilligung der Empfänger, laut Telekommunikationsgesetz (TKG) verboten ist.

Videotelefonie und Chat

Für **Videotelefonie** braucht man eigentlich nur eine Internetverbindung, eine Webcam und ein Mikrofon, wobei beides in den meisten Laptops oder Monitoren bereits integriert ist, und eine Software, welche Videotelefonie zur Verfügung stellt. Im Vergleich zu einem herkömmlichen Telefongespräch mittels Mobiltelefons oder Smartphone bietet die Videotelefonie über den Computer einen großen Vorteil: Es ist eine günstige Variante.

Videokonferenzen waren besonders in Pandemiezeiten eine gute Möglichkeit, um mit den Kund*innen „persönliche" Kontakte zu pflegen. Zoom, GoTo-Meeting, MS Teams und viele andere technische Tools können hier genannt werden. Beachten Sie dabei aber immer den Faktor Datenschutz. Sorgen Sie dafür, dass bei Übertragung von Ton- und Bild keine Privaträumlichkeiten bzw. andere Personen zu sehen sind und eine Aufzeichnung des Gesprächs nur mit Einwilligung aller Beteiligten möglich ist.
Über Instant Messaging oder Chat können sich zwei oder mehr Teilnehmer*innen per Textnachrichten unterhalten.

Chatten ist das Plaudern im Internet oder die Interaktion mit einem Online-Chatbot. Der Online-Chat ist meist öffentlich, man braucht dazu nur einen Chatnamen. Es gibt auch private Chatrooms.

Web 2.0

Web 2.0 bietet eine Möglichkeit der zwischenmenschlichen Kommunikation und des Austausches von Inhalten auf Webseiten. Der Inhalt wird von Benutzern generiert (z.B. Wikis, Blogs). Social Media und Social Networks sind die Online-Kommunikationskanäle des Web 2.0.

Bei **Social Media** geht es darum, dass jedem ermöglicht wird, Inhalte zu erstellen, zu verbreiten und teilweise auch zu bewerten. Die bekanntesten Social Media Plattformen sind Wikipedia und Twitter (X).

Ein Twitter Blog ist ein Online geführtes Tagebuch, das es ermöglicht, Nachrichten, von wo auch immer, so oft wie möglich zu aktualisieren. Das Twitter Konto ist öffentlich.
Der soziale Teil des Web 2.0 ist **Social Network**. In erster Linie dienen sie der Vernetzung der Nutzer*innen und erfreuen sich großer Beliebtheit. Es gibt eine Vielzahl von Plattformen für Businesskontakte, Singles, Musik und zum „Freunde" finden (z.B. Facebook, Netlog, MySpace, StayFriends, Xing, LinkedIn).

Beachten Sie dabei aber immer die Sicherheitsaspekte und prüfen Sie die **Sicherheitseinstellungen**.

Das Web vergisst nie! Alles, was man bereit ist zu zeigen, kann auch nach Entfernung schwer bis nie ganz gelöscht werden!

Social Media-Auftritte verlangen ein großes Engagement. Nichts ist schlimmer als veraltete Auftritte. Kommunizieren Sie daher regelmäßig und reagieren Sie auf Fragen, Beiträge, Kommentare und Kritik. Wenn Sie sich dafür entscheiden über Social Network Portale präsent zu sein, ist es gut, sich vorher zu überlegen, welches Ziel Sie damit verfolgen wollen. Die Auftritte sollten als Privatperson und besonders als Firma kritisch hinterfragt werden.

Treffen Sie Vereinbarungen mit Ihren Mitarbeiter*innen über die Nutzung von Social Network in der Arbeitszeit. Klären Sie die Mitarbeiter*innen auf, welche Informationen über das Unternehmen nach außen kommuniziert werden dürfen und welche nicht.
Es gibt auch Möglichkeiten Ihre Aktivitäten auf Social Network Portalen auszuspionieren, immer mit dem Ziel an Benutzerdaten zu kommen.

Eigene Homepage

Immer mehr Menschen nutzen die Möglichkeit, Waren online zu kaufen. Dies wird nicht mehr ausschließlich gemacht, um Kosten zu sparen, sondern vor allem aus Bequemlichkeit.

Kund*innen informieren sich heute online und verzichten möglicherweise auf einen Einkauf im Netz, wenn auch die lokale Apotheke das Produkt anbietet. Dazu müssen Kund*innen, die im Internet oder auch in Zeitschriften oder TV auf ein passendes Präparat stoßen, Ihre Apotheke auch finden. Genauso wie Sie in der analogen Welt auf Ihre Apotheke aufmerksam machen (sichtbares Apotheken-A, auffälliges Logo, ein schön dekoriertes Schaufenster, Flyer, Anzeigen, usw.) sollten Sie dies daher auch in der digitalen Welt tun. Neben der Pflege der Informationen in Google sollten Sie auch Ihre Homepage und vor allem Ihr **digitales Schaufenster** pflegen. Vorteilhaft für den Verbraucher ist dabei, dass er das Präparat sofort vor Ort einfach abholen kann. Sollte ein Artikel bestellt werden müssen, so liegt er wenige Stunden später in der Apotheke bereit und der/die Kund*in muss kein zweites Mal kommen. Ergänzt wird dieses regionale Angebot durch Botendienste der Apotheke. In Zukunft vielleicht sogar über eine Lieferdrohne.

Wenn Sie Ihre **Apotheke im Internet** präsentieren möchten, müssen Sie sich erst einmal entscheiden, ob Sie Ihre Website selbst erstellen, oder ob Sie jemanden dafür engagieren wollen.

Unabhängig von dieser Entscheidung benötigen Sie für Ihre eigene Website einen Webserver und einen Domänennamen. Eine Domain können Sie beim zuständigen Registrar anmelden und mit der IP-Adresse des dazugehörigen Servers verknüpfen. Für Österreich ist als Registrar NIC (Network Information Center) zuständig.

Wenn Sie wissen wollen, wer der Inhaber einer Domäne ist, dann können Sie zum Beispiel auf den Webseiten www.nic.at oder www.whois.net nachschauen. Achten Sie darauf, dass Ihre Seiten gut abgesichert sind und dass Sie die Möglichkeit haben die Inhalte jederzeit zu verändern.

Das **E-Commerce Gesetz, das Mediengesetz bzw. die Datenschutzgesetze** sind relevant, wenn Sie Ihre Apotheke im Internet präsentieren oder einen Online-Shop betreiben wollen.

Aus den Datenschutzgesetzen ergibt sich für alle Betreiber einer Homepage, dass Datenschutzhinweise bzw. eine Datenschutzerklärung auf der Homepage zu finden sein muss. In der Erklärung muss sich der Hinweis befinden, dass grundsätzlich personenbezogene Daten erhoben werden und welche Daten es betrifft. Auf nahezu jeder Website agieren Server-Logfiles, welche die IP-Adresse der Nutzer, Zeitpunkt und Verweildauer auf der Homepage anzeigen. Weiterhin werden meisten Cookies gesetzt. Server-Logfiles und Cookies müssen in der Datenschutzerklärung erwähnt werden.

Jede Homepage verlangt nach einem Cookies Banner zum Einholen der Einwilligung zur Cookie Nutzung bei den Besuchern der Website. Das ist notwendig, wenn auf der Website Dienste von Drittanbietern eingebunden sind, die Reichweitenmessungen durchführen und Nutzerverhalten auf der Webseite analysieren. Seien Sie vorsichtig beim Einsatz von Google Analytics. Mittlerweile gibt es gute europäische Alternativen.
Wertvolle Informationen zum Betreiben der eigenen Website und den damit verbundenen rechtlichen Anforderungen finden sie auf Österreichs digitalem Amt.

Bezahlsysteme und elektronische Bankgeschäfte

Die beliebteste Form im Internet zu bezahlen, ist die Kreditkarte. Wir empfehlen die Kreditkartennummer nur bekannt zu geben, wenn zur Verschlüsselung ein digitales Zertifikat verwendet wird. Das Zertifikat zeigt Ihnen an, wer der Betreiber des Servers ist und wo der Standort desselben ist.

Bei elektronischen **Zahlungssystemen** oder E-Wallet (Online-Geldbörsen), wie etwa PayPal und dergleichen, wird die Möglichkeit gegeben Geld auf einfache Weise zwischen Konten und unterschiedlichen Banken zu transferieren. Diese sind eine sichere Option für Online-Einkäufe, da die eigene Kontonummer bzw. Kreditkartennummer anonym bleiben. Achten Sie darauf, dass das Geld auch wieder rückbuchbar ist. Solche Dienste sind für gewöhnlich kostenpflichtig.

Meiden Sie Webseiten, die nur Zahlungen in Kryptowährungen (Bitcoin) akzeptieren oder andere, obskure Zahlungsmethoden verlangen.

Sofortüberweisung ist ein Direktüberweisungsverfahren, bei dem zwischen dem Buchungssystem des Anbieters und dem Online-Bankkonto eine Schnittstelle bereitgestellt wird.

Mobiles Bezahlen mit dem Handy oder anderen mobilen Geräten bzw. auch mit Smartcards, ist das sogenannte kontaktlose Bezahlen. Hier wird ein Chip in die Kreditkarte oder das Handy eingelassen und über ein Lesegerät gehalten, wobei eine hochsichere Verbindung aufgebaut wird.

Die Abwicklung von **Bankgeschäften** über Datenleitungen (Online-Banking) oder über Telefonverbindungen (Telebanking) mit Hilfe von PC, Smartphone oder anderen elektronischen Endgeräten, wird häufig genutzt. Machen Sie Ihre Bankgeschäfte nur über gut abgesicherte Endgeräte (Virenschutz und Firewall) und nie von einem öffentlichen Hotspot[23] aus. Der Zugriff ist nur mit persönlicher Identifikation (PIN) möglich und die Übertragung wird verschlüsselt (TAN-Nummer). PIN und TAN (auch E-TAN) sollte nie für Dritte zugänglich sein.

[23] WLAN-Hotspot ist ein ungesichertes Internet, das nur zum Surfen verwendet werden soll.

Mobiles Banking über das Smartphone ist im Vormarsch. Fast jede Bank bietet für ein zeit- und ortsunabhängiges Internet-Banking eine entsprechende App an. Wenn Sie allerdings Schadsoftware auf Ihrem mobilen Gerät haben, können die Daten ausspioniert werden. Beim pushTAN-Verfahren führen Sie die Auftragsfreigabe direkt auf Ihrem Smartphone oder Tablet in einer speziellen App durch. Es kann von einem einzigen Gerät aus sicher auf Online-Banking zugegriffen und Aufträge freigegeben werden. Ein zusätzliches Gerät ist nicht nötig.

6. Digitale Dienste

2024

Zunehmend werden digitale Dienste bereitgestellt. Im Gesundheitsbereich ist die Digitalisierung auch angekommen. Viele Services sind heute online möglich, wie Steuererklärung auf elektronischem Weg, Melden eines Gewerbes bei der Behörde, die Anmeldungen zur Sozialversicherung, die Zulassung eines KFZ, usw. Wer sich die App „Digitales Amt" im App Store herunterlädt und sich mit der ID Austria anmeldet, kann eine Vielzahl von Bürgerservices nutzen und seine Amtswege rund um die Uhr online erledigen. Eine virtuelle Anlaufstelle bietet das Portal „österreich.gv.at".

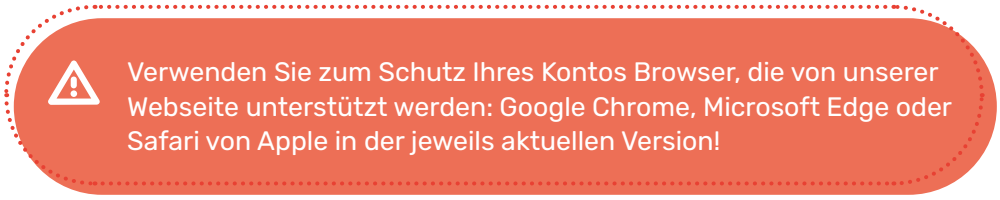
Riesige Datenmengen unterschiedlicher Herkunft, Qualität und Größenordnung sind es, die in der **Digitalisierung des Gesundheitswesens** eine Gesamtschau ermöglichen. Medizinische Daten von Laborbefunden, Bilddaten, Daten aus Krankheitsverläufen, Mobile-Health Daten von diversen Gesundheits-Apps, Patienten Communities, Social Media Daten, Versicherungsdaten, Diagnostikdaten, Medikationen, usw. bilden BIG Data im Gesundheitswesen. Wie alles im Leben haben auch Daten zwei Seiten, sobald sie genutzt werden. Die Digitalisierung im Gesundheitswesen bietet viele Chancen und Digital Health stiftet Nutzen. Die wertvollen Datensätze sind aber auch für Hacker sehr interessant.

In der Pharmazeutischen Gehaltskasse steht das Thema Digitalisierung ebenso im Zentrum unserer Entwicklungen und wir arbeiten intensiv daran, unsere Services noch mitgliederfreundlicher, schneller und effizienter zu gestalten. Informationssicherheit und Datenschutz sind uns dabei ein großes Anliegen. Informieren Sie sich auf den nachfolgenden Seiten über unsere Services und weitere digitale Dienste mit denen Sie als Apotheker*in konfrontiert sind.

Homepage der Gehaltskasse

Die Homepage der Gehaltskasse spiegelt die Aufgaben und das Selbstverständnis der Pharmazeutischen Gehaltskasse wider und fungiert als Informationsdrehscheibe für allgemeine, persönliche und betriebliche Informationen.

Durch die einfache und bequeme Handhabung, sowie die ständige Erreichbarkeit auf verschiedenen Endgeräten erleichtern wir Ihnen die organisatorischen Abläufe innerhalb des digitalen e-Service Portals - **dem digitalen Tor zu unseren Mitgliedern**. Besonderes Augenmerk haben wir auf die Aspekte des Datenschutzes und der Datensicherheit gelegt.



Eine durchgängige digitale Kommunikation der Mitglieder mit der Gehaltskasse ist uns ein Anliegen und das Thema Digitalisierung wird auch 2024 einen Schwerpunkt bilden. Für die Homepage wurde bereits eine neue technische Basis geschaffen und so können wir auf Wünsche unserer Mitglieder noch rascher reagieren und Verbesserungen im Bereich des e-Service Portals und der e-Formulare umsetzen. Besonders auf die neuen Features in der Zustellbox und auf die neuen Rechner möchten wir hinweisen. Damit ermöglichen wir Ihnen eine intuitive Bedienung, einen besonders benutzerfreundlichen Look und eine optimierte Ausrichtung für mobile Endgeräte.

Die Digitalisierung darf aber nie zum Selbstzweck werden und jenseits aller technologischen Entwicklungen steht für uns immer das Mitglied im Zentrum.

e-Service Portal der Gehaltskasse

Das e-Service Portal ist die Plattform für die persönliche und betriebliche Kommunikation. Innerhalb von diesem geschützten Bereich stehen Ihnen je nach Rolle und Berechtigung folgende Anwendungen bzw. Bereiche zur Verfügung:

- Formulare und Anträge (An/Ab/Ummeldungen, Anträge für Vergütungen, Zuschüsse, usw.)
- Rundschreiben
- Sitzungsprotokolle für Vorstandsmitglieder und Delegierte
- Zustellbox für unsere Mitglieder
- Zustellbox für die Steuerberater*innen / Wirtschaftstreuhänder*innen unserer Mitglieder
- Zugang für Mitarbeiter*innen von Apothekenbetrieben
- Stammdaten der Mitglieder und Betriebe
- Stellensuche
- Upload Rezeptdaten
- Upload Sonderverrechnung
- Erteilung von Berechtigungen für Mitarbeiter*innen und Steuerberater*innen / Wirtschaftstreuhänder*innen durch die jeweilige Apothekenleiter*in
- Zugang für die Hersteller von Apothekensoftware

Die **Zustellbox** ist einfach und benutzerfreundlich gestaltet, bietet eine gute Navigation und ist für mobile Endgeräte optimiert. Innerhalb der e-Formulare wurde auf eine intuitive Bedienbarkeit geachtet. Dokumente werden nun auch länger als drei Monate angezeigt.

Für angestellte Apotheker*innen werden derzeit die eigenen Gehaltszettel hinterlegt, e-Formulare/Anträge, Stammdaten und Rundschreiben bereitgestellt bzw. für Funktionär*innen Protokolle.

In der Zustellbox der Betriebe finden Sie viele Dokumente, wie etwa Fakturen zur Rezeptabrechnung, Rohaufschlagsstatistik, Sondernachlass, Erfassungsbeitrag, Hochpreislisten, Überweisungen der Impfaktionen, DFÜ-Protokolle der Rezepteinreichung, die Vorschreibung und das Summenblatt der Gehaltszettel und viele mehr.

Wenn neue Schriftstücke in die Zustellbox einlangen, erhalten Sie ein Verständigungsmail. Sie können dieses Service jedoch auch ausschalten, in dem Sie in der Kachel „Stammdaten“ das „Hakerl“ entfernen. Grundlegende Voraussetzung, um auf das e-

Service Portal zuzugreifen, ist eine einmalige Verifizierung der e-Mailadresse zu Ihrem Profil. Nachdem die Verifikationsnachricht in Ihrem Posteingang angekommen ist, ist der Bestätigungslink innerhalb von 15 Minuten zu aktivieren.

e-Formulare werden sukzessive die Papierformulare ersetzen. Durch die elektronischen Formulare können wir die Servicequalität verbessern, da sie über Plausibilitätsprüfungen verfügen und mittels ID Austria unterzeichnet und verschlüsselt übermittelt werden. Speziell die e-Formulare für An/Ab/Ummeldungen erleichtern Ihnen den organisatorischen Aufwand in der Apotheke. Diese e-Formulare können auch von Ihrem Steuerberater / Wirtschaftstreuhänder initiiert werden.

Der Zugang für Steuerberater und Wirtschaftstreuhänder wurde eingerichtet, um den Apothekenbetrieben eine Weiterleitung von Papierdokumenten zu ersparen und somit die administrative Arbeit zu erleichtern. Es besteht die Möglichkeit Gehaltszettel, das Summenblatt und die Vorschreibung, Fakturen, Hochpreislisten und viele mehr anzeigen zu lassen. Die Berechtigungen vergibt aber ausschließlich die/der jeweilige Apothekenleiter*in.

Login und Berechtigungen im e-Service Portal

Je nach Rolle und Berechtigung können innerhalb des e-Service Portals unterschiedliche Bereiche geöffnet und Informationen eingesehen werden. Die Logindaten benötigen Sie auch für www.apothekerkammer.at und www.apofortbildung.at. Weitere Dienste werden folgen.

Um unsere Online-Services nutzen zu können, ist es nötig sich anzumelden. Sie können sich mit der ID Austria anmelden oder über Benutzername und Kennwort identifizieren. Hilfe dazu finden Sie unter diesem Link: https://gehaltskasse.at/hilfe-zum-login.

Es stehen folgende Zugänge zur Verfügung:

- Apotheker*innen - P-Nummer + Kennwort
  Die P-Nummer ist Ihre Personalnummer (z.B. P9999002)
- Mitarbeiter*innen von Apotheken – M-Nummer + Kennwort
  Die M-Nummer ist die fünfstellige Apothekenbetriebsnummer (z.B. M00123)
- Steuerberater*innen / Wirtschaftstreuhänder*innen – W-Nummer + Kennwort
  Die W-Nummer ist eine eigenständige Nummer (z.B. W0000999)
- Softwareanbieter – S-Nummer + Kennwort
  Die S-Nummer ist eine eigenständige Nummer (z.B. S0000123)

Der Zugang zum e-Service Portal für Apothekenbetriebe erfolgt zweigeteilt:

- Die Mitarbeiter*innen einer Apotheke können sich mit M-Nummer + Kennwort einloggen. Damit können sie Rezeptdaten hochladen und Rundschreiben der Gehaltskasse einsehen, sofern Apothekenleiter*innen die Berechtigung dazu vergeben.
- Apothekenleiter*innen können sich mit P-Nummer + Kennwort in das e-Service Portal einloggen und sehen damit die privaten und apothekenspezifischen Inhalte.

Bewahren Sie die Zugangsdaten gut auf und lassen Sie sie nicht frei in der Apotheke liegen, es handelt sich um wichtige **Zugangsdaten**. Wir empfehlen Ihnen vorzugsweise die ID Austria zur Anmeldung auf unser Serviceportal zu verwenden.

Loggen Sie sich, nach Beendigung Ihres Besuches immer aus dem e-Service Portal aus, damit kein Dritter mit Ihren Zugangsdaten arbeiten kann. Beachten Sie das auch für alle anderen Internet-Bereiche.

Hilfestellung zum Kennwortwechsel können sie der Rubrik „Häufig gestellte Fragen“ entnehmen.[24]

[24] https://www.gehaltskasse.at/h%C3%A4ufig-gestellte-fragen/-/categories/45776?p_r_p_resetCur=true&p_r_p_categoryId=45776 (31.01.2024)

Elektronische Rezeptverrechnung

Über das e-Service Portal auf unserer Homepage www.gehaltskasse.at haben Sie die Kachel „Upload Rezeptdaten“ über welche Sie die elektronische Rezeptdatei hochladen können. Davor ist es notwendig sich zu authentifizieren. Über den „Upload Sonderverrechnung“ können spezifische Dateien hochgeladen werden.

- Personen, die nicht Apothekenleiter*innen sind, loggen sich mit M-Nummer und Kennwort ein, um die Rezeptabrechnungsdaten an die Gehaltskasse zu übermitteln.
- Apothekenleiter*innen können sich mit ihrer P-Nummer oder vorzugsweise mit der ID Austria einloggen und haben damit Zugriff auf alle Daten der von Ihnen geleiteten Apotheke.
- Die Anbieter von Apothekensoftware können sich mit der eigenen S-Nummer und Kennwort einloggen, um Ihnen beim Upload der Daten zu helfen.

Für die Übertragung der Rezeptabrechnungsdatei (ZIP-Datei) laden Sie die Datei hoch und senden sie diese ab. Nach erfolgreichem Upload erhalten Sie die Meldung „Upload abgeschlossen“ und erhalten ein Übernahmeprotokoll in Ihre betriebliche Zustellbox. Hier finden Sie immer die aktuelle Anleitung https://www.gehaltskasse.at/upload-der-rezeptdaten.

Bei Fragen zur Homepage wenden Sie sich bitte an unser Mitgliederservice unter der Telefonnummer (01) 40414 – 222.

In der Apotheke verarbeiten und übertragen Sie im Rahmen der elektronischen Rezeptverrechnung gesundheitsbezogene und somit sensible Daten. Durch das Datenschutzgesetz besteht die Verpflichtung, Maßnahmen zur Gewährleistung der Datensicherheit zu treffen und den Sicherheitsstandard entsprechend hochzuhalten. Deshalb ist zwingend darauf zu achten, immer ein aktuelles Betriebssystem einzusetzen und auch den verwendeten Browser stets aktuell zu halten. Wir empfehlen Ihnen, sich bei Ihrem Softwarehaus bzw. Systembetreuer über den aktuellen Sicherheitsstandard zu informieren und notwendige Aktualisierungen vornehmen zu lassen.

Achten Sie auf die Sicherheit bei allen Datenverbindungen. Dazu gehört nicht nur die Rezeptdatenübertragung, sondern auch die Übertragung der Bestellung an den Großhandel bzw. die Fernwartung Ihrer Systeme durch den Systembetreuer. Achten Sie darauf, dass jede Datenverbindung von Ihnen aktiv gestartet oder bestätigt werden muss und auch von Ihnen abgebrochen werden kann.

e-Medikation

e-Medikation ist immer noch präsent in den Medien. Einige von Ihnen werden im Rahmen der Teilnahme an einem der Pilotprojekte schon Erfahrungen damit gesammelt haben. Sei es nun durch das 1. Pilotprojekt „Arzneimittel-Sicherheitsgurt", welches 2007 in Salzburger Apotheken im Einsatz war und von der Apothekerschaft organisiert wurde oder durch das Pilotprojekt „e-Medikation", das von April bis Dezember 2011 in drei Regionen Österreichs getestet wurde und über den Hauptverband der Sozialversicherungsträger (SVC) initiiert wurde. Die Teilnahme an e-Medikation war freiwillig und kostenlos.

Im Jänner 2013 trat das Gesundheitstelematikgesetz (GTelG 2012) in Kraft und im September 2014 wurde ein Implementierungsleitfaden für e-Medikation veröffentlicht. Seit Inkrafttreten der **ELGA-Verordnung 2015** steht fest, dass e-Medikation für alle öffentlichen Apotheken **verpflichtend** ist.

Apotheken sind als Gesundheitsdiensteanbieter (GDA) in dieses System eingebunden und können bei der Arzneimittelabgabe die Medikationsdaten in der elektronischen Gesundheitsakte ihrer Kund*innen speichern. Auf Basis des Implementierungsleitfadens wurde ein Probebetrieb zur e-Medikation von Mai bis November 2016 in der steirischen Region Deutschlandsberg durchgeführt. Damit wurde der Nachweis erbracht, dass e-Medikation technisch umsetzbar ist und auch funktioniert.

Am 15. Dezember 2017 wurde durch das Bundesministerium für Gesundheit die ELGA-Verordnungsnovelle 2017 erlassen und damit der österreichische roll-out von e-Medikation über alle Bundesländer geregelt. Der roll-out begann im ersten Quartal 2018 und endete im Herbst 2019. Die e-Medikation wird flächendeckend gemäß Gesundheitstelematikgesetz 2012[25] in den österreichischen Apotheken umgesetzt.

[25] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20008120 (31.01.2024)

Was verstehen wir unter e-Medikation?

Viele Patient*innen nehmen oft mehrere Medikamente gleichzeitig oder kurz hintereinander ein. Dabei kann es

- zu Mehrfachverordnungen bzw. Überdosierung eines Wirkstoffes oder
- unerwünschten Wechselwirkungen kommen.

Das kann in manchen Fällen eine gesundheitliche Gefahr für die Patient*innen darstellen. Das Ziel von e-Medikation ist, dieses Risiko zu minimieren und die Sicherheit bei der Einnahme von Medikamenten für Patient*innen zu erhöhen.

Bei e-Medikation handelt es sich um eine Anwendung der Elektronischen Gesundheitsakte (ELGA).

„e-Medikation ist eine Funktion der Elektronischen Gesundheitsakte (ELGA). Von Ärztinnen und Ärzten verordnete und in der Apotheke abgegebene Medikamente werden als sogenannte e-Medikationsliste für ein Jahr gespeichert. In Ihrer e-Medikationsliste sehen Sie alle ärztlich verordneten Medikamente, auch wenn sie noch nicht in der Apotheke eingelöst wurden. Die gleiche Information hat auch Ihre Ärztin bzw. Ihr Arzt, eine Ambulanz oder ein Spital, wenn Sie dort in Behandlung sind. Die Behandlungseinrichtungen haben damit die Möglichkeit, vor der Verordnung eines Medikamentes zu prüfen, ob die Gefahr von Wechselwirkungen mit Ihrer bestehenden Medikation besteht oder ob Ihnen das Medikament bereits einmal verordnet wurde.“[26]

Die technische Basis für e-Medikation bildet das hoch sichere **G**esundheits-**I**nformations-**N**etz (**GIN**) des Hauptverbandes der Sozialversicherungsträger. Dieses Netz besteht aus zwei getrennten Kanälen, dem **Sozialversicherungskanal** (zwischen Gesundheitsdiensteanbietern) und dem **Mehrwertdienstekanal**. Über den Mehrwertdienstekanal können sonstige Dienstleister ihre Services den Gesundheitsdiensteanbietern, wie zum Beispiel Apotheken, Ärzte, usw. anbieten. Das ELGA Gesetz sieht für alle Apotheken einen GIN Anschluss vor. Der GIN - Mehrwertkanal wird von der Peering Point Gesellschaft kontrolliert (50% Ärztekammer, 50% Hauptverband).

Der Hauptverband verwaltet mit der e-Card, eine „Gesundheits-Karte“, die praktisch alle in Österreich lebenden Personen erhalten und als „Schlüsselkarte“ für e-Health Anwendungen verwendet wird.

Die Arzneimitteldaten werden allerdings nicht auf der e-Card selbst, sondern in einem persönlichen Arzneimittelkonto gespeichert. Die e-Card der Patient*innen dient dabei als Zugangs-Schlüssel zu den Arzneimitteldaten, nicht aber als Identifikationsnachweis der jeweiligen Person.

Das e-Card-System ist neben dem Bankomatsystem, Bürgerkarten, Kundenkarten, Zutrittssystemen usw. ein technisches System, mit dem die Menschen tagtäglich konfrontiert sind.

[26] https://www.sozialversicherung.at/cdscontent/?contentid=10007.844040&portal=svportal#:~:text=e%2DMedikation%20ist%20eine%20Funktion,gesundheit.gv.at%20abrufen (31.01.2024)

e-Rezept ist NICHT gleich e-Medikation
Während der Pandemie hat uns das Service rund um die e-Medikation große Dienste geleistet. Erstmals konnten man sich ein Bild davon machen, wie sehr die Digitalisierung uns unterstützen kann.

Für die Zeit der Pandemie wurde eine Rezeptierung über e-Medikation ermöglicht, um die persönlichen Patientenkontakte auf das Notwendigste zu reduzieren. Patient*innen konnten die Arztordination telefonisch kontaktieren und die Verordnungsinformationen wurden von Ärzt*innen in der e-Medikation erfasst. In der Apotheke konnte mittels der SVNR die Verordnung innerhalb der e-Medikation aufgerufen und die Medikamente expediert werden. Weder für die Patient*innen, noch für die weitere Rezeptverrechnung war ein Papierrezept notwendig.[27]

Eine großartige Möglichkeit, jedoch kein Ersatz für das e-Rezept, da der Fokus der e-Medikation auf medizinischen Informationen liegt. Die e-Medikation nahm damit Aufgaben wahr, für die sie nie konzipiert war.

Mit dem e-Rezept hingegen können all diese notwendigen Prozesse digital abgebildet werden. Von e-Rezept können sich Versicherte daher auch nicht abmelden.

Die e-card ist der Schlüssel zum e-card System. Auf der e-card selbst werden keine Rezepte und auch keine Daten über Medikamente gespeichert. E-Rezepte werden zentral im e-card System gespeichert. Weitere Informationen dazu finden Sie hier: www.chipkarte.at/e-rezept (31.01.2024)

[27] https://www.ihe-austria.at/wp-content/uploads/2020/08/200609_IHE_514_kontaktlose-Medikamentenverschreibung_SVC.pdf (31.01.2024)

e-Rezept

Das e-Rezept ist ein lang geplantes gemeinschaftliches Projekt von Ärztekammer, Apothekerkammer und Sozialversicherung. Grundidee ist die Reduktion der papiergebundenen Prozesse durch elektronisches Erfassen, Einlösen und Abrechnen von Kassenrezepten. Die Pharmazeutische Gehaltskasse bildet die Schnittstelle zu den Herstellern von Apothekensoftware und hat 2021 die Pilotierung in zwei Bezirken in Kärnten begleitet. 2022 stand die Begleitung des österreichischen Rollouts und Hilfestellung in Form von Online-Sprecherstunden für Apotheker*innen am Programm.

Mit dem e-Rezept werden Kassenrezepte anstatt auf Papier als elektronisches Rezept ausgestellt. Die Einlösung in der Apotheke erfolgt einfach mit der e-card oder dem e-Rezept Code am Handy oder mit einem e-Rezept Ausdruck.

Folgender Nutzen ergibt sich von e-Rezept für Apotheker*innen:

- Die Daten für die Erfassung der Abgabe und für die Abrechnung sind elektronisch verfügbar.
- Ein e-Rezept ist fälschungssicher und kann damit nicht mehrmals eingelöst werden.
- Ein e-Rezept kann nicht manipuliert werden (Ausstellungsdatum, Verordnungsdaten etc.).
- Die Anzahl der zu lagernden Rezeptbelege wird durch das e-Rezept deutlich reduziert.
- Vereinfachung von papiergebundenen Prozessen in Apotheken und damit eine verbundenen Effizienzsteigerung.
- Tagesaktuelle Anrechnung bezahlter Rezeptgebühren zur Ermittlung einer Rezeptgebührenbefreiung aufgrund der Erreichung der Obergrenze (REGO Tagesaktuell).

Wie funktioniert e-Rezept?
Ihr Softwareanbieter implementiert das e-Rezept Service direkt in die gewohnte Apothekensoftware. Manche e-Rezept Funktionalitäten können Sie auch über das e-card System mit der e-card Web-Oberfläche nutzen. Folgende Schritte sind in ihrer Apotheke notwendig:

- Die Apotheke ruft das einzulösende e-Rezept im e-card System durch Stecken der e-card oder durch Scan des e-Rezept Codes vom Ausdruck oder durch eine manuelle Eingabe der REZ-ID ab.
- Die Apotheke erfasst die Abgabe in der Software bzw. im Hintergrund im e-card System. Das e-Rezept wird als eingelöst gekennzeichnet (auch in der e-Medikation)
  Daten für die Aktualisierung des Rezeptgebührenobergrenze-Kontos der versicherten Person werden im e-card System erfasst

- Einmal pro Monat erstellt die Apotheke eine Abrechnungsdatei und übermittelt diese sowie die elektronischen Rezepte (e-Rezept Datensätze) über die Pharmazeutische Gehaltskasse (öffentliche Apotheken) zur Abrechnung an die Versicherungsträger.
  Rezeptdaten werden aus e-Rezept in den Abrechnungsdatensatz übernommen
  Weitere Daten werden von der Apotheke ergänzt.

Die SVC hat ein Handout zum korrekten Umgang mit eRezepten veröffentlicht, mit Fokus auf verschiedene Rezeptarten und -formen. www.chipkarte.at/e-rezept/handout (07.02.2024)

[28] https://www.chipkarte.at/cdscontent/?contentid=10007.865480&portal=ecardportal (31.01.2024)

Die elektronische Gesundheitsakte - ELGA

ELGA steht als moderne und sichere Infrastruktur allen Bürger*innen und allen, die im österreichischen Gesundheitssystem versorgt werden, zur Verfügung. Als modernes Informationssystem erleichtert ELGA zukünftig Patient*innen sowie berechtigten ELGA-Gesundheitsdiensteanbieter – behandelnde Ärzt*innen, Spitäler, Pflegeeinrichtungen oder Apotheken – den Zugang zu Gesundheitsdaten. Ein wichtiges Ziel von ELGA ist somit die Unterstützung der medizinischen, pflegerischen und therapeutischen Behandlung und Betreuung durch einen besseren Informationsfluss, vor allem, wenn mehrere Gesundheitseinrichtungen oder Berufsgruppen entlang einer Behandlungskette zusammenarbeiten.

Die schrittweise Umsetzung begann im Dezember 2015. Beginnend mit öffentlichen Spitälern in Wien und in der Steiermark, wo Entlassungsbriefe sowie ausgewählte Labor- und Radiologie-Befunde via ELGA verfügbar gemacht wurden. Zug um Zug werden die öffentlichen Spitäler in den Bundesländern und die Pflegeeinrichtungen Österreichs flächendeckend daran teilnehmen. 2016 wurde e-Medikation als ELGA-Funktion getestet und wird im niedergelassenen Bereich bei Kassenärzten und in den Apotheken zur Verfügung stehen. In weiterer Folge auch den Kassenambulatorien, privaten Krankenanstalten und später auch Zahnarztpraxen mit Kassenvertrag.

Ihre ELGA-Daten können Sie seit Dezember 2015 über das ELGA-Zugangsportal abrufen (www.gesundheit.gv.at). Über dieses Portal können Sie auch die Verwaltung der Zugriffsrechte und Ihrer Dokumente vornehmen.

Falls Sie an diesem Thema mehr interessiert sind, besuchen Sie unsere Webseite (www.gehaltskasse.at), die Seite des Hauptverbandes der Sozialversicherungsträger (www.sozialversicherung.at), sowie die Seite der ELGA GmbH (www.elga.gv.at) und des Öffentlichen Gesundheitsportales Österreichs (www.gesundheit.gv.at).

7. Gesetzliche Grundlagen

In diesem Kapitel sind die wichtigsten Gesetze, denen Ihr Handeln in der Apotheke unterliegt, aufgelistet.

Für weitere Informationen gibt es in Österreich zwei herausragende Informationsplattformen: das Rechtsinformationssystem des Bundes (RIS) und www.österreich.gv.at. Sie finden dort alle Gesetzestexte und können sich detaillierter informieren.

Wenn Sie die Pharmazeutische Gehaltskasse zu Rechtsfragen kontaktieren möchten, wenden Sie sich an das Sekretariat unter der Telefonnummer 01/40414-211 bzw. richten Sie Ihre Anfrage per Mail an office@gk.or.at .

- Apothekenbetriebsordnung 2005 (ABO 2005), BGBl. II Nr. 65/2005, idF BGBl II Nr. 5/2016: Verordnung der Bundesministerin für Gesundheit und Frauen über den Betrieb von Apotheken und ärztlichen und tierärztlichen Hausapotheken
- Apothekergesamtvertrag gemäß §§348a ff ASVG, §181 BSVG, §193 GSVG, §128 B-KUVG
- Apothekengesetz (ApG), RGBl. Nr. 5/1907, idF BGBl. I Nr. 127/2017: Gesetz vom 18. Dezember 1906, betreffend die Regelung des Apothekenwesens
- Apothekerkammergesetz 2001, BGBl. I Nr. 111/2001, idf BGBL I Nr. 48/2017: Bundesgesetz über die Österreichische Apothekerkammer
- Datenschutzgesetz (DSG), BGBl. I Nr. 165/1999, idf BGBl. I Nr. 24/2018: Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten
- Datenschutzgrundverordnung (DSGVO) EU-Verordnung 2016/679: zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
- Datenschutz-Anpassungsgesetz 2018 (Datenschutzgesetz – DSG) BGBl. I Nr. 120/2017: Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten
- Datenschutz-Folgenabschätzung Verordnung (DSFA-AV), BGBl. II Nr. 108/2018: Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung
- E-Commerce Gesetz (ECG), BGBl. I Nr. 152/2001: Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden
- E-Government Gesetz (E-GovG), BGBl. I Nr. 10/2004: Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen
- ELGA-Verordnung 2015 (ELGA-VO 2015), BGBl. II Nr. 106/2015: Verordnung der Bundesministerin für Gesundheit zur Implementierung und Weiterentwicklung von ELGA
- ELGA Verordnungsnovelle 2017 (ELGA-VO_Nov 2017), BGBl. Nr. 380/2017: Verordnung

der Bundesministerin für Gesundheit und Frauen zur Änderung der ELGA-Verordnung 2015

- Gehaltskassengesetz (GKG 2002), BGBl. I Nr.154/2001: Bundesgesetz über die Pharmazeutische Gehaltskasse für Österreich
- Gesundheitstelematikgesetz 2012 (GTelG 2012), BGBl. I Nr. 111/2012: Bundesgesetz betreffend Datensicherheitsmaßnahmen bei der Verwendung elektronischer Gesundheitsdaten
- Informationssicherheitsgesetz (InfoSiG), BGBl. I Nr. 23/2002): Bundesgesetz über die Umsetzung völkerrechtlicher Verpflichtungen zur sicheren Verwendung von Informationen
- Informationssicherheitsverordnung (InfoSiV), BGBl. II Nr. 548/2003: Verordnung der Bundesregierung über die Informationssicherheit
- Pharmazeutische Fachkräfteverordnung, BGBl. Nr. 40/1930: Verordnung des Bundesministers für soziale Verwaltung vom 31. Jänner 1930, BGBL. Nr. 40, über die Verwendung des pharmazeutischen Fachpersonals in Betriebe der öffentlichen und Anstaltsapotheken, ferner die fachliche Ausbildung und Fachprüfung für den Apothekerberuf
- Signaturgesetz (SigG), BGBl. I Nr. 190/1999: Bundesgesetz über elektronische Signaturen
- Telekommunikationsgesetz 2003 (TKG 2003), BGBL. I Nr. 70/2003: Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird

8. Anhang

Quellenangaben - Bücher

Allweyer, Thomas: Geschäftsprozeßmanagement. Strategie, Entwurf, Implementierung, Controlling, Herdecke/Bochum 2010

Androsch, Hannes: Digitalisierung verstehen. Was wir über Arbeit, Bildung und die Gesellschaft der Zukunft wissen müssen, Wien 2021

Eckert, Claudia: IT-Sicherheit; Konzepte-Verfahren-Protokolle, Oldenbourg 2014

Greßler, Uli; Göppel, Rainer: Qualitätsmanagement – eine Einführung, Troisdorf 2010

Höllwarth, Tobias (Hrsg.): Der Weg in die Cloud, Heidelberg 2011

Kersten, Heinrich; Klett, Gerhard: Der IT Security Manager, Wiesbaden 2008

Kersten, Heinrich; Reuter, Jürgen; Schröder, Klaus-Werner: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz, Wiesbaden 2008

Köhler, Thomas: Chefsache Cybersicherheit, Frankfurt/New York 2021

Königs, Hans-Peter: IT-Risikomanagement mit System, Wiesbaden 2013

Levine, John; Levine Young, Margaret: Internet für Dummies, Weinheim 2010

Li Charlene; Bernoff, Josh: Facebook, YouTube, Xing & Co, München 2009

Lowe, Doug: Netzwerke für Dummies, Weinheim 2010

Knyrim, Rainer (Hrsg.): Datenschutz-Grundverordnung, Das neue Datenschutzrecht in Österreich und der EU, Wien 2016

Kreindl, Ricarda, Mösenbichler, Stefan, Thoß, Axel, Thurnher, Bettina (Hrsg.): Datenschutz für Unternehmen, Wien 2020

Köhler-Schute, Christiana (Hrsg.): Cloud Security: Praxisorientierte Methoden und Lösungen für sicheres Cloud Computing, Berlin 2021

Müller, Klaus-Rainer: IT-Sicherheit mit System, Wiesbaden 2008

Pachinger, Michael; Beham, Georg (Hrsg.): Datenschutz-Audit, Recht – Organisation – Prozess - IT, Wien 2020

Pollirer, Hans-Jürgen; Weiss, Ernest; Knyrim, Rainer; Haidinger, Viktoria: DSGVO Daten-

schutz-Grundverordnung, Wien 2022

Quellenangaben - Internet

A-Trust - Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH
https://www.a-trust.at

Arbeiterkammer Wien
https://wien.arbeiterkammer.at

ARGE DATEN
https://www.argedaten.at

Bundesamt für Sicherheit in der Informationstechnik
https://www.bsi.bund.de

Bundeskanzleramt Österreich
https://www.bka.gv.at/

Bundesministerium für Inneres
https://www.bmi.gv.at/

Computer Emergency Response Team (CERT)
https://www.cert.at/de/

Dataprotect – Informationen zum Datenschutz in Österreich
https://www.dataprotect.at/

Datenschutz-Anpassungsgesetz 2018
https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdf

Datenschutzbehörde der Republik Österreich
https://www.dsb.gv.at/

Deutsche Apothekerzeitung
https://www.deutsche-apotheker-zeitung.de

Digitales Österreich
https://www.digitales.oesterreich.gv.at

e-card
https://www.chipkarte.at

GovCERT Die vorliegende Informationsbroschüre wurde mit größter Sorgfalt erstellt. Dennoch kann keine Gewähr für die Richtigkeit, Vollständigkeit und Aktualität sämtlicher Informationen übernommen werden. Eine Haftung der Autorin ist ausgeschlossen.
https://www.govcert.gv.at

e-commerce monitoring GmbH
https://www.e-monitoring.at
ELGA GmbH
https://www.elga.gv.at

Forum!pharmazie
https://www.forumpharmazie.at/

Gesellschaft für Prozessmanagement
https://www.prozesse.at

Hauptverband der Österreichischen Sozialversicherungsträger
https://www.sozialversicherung.at

ID Austria
https://www.oesterreich.gv.at/id-austria.html

Netzrecht.at
https://www.netz-recht.at/

Österreichs digitales Amt
https://www.oesterreich.gv.at/

Öffentliches Gesundheitsportal Österreichs
https://www.gesundheit.gv.at

Online-Kündigung
https://www.online-kuendigen.at

Online-Sicherheit
https://www.onlinesicherheit.gv.at

Österreichische Apothekerkammer
https://www.apotheker.or.at

Österreichischer Apothekerverband
https://www.apothekerverband.at

Österreichischer Apothekerverlag - ÖAZ
https://www.apoverlag.at

Österreichisches Informationssicherheitshandbuch
https://www.sicherheitshandbuch.gv.at

Pharmazeutische Gehaltskasse für Österreich
https://www.gehaltskasse.at

SANS-Institute
https://www.sans.org/newsletters/ouch/top-cybersecurity-tips-for-vacations/

Secure Business Austria Autorengruppe: OCG IT-Security, Wien 2008
https://www.ocg.at

Rechtssystem des Bundes (RIS)
https://www.ris.bka.gv.at

Rechtsvorschrift für Rechtsanwaltsordnung
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001673

Rechtsvorschrift für Wirtschaftstreuhandberufsgesetz
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009983

Tactical Tech – Data Detox Kit
https://datadetoxkit.org/de/home/

Unternehmensserviceportal
https://www.usp.gv.at

Verband Angestellter Apotheker Österreichs
https://www.vaaoe.at

Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010206

Verein zur Förderung der Sicherheit Österreichs strategischer Infrastruktur
https://www.cybersecurityaustria.at

Zentrum für sichere Informationstechnologie – Austria
https://www.a-sit.at

Ansprechpartnerin

Mag.phil. Monika Kerschenbauer, MSc

monika.kerschenbauer@gk.or.at

+43 1 40414 – 281

Bei Fragen zu konkreten Situationen in Ihrer Apotheke wenden Sie sich am besten an Ihre Hard- und Software Lieferanten!

Impressum

Medieninhaber:
Pharmazeutische Gehaltskase für Österreich

Spitalgasse 31

1090 Wien

Redaktion:
Mag. phil. Monika Kerschenbauer, MSc