# Cyber Security für Arztpraxen

| | |
|---|---|
| Datum: | 09.02.2023 |
| Projekt: | jameda |
| Thema: | Cyber Security für Arztpraxen |
| Keywords: | |
| Ansprache | Sie |
| Title: | Cyber Security für Arztpraxen – alles, was Sie wissen müssen |
| Description: | Cyber Security für Arztpraxen – alles, was Sie wissen müssen ✓ Entwickeln Sie eine Datenschutzstrategie für Ihre Praxis ✓ Checkliste: Wie Sie Ihre Praxis bei dem Thema Cyber Security fit machen ✓ Fazit ▶️ Jetzt lesen! |

## Content:

In diesem Blogartikel erfahren Sie, wie Sie eine Datenschutzstrategie für Ihre Arztpraxis entwickeln können.

**<h1> Warum Datenschutz im Praxisalltag wichtig ist</h1>**

Haben Sie als Ärztin bzw. Arzt schon einmal über mögliche Sicherheitsrisiken in Ihrer Praxis nachgedacht? Schließlich haben Sie täglich mit unzähligen sensiblen Daten Ihrer Patient:innen zu tun.

Die Verwaltung dieser Daten findet in der Regel digital statt. Die Digitalisierung ermöglicht auf der einen Seite zwar eine enorme Arbeitsentlastung, jedoch birgt sie auch Gefahren wie mögliche Cyber-Attacken auf Ihre Praxisdaten.

83 % der niedergelassenen Ärzteschaft befürchtet, dass mit der Digitalisierung auch Cyberangriffen Tür und Tor geöffnet wird.[1] Doch nicht nur von außen drohen Gefahren, auch durch ein internes Versehen, wie in unserem Beispiel gezeigt, können Daten schnell in falsche Hände geraten.

In diesem Blogartikel möchten wir Ihnen daher aufzeigen, welche Schritte Sie für eine optimale Cyber Security einleiten müssen, um die Daten Ihrer Praxis sowie Ihre Patient:innen zu schützen.

**<h2> Entwickeln Sie eine Datensicherheitsstrategie für Ihre Praxis </h2>**

Es ist wichtig, dass Sie für Ihre Praxis von Anfang an sichere Online-Tools verwenden, die einen reglementierten Zugang erlauben und eine strenge Datenschutzrichtlinie verfolgen.

Unsere Arzt-Patienten-Plattform bspw. verschlüsselt die Übertragung von vertraulichen Daten und ermöglicht sicherheitskonforme Videosprechstunden, sodass Sie sich keine Sorgen um Ihren Datenschutz machen müssen.

Bei der Einführung Ihrer Sicherheitsrichtlinie und der Einhaltung der Datenschutzvorgaben gilt es vieles zu beachten. Externe Datenschutzbeauftragte können Ihre Praxis dabei unterstützen.

Die Anstellung / Ernennung einer bzw. eines internen Datenschutzbeauftragten ist dann **verpflichtend**, wenn mindestens 10 Personen in Ihrer Praxis ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.[4]

Darüber hinaus macht es für Ihre Praxis Sinn, sich über eine mögliche Cyber-Security-Versicherung Gedanken zu machen, mit der Sie und Ihre Mitarbeitenden in folgenden Fällen geschützt sind:[5]

**Das leistet eine Cyberversicherung**

**Eigenschäden**

- Wirtschaftliche Schäden durch Unterbrechungen des Praxisbetriebs. **Leistung: Zahlung eines Tagessatzes**
- Kosten der Datenwiederherstellung und Systemrekonstruktion. **Leistung: Übernahme der Kosten**

**Drittschäden**

- Schadenersatzforderungen von Patienten wegen Datenmissbrauchs. **Leistung: Entschädigung und Abwehr unberechtigter Forderungen**

**Serviceleistungen**

- IT-Forensik-Experten zur Analyse, Beweissicherung und Schadenbegrenzung
- Anwälte für IT und Datenschutzrecht zur Beratung
- PR-Spezialisten für Krisenkommunikation zur Eindämmung des Imageschadens. **Leistung: jeweils Vermittlung und Kostenübernahme**

Neben der Entwicklung und Etablierung einer Datenschutzstrategie und der Verwendung sicherheitskonformer digitaler Tools ist die Sensibilisierung Ihrer Belegschaft ein weiterer Kernfaktor, um Ihre Praxis vor Sicherheitslücken zu schützen.

Was Sie als Ärztin bzw. Arzt hier berücksichtigen sollten, erfahren Sie im folgenden Abschnitt.

**<h2> Mitarbeiter:innenbezogene Sicherheitsmaßnahmen </h2>**

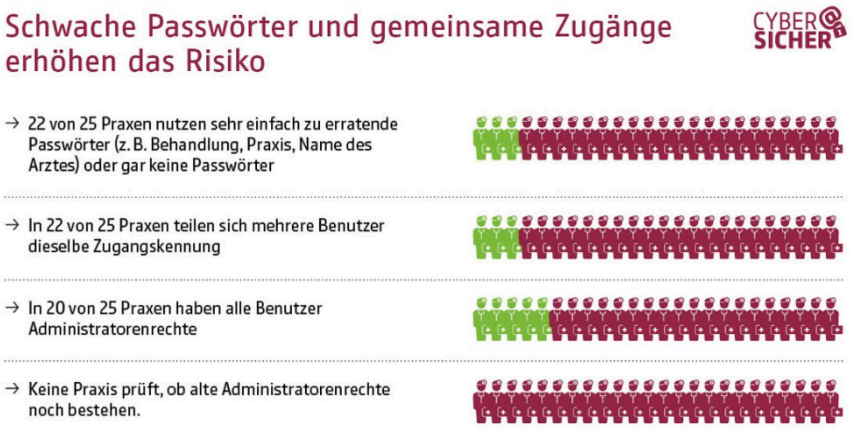
Der einfachste und schnellste Weg für Cyberkriminelle ist der über Ihre Mitarbeitenden. So können diese aus Versehen auf eine Phishing-Mail klicken, Daten an falsche Empfänger:innen schicken oder Arbeitsgeräte verlieren.

Wichtig ist daher, nicht nur sich selbst, sondern auch Ihre Mitarbeitenden für die genannten Sicherheitsrichtlinien und -verfahren zu sensibilisieren.

Im Rahmen dessen gilt es, sich über die Verwendung sicherer Passwörter, geregelte Zugriffsrechte und Datenschutzschulungen Gedanken zu machen.

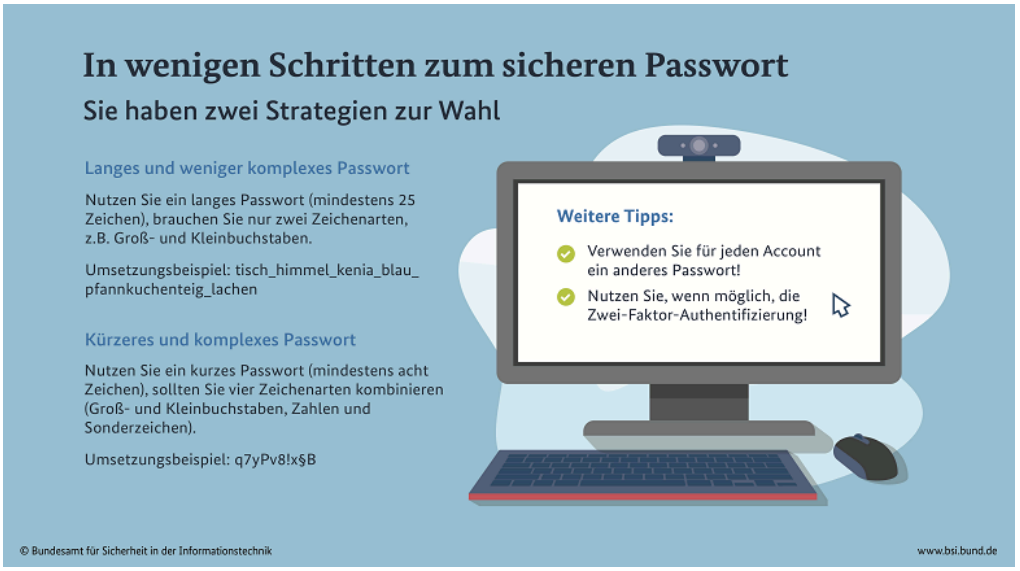
**<h3> Verwendung sicherer Passwörter </h3>**

Die simpelste Datenschutz-Methode für Sie und Ihr Praxispersonal: sichere Passwörter. Der Branchenreport des GDV[6] offenbarte, dass in rund 90 % der getesteten Arztpraxen mehrere Benutzer:innen dieselbe Zugangskennung mit sehr einfachen oder sogar ohne Passwörter nutzen:




Ungenügend gesicherte oder gar ungeschützte Zugänge zu Tools ermöglichen Cyberkriminellen leichtes Spiel. Achten Sie also dringend darauf, dass Ihre Mitarbeitenden sichere Passwörter benutzen.

Das Bundesamt für Sicherheit in der Informationstechnik zeigt folgende zwei Strategien für die Generierung von sicheren Passwörtern auf:[7]




Auch eine Zwei-Faktor-Authentifizierung, die mittlerweile von vielen Online-Dienstleistern angeboten wird, erhöht ihre Datensicherheit zusätzlich.

Bei diesem Verfahren wird ein zweiter Faktor nach dem Anmelden benötigt, bspw. eine SMS oder eine generierte TAN-Nummer, um sich final einloggen zu können.

Doch nicht nur die Sicherheit und Komplexität der Passwörter ist entscheidend, sondern auch die regelmäßige Erneuerung dieser.

Setzen Sie sich und Ihren Mitarbeitenden am besten Termine, um die Passwörter der von Ihnen genutzten Online-Tools wie bspw. der jameda Arzt-Patienten-Plattform upzudaten.

**<h3> Zugriffsberechtigungen managen </h3>**

Ihr Team kann in Ihren eigenen IT-Systemen und Tools unzählige Daten lesen und verändern. Allerdings können Ihre Mitarbeitenden Daten auch unauffällig kopieren oder löschen, obwohl sie dies nicht dürfen.

Hier spricht man von sogenannten „Innentäter:innen“ und sie stellen ein besonders hohes Datenrisiko für Ihre Arztpraxis dar – dies muss nicht einmal bewusst geschehen, wie Sie an folgender Grafik ablesen können: [8,9]

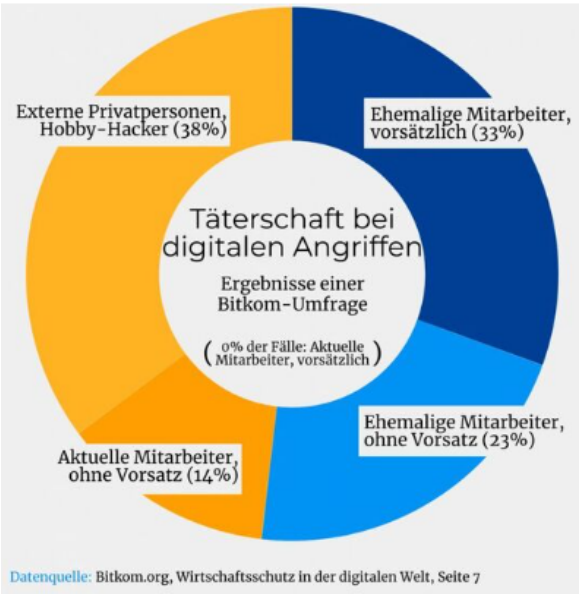



Bild muss nachgebaut werden und stammt von
https://www.storage-insider.de/storage-datenschutz-wenn-eigene-ex-mitarbeiter-zu-taetern-werden-a-1035503/ (nicht in Quellen angegeben)
**Original kommt von:**
https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019_0.pdf

Achten Sie also darauf, welche Teammitglieder auf welche Daten Zugriff haben. Denn: Je mehr Personen Zugriff auf Patientendaten haben, desto größer ist auch die Gefahr für Sicherheitslücken.

Hinterlegen Sie die Zugriffe in einem zentralen Rechtemanagement, um die Kontrolle über die von Ihrem Personal genutzten Konten und den damit verbundenen Daten zu haben.

So können Sie nach dem Ausscheiden eines Teammitglieds hier einfach überprüfen, welche Konten mit dieser Person verknüpft waren und die Zugriffsrechte wieder entziehen.

Laut der Bitkom-Umfrage „Wirtschaftsschutz in der digitalen Welt“ von 2019 sind es ganze 33 % der ehemaligen Mitarbeitenden, die vorsätzlich bei digitalen Angriffen auf Unternehmen agieren.[9]

**<h3> Kontinuierliche Schulung Ihres Praxispersonals </h3>**

Das Thema Datenschutz und die damit einhergehenden Verpflichtungen und kontinuierlichen Anpassungen sind sehr komplex und ohne professionelle Hilfe nur mit viel Zeit und Energie in Eigenregie zu durchdringen.

Zeit, die Sie als Ärztin bzw. Arzt und Ihr Team nicht haben. Nutzen Sie also Schulungen von professionellen Anbietenden, um sich selbst und Ihre Belegschaft auf dem neuesten Stand zu halten und Ihre Praxis datenschutzkonform einzurichten.

Mitarbeitende, die mit personenbezogenen Daten zu tun haben, müssen laut der Datenschutz-Grundverordnung sogar zwingend in den Regeln des Datenschutzes geschult werden.

Hierfür finden Sie ebenfalls ein breites Angebot an Online-Schulungen, aus dem Sie sich das für Sie und Ihr Team passende Format aussuchen können. Inhalte sollten sein:[10]

- Identifizierung von Phishing-Attacken,
- Nutzung von Social Media und Internet,
- sichere Passworterstellung sowie
- Clean Desk Policy.

**<h2> Maßnahmen zum Schutz sensibler Patientendaten </h2>**

Das Thema Datenschutz kommt im Berufsalltag oft zu kurz. Aber gerade Praxen arbeiten mit hochsensiblen Patient:innendaten. Sie als Ärztin bzw. Arzt sollten sich daher unbedingt intensiv mit dem Thema auseinandersetzen, um Ihre Praxis vor Cyberattacken zu schützen.

Eine eigene Datenschutzrichtlinie und die Unterstützung durch eine oder einen internen oder externen Datenschutzbeauftragten bringen Sie hier auf den richtigen Weg. Die Sensibilisierung und regelmäßige Schulung Ihrer Mitarbeitenden sowie ein geregeltes Zugriffsmanagement minimieren zusätzlich interne Sicherheitslücken.

Ein professionelles und datenschutzkonformes Online-Tool wie die jameda Arzt-Patienten-Plattform ermöglicht Ihnen von vornherein eine verschlüsselte und somit sichere Kommunikation mit Ihren Patient:innen.

*CTA:*

Vorschlag 1:
Über jameda
Unsere Arzt-Patienten-Plattform erlaubt Patientinnen und Patienten ein selbstständiges Terminmanagement und spart dem Praxispersonal viel Zeit für andere Aufgaben. Mit den Videosprechstunden über jameda kann eine moderne und flexible Patientenversorgung sichergestellt werden. Dank einer optimalen Sichtbarkeit Ihres Arztprofils können Patientinnen und Patienten den passenden Arzt oder Ärztin schneller finden.

Vorschlag 2:
Mehr als 6 Millionen Nutzer greifen monatlich auf die Plattform von jameda zu, um die Online-Terminvergabe zu nutzen oder sich über Arztpraxen zu informieren. Planen auch Sie den

Einsatz eines Online-Terminbuchungstools in Ihrer Praxis? Kontaktieren Sie uns für eine kostenfreie Beratung

*Vorschlag 3:*

>> Weitere praxisrelevante Informationen finden Sie in unserem Blog für Ärztinnen und Ärzte hier: https://pro.jameda.de/blog

Vorschlag 4:

Wussten Sie, dass bereits mehr als 15.000 Ärzt:innen in Deutschland jameda nutzen, um bis zu 10 Stunden pro Woche bei administrativen Aufgaben einzusparen und so ihr Praxisteam zu entlasten?

- Mit der Online-Terminvergabe können Sie Ihr Praxisteam durch Funktionen wie das automatische Terminmanagement, Terminbenachrichtigungen für Patienten und die Nachrücker-Funktion entlasten, um mehr Zeit mit den Patienten in der Praxis zu verbringen.
- Ihre Patient:innen haben die Möglichkeit, Termine außerhalb ihrer Geschäftszeiten direkt am Smartphone zu buchen. Durch Terminerinnerungen sinkt die Ausfallrate und über unseren verschlüsselten Messenger können Sie bereits vor der Behandlung direkt mit Ihren Patientinnen kommunizieren.

Das jameda Team berät Sie gerne telefonisch oder persönlich zu Lösungen, um dem Fachkräftemangel in Ihrer Praxis entgegenzuwirken und Zeit für Sie und Ihr Praxisteam einzusparen. Klicken Sie auf den folgenden Button, um einen kostenlosen Rückruf zu vereinbaren.

CTA: Jetzt Kontakt aufnehmen

Link: https://pro.jameda.de/kontakt

___

**Quellen:**


1 https://www.cgm.com/deu_de/magazin/artikel/praxissoftware/bitkom-studie-praxen-sorgen-sich-um-ihre-it-sicherheit.html
(09.02.2023)

2 https://www.kvb.de/index.php?eID=dumpFile&t=f&f=31231&token=14d2146fb5fc694497139c1a6e7e14de0f3db77b
(09.02.2023)

3 https://www.datenschutz.org/datenschutzbeauftragter-arztpraxis/

(09.02.2023)

4 https://www.gdv.de/resource/blob/48328/ae262d6702e2d9f5446c780a22450d23/branchenreport-cyberrisiken-bei-aerzten-und-apothekern-data.pdf
(09.02.2023)

5 https://www.gdv.de/gdv/medien/medieninformationen/deutschlands-aerzte-haben-ein-passwort-problem-zugangsdaten-haeufig-im-darknet-zu-finden-45192
(09.02.2023)

6 https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html
(09.02.2023)

7 https://www.datenschutz-praxis.de/tom/zugriffskontrolle-unerlaubten-zugriffen-auf-der-spur/
(09.02.2023)

8 https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019_0.pdf
(09.02.2023)

9 https://info.care4it.ch/blog/cyber-security-in-der-arztpraxis
(09.02.2023)