Lösungen und Strategien
für den medizinischen Sektor

TRUST IN
GERMAN
SICHERHEIT

IT-Security in Arztpraxen

»Grundsätzlich stehen Ärzte, Apotheker und ihre Teams mit der fortschreitenden Digitalisierung vor der Herausforderung, dass ihre IT-Ausstattung einfach verlässlich laufen muss

Grundlagen zur Sicherheit in den Arztpraxen

Unser Gesundheitswesen ist leistungsfähig, wie das vielerorts vorbildliche Management der Corona-Pandemie beweist. Aber in Sachen digitales Gesundheitswesen sind uns Länder wie Lettland, Dänemark oder auch die Niederlande teils deutlich voraus. Das Bundesgesundheitsministerium hat deshalb Maßnahmen auf die Agenda gesetzt, die hier den Rückstand Deutschlands kompensieren sollen und digitale Abläufe fest etablieren.

Aktuell folgen Neuerungen Schlag auf Schlag: Bereits seit Jahresbeginn 2021 kann jeder Patient (freiwillig) die elektronische Patientenakte – kurz: ePA - nutzen. Auch die elektronische Arbeitsunfähigkeitsbescheinigung, das E-Rezept, der E-Arztbrief und die Qualifizierte Elektronische Signatur werden – gesetzlich klar geregelt - fester Bestandteil des Praxisalltags.

Für manche Arztpraxis ändert sich durch diese Digitalisierungsschritte wenig – ihr Praxisinformationssystem ist bereits für den Start aller Lösungen bestens vorbereitet, intern werden Patientenakten längst digital geführt. Dort, wo erst jetzt vermehrt Informationstechnologie Einzug hält, sollte von Beginn an darauf geachtet werden, dass alle Datenschutzanforderungen eingehalten werden. Der Gesetzgeber hat mit dem Digitale-Versorgung-Gesetz die Grundlage für klare IT-Sicherheitsrichtlinien geschaffen. So werden Praxen (gemäß § 75b Abs 1 SGB V) dazu verpflichtet, die IT-Sicherheit innerhalb ihrer Praxis zu gewährleisten. Dazu gehört es, unbefugte Zugriffe oder Cyberangriffe auf Praxisrechner und Speichermedien zu verhindern. Für niedergelassene Ärzte und Zahnärzte wird die genaue Umsetzung dieser Schutzmaßnahmen durch die von der KBV oder KZBV beschlossenen IT-Sicherheitsrichtlinien vorgegeben. Im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik werden die technischen Anforderungen jährlich aktualisiert. Die Sicherheitsanforderungen an Arzt- und Psychotherapeutenpraxen beinhalten Punkte wie Sicherheitsmanagement, Organisation und Personal, IT-Systeme, Anwendungen und Dienste oder das Aufspüren von Sicherheitsvorfällen.

Allein durch die fachmännische Installation neuer Anschlüsse, Firewalls und anderer Geräte ist es nicht getan. Jede Mitarbeiterin und jeder Mitarbeiter sollte mit der Technik und den wichtigsten Sicherheitsmaßnahmen vertraut sein. So, wie es in der ausschließlich analogen Arztpraxis selbstverständlich war, dass Patientenakten nicht offen herumlagen und die Praxistür am Abend fest verschlossen wurde, müssen auch digitale Akten und Daten verantwortungsbewusst verwendet und sicher geschützt werden.

Was die Digitalisierung verändert

Der Staat sorgt mit der Telematikinfrastruktur (TI) für die bundesweite Vernetzung aller Akteure einschließlich Absicherung, die schwere Missbrauchsfälle weitgehend ausschließt - sofern alle Regeln eingehalten werden. Niedergelassene Ärzte, MVZ, Apotheker und ihre Teams stehen mit diesen Digitalisierungsmaßnahmen aber fraglos vor der Herausforderung, dass ihre gesamte IT-Ausstattung rundum abgesichert sein muss. Dazu zählen sämtliche Notebooks, Tablet-PC und Smartphones in der Praxis! Außerdem Drucker, Multifunktionssysteme und diverse Bildschirme. Auch Medizintechnik ist zunehmend vernetzt! Machen Sie sich klar: Kommt es zu Hacker-Angriffen oder anderen IT-Ausfällen, steht der gesamte Praxisbetrieb still.

Vorausschauend handeln

Sämtliche Technik sollte so abgesichert sein, dass Daten-Diebstahl unmöglich ist und bei Schäden jedweder Art sofort eine Möglichkeit besteht, den ursprünglichen (funktionsfähigen) Zustand wiederherzustellen. Die gute Nachricht ist: Das alles ist möglich! Realisierbar ist das aber nicht von Medizinern und Praxismitarbeitern allein. Es empfiehlt sich, diese strategischen Entscheidungen in die Hände von qualifizierten Fachleuten zu geben.

TIPP *Alte Hardware gehört ins Museum, nicht in ihre Praxis! Ein Computersystem aus dem Jahr 2003 mit „Windows XP“, ein Smartphone mit einer Android-Version von 2009, eine Telefonanlage, die noch aus dem letzten Jahrhundert stammt – alles das sind gefährliche Einfallstore für Computerkriminelle! Ersetzen Sie Uralt-Technik so schnell wie möglich, wenn sie in ihrer Praxis die Sicherheit der Patientendaten weiterhin gewährleisten möchten.*

IT-Sicherheit
Das müssen Arztpraxen und MVZ beachten

Büroräume immer abschließen oder mit Codekarten betreten

Zugangsdaten (Passwörter) keinesfalls auf Notizzetteln notieren

PC-Updates (Software und Betriebssystem) regelmäßig installieren

Regelmäßig eine Datensicherung erstellen

Vom Müssen und Wollen

Das Thema Datenschutz spielt im Gesundheitsbereich eine zentrale Rolle, nicht erst seit der Datenschutz-Grundverordnung (DSGVO), die seit Mai 2018 gilt. Die Europäische Union definiert Datenschutz in ihrer Richtlinie 95/46/EG als „den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten“. Organisatorische und technische Maßnahmen müssen überall gewährleisten, dass persönliche Daten bei der Speicherung und Übertragung sicher und geschützt sind. Das gilt selbstverständlich überall.

»Für alle in der Telematikinfrastruktur übermittelten Daten gilt Schutzstufe E. Das ist die höchste Sicherheitsstufe in Deutschland

Gesundheitsdaten unter besonderem Schutz

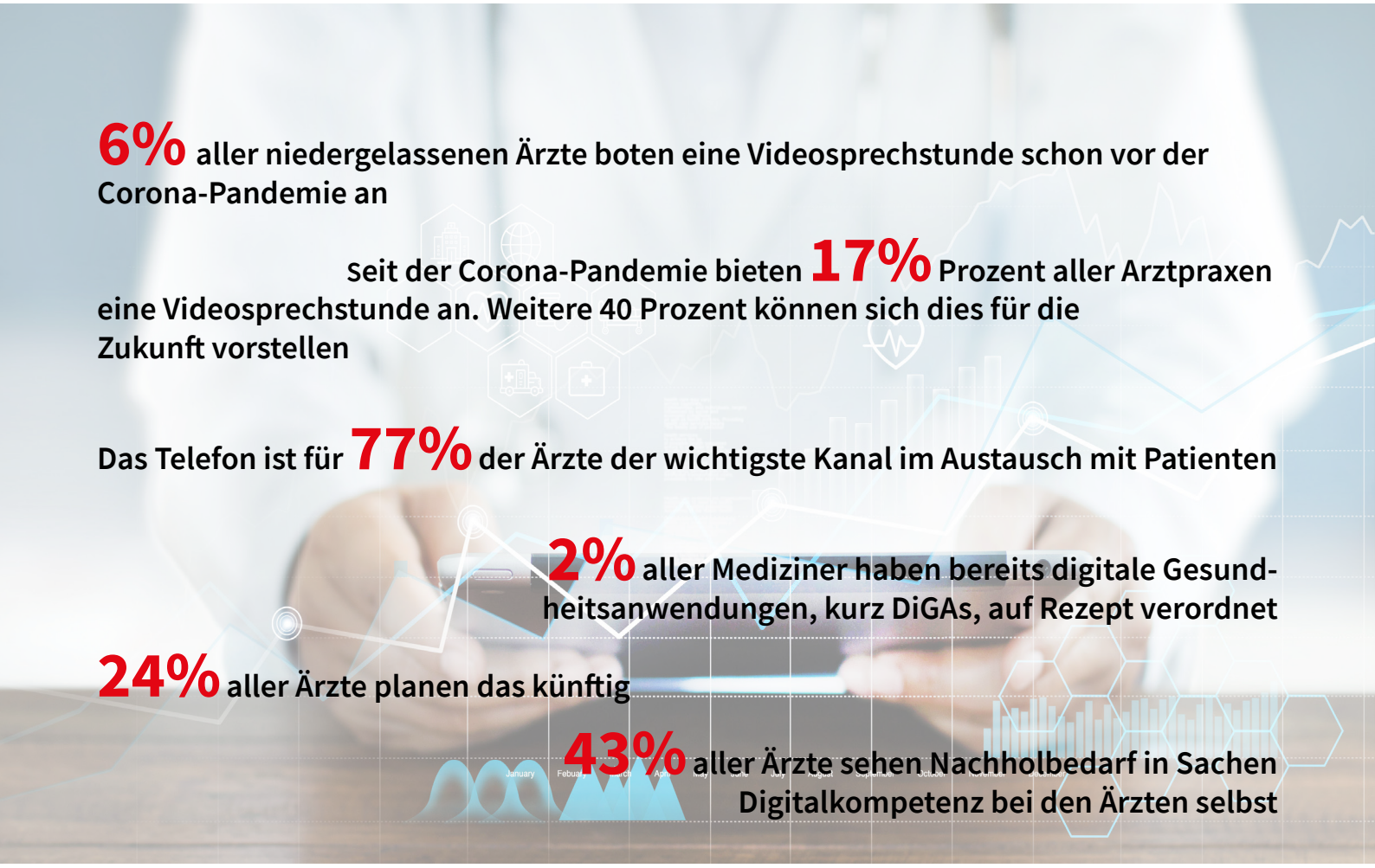
Es gibt jedoch Abstufungen. Daten aus dem gesundheitlichen Umfeld sind dabei besonders schutzwürdig. Für alle in der Telematikinfrastruktur übermittelten Daten gilt Schutzstufe E. Das ist die höchste Sicherheitsstufe in Deutschland. Zum Vergleich: Für das Onlinebanking gilt Stufe C. Die Zertifizierung der Telematikinfrastruktur nimmt das Bundesamt für Sicherheit in der Informationstechnik vor. Es ist auch für die Sicherheitszertifizierung sämtlicher Komponenten und Produkte in der Telematikinfrastruktur (TI) verantwortlich.

Die Übermittlung von Gesundheitsdaten zwischen Ärzten, Psychotherapeuten, Apothekern und Krankenhäusern –zum Beispiel Befunde, Röntgenbilder, Informationen zu Vorerkrankungen, Blutbilder oder Arztbriefe - darf nur durch autorisierte Personen erfolgen. Jeder Zugriff erfolgt über eine Smartcard – entweder einen elektronischen Heilberufsausweis oder einen Institutionsausweis. Möglich ist das Ärzten, Apothekern, Psychotherapeuten, medizinischen Fachangestellten sowie Gesundheits- und Krankenpflegern. Die Speicherung und Übermittlung medizinischer Daten ist nur möglich, wenn Versicherte dem im Vorfeld zustimmen.

Entschlossen über den Tellerrand blicken

Doch was ist mit Gesundheits-Apps, die künftig jeder Hausarzt auswerten soll? Ist das Smartphone des Patienten, auf dem die Apps installiert sind, wirklich gut abgesichert? Wie sieht es in ihrem Praxis-Netzwerk aus? Wann haben die PC und andere Geräte das letzte Update erhalten? Was geschieht mit Anfragen von Patientinnen und Patienten oder Kollegen, die – außerhalb der TI - per E-Mail oder Smartphone-Messenger gesendet werden? Enthält die angehängte Röntgenaufnahme womöglich Schadsoftware? Selbst ein vermeintlich harmloser Kopierer lässt sich mit etwas krimineller Energie in ein Spionageinstrument verwandeln.

Kein Arzt und keine Fachangestellte kann das alles hundertprozentig im Blick behalten! Dennoch müssen sie künftig keinen eigenen IT-Experten beschäftigen, um den Anforderungen des digitalen Gesundheitswesens gerecht zu werden. Wer die Vernetzung nicht nur als Pflicht begreift, sondern sie für die eigenen Zwecke smart einsetzt, erreicht erfolgreich ein hervorragendes IT-Sicherheitsniveau. Das gibt es nicht umsonst, aber ganz sicher ohne eine Kostenlawine.



6% aller niedergelassenen Ärzte boten eine Videosprechstunde schon vor der Corona-Pandemie an

Seit der Corona-Pandemie bieten **17%** Prozent aller Arztpraxen eine Videosprechstunde an. Weitere 40 Prozent können sich dies für die Zukunft vorstellen

Das Telefon ist für **77%** der Ärzte der wichtigste Kanal im Austausch mit Patienten

2% aller Mediziner haben bereits digitale Gesundheitsanwendungen, kurz DiGAs, auf Rezept verordnet

24% aller Ärzte planen das künftig

43% aller Ärzte sehen Nachholbedarf in Sachen Digitalkompetenz bei den Ärzten selbst

Quelle: bitkom.org/ 02. Februar 2021 // Grundlage der Angaben ist eine Befragung, die Bitkom Research im Auftrag des Digitalverbands Bitkom und des Hartmannbundes im November 2020 durchgeführt hat. Dabei wurden 528 Ärzte aller Funktionen und Fachrichtungen befragt, darunter Ärzte im Krankenhaus und niedergelassene Ärzte.

Digitalisierung: Hilfreich statt nur unvermeidlich

Die Digitalisierung im Gesundheitswesen soll den Rückstand Deutschlands in der (digitalen) medizinischen Versorgung verringern. Die meisten niedergelassenen Ärzte, Praxisgemeinschaften und medizinische Versorgungszentren (MVZ) fangen hier nicht bei Null an: Praxissoftware für die Verwaltung, die Organisation und den Betrieb der Praxis wird bereits in tausenden Arztpraxen verwendet. Services wie Videosprechstunden, elektronische Rezepte und die elektronische Patientenakte werden aktuell zum selbstverständlichen Teil des Versorgungsalltags.

Viele Bürger sehen hier Chancen, ihre Gesundheit besser zu „managen“. Immer mehr Patientinnen und Patienten informieren sich im Internet und nutzen Wearables und Apps, um ihre Gesundheitsdaten zu erfassen und auszuwerten. Sie sind motiviert, mithilfe digitaler Tools ihre täglich geleisteten Schritte zu zählen oder den Kalorienverbrauch zu prüfen. Betrachten sie diese Entwicklung nicht als Modewelle – Gesundheitsapps, elektronische Rezepte und der Patientenkontakt per Video werden sich fest etablieren.

Die Digitalisierung sorgt nicht zuletzt für neue Diagnostik- und Behandlungsmöglichkeiten wie die personalisierte Medizin. Mit ihr kann die Kommunikation zwischen den einzelnen Akteuren im Gesundheitswesen (etwa Haus- und Facharzt) sowie mit jedem einzelnen Patienten verbessert werden. So werden sich Versorgungsprozesse, die Inanspruchnahme von Gesundheitsleistungen grundlegend verändern. Der Point of Care wird sich von Arztpraxis und Klinik immer stärker hin zum Patienten verlagern. Neue diagnostische und therapeutische Möglichkeiten entstehen durch das Zusammenspiel von Software, Sensorik und Medizintechnik. Innovative, digitale Medizinprodukte werden Teil der Regelversorgung.

Mehrwert für den behandelnden Arzt

Digitale Gesundheitslösungen werden zunehmend auch jedem behandelnden Arzt erkennbare Mehrwerte liefern. Zusätzlich gewonnene Daten erfassen effizient die Phasen zwischen den Arztbesuchen, wodurch präzisere und passgenauere Behandlungen möglich werden. Der Behandler kann frühzeitiger und exakter als bisher auf die Entwicklung des Gesundheitszustandes seiner Patienten eingehen. Dem Patienten kann passgenau ein Praxisbesuch empfohlen werden, wenn dies erforderlich erscheint. Ärztinnen und Ärzte können Rat und Hilfestellungen via Internet anbieten. Videosprechstunden haben sich im Zuge der Corona-Pandemie bereits in jeder fünften Arztpraxis fest etabliert und sie werden auch von Krankenkassen honoriert.

Das spart oft lange Wege und Wartezeiten – auch die Infektionsgefahr sinkt. Patientinnen und Patienten nehmen diese Angebote dementsprechend gerne in Anspruch - wenn sie denn von ihrer Arztpraxis offeriert werden.

Die Digitalisierung sollte weder als Selbstzweck, noch als von der IT-Branche getriebene Maßnahme angesehen werden. Noch nie war es ratsam, realisierbare (technologische) Lösungen als nicht wünschenswert abzutun und deshalb nicht aufzugreifen. Zukunftsverweigerung hat noch nie nachhaltig funktioniert.

Soziale Herausforderungen meistern

Digitale Technologien können dabei helfen, die Herausforderungen aller Gesundheitssysteme der westlichen Welt besser zu lösen. Fast alle Länder sind mit der Problematik konfrontiert, dass immer mehr ältere und chronisch kranke Menschen behandelt werden müssen – man denke hierzulande nur an die Generation der „Babyboomer“, die bald das Rentenalter erreicht. Sollen teure medizinische Innovationen etwa nur einem exklusiven Personenkreis zur Verfügung stehen, der es sich leisten kann? Wie kann es gelingen, auch strukturschwache ländliche Gebiete medizinisch zu versorgen? Die Digitalisierung ist nicht die Antwort auf alles, aber sie kann dazu beitragen, viele Probleme besser zu lösen.

Künstliche Intelligenz und Big Data

Künstliche Intelligenz (KI) kann ebenfalls zu einer verbesserten Patientenversorgung beitragen. KI unterstützt Ärzte dabei, eine Diagnose zu stellen. Durch KI können Therapien individueller auf Patienten abgestimmt werden, so wie es in der Krebsbehandlung bereits geschieht. Künstliche Intelligenz wird nicht den Arzt ersetzen, aber sie kann Mediziner dabei unterstützen, schneller und präziser eine Therapie einzuleiten.

Fester Bestandteil all dieser Lösungen muss IT-Security sein. Sie ist eine Grundlage bei der Praxisdigitalisierung. Externe Unterstützung ist dabei gefragt, denn Ärzte und ihre Mitarbeiter können das nicht selbst leisten. Doch keine Frage: Wenn die IT-Sicherheit gewährleitet ist, werden die Behandler und ihre Teams mehr Zeit für die Patienten gewinnen.

Patientendaten - Das müssen Arztpraxen und MVZ beachten

- ***Patienten, die kurzzeitig alleine im Behandlungsraum sind, sollten auf keinen Fall freien Blick oder Zugriff auf einen Computermonitor haben.***
- ***Schützen Sie Büroräume, indem diese nur mit Code- oder Schlüsselkarten betreten werden können.***
- ***Geben Sie telefonisch oder per E-Mail keine Auskünfte, ohne Absicherung, dass der Adressat tatsächlich der Betroffene Patient oder anderweitig zur Einsicht in die Daten berechtigt ist.***
- ***Sprechen Sie über Testergebnisse von Patienten nicht am Empfangsbereich.***
- ***Auch an Versicherungen und andere Dritte dürfen Informationen aus der Patientenakte nicht automatisch weitergegeben werden. Hierfür muss in der Regel eine Einwilligungserklärung der oder des Betroffenen vorliegen.***
- ***Entsorgen Sie Patientenakten und alle Datenträger gemäß den Datenschutzbestimmungen.***
- ***Achten Sie auf die Fristen für die Aufbewahrung und Löschung von Gesundheitsdaten.***
- ***Informieren Sie sich bei Fragen zum Datenschutz bei Systemhäusern oder einem Datenschutzbeauftragten.***
- ***Die Kassenärztliche Bundesvereinigung hat im Dezember 2020 die Anforderungen zur Gewährleistung der IT- Sicherheit in Arztpraxen nach § 75b SGB V festgelegt. Darin genannt sind die Schutzziele, technische Anforderungen und das Mindestmaß der zu ergreifenden Maßnahmen.***

Stress als Security-Killer

Der Betrieb in der Arztpraxis muss laufen. Es gibt oft kaum Zeit für andere Dinge, die nicht unmittelbar mit dem Patienten und der Praxisorganisation zu tun haben. In besonders kritischen Phasen wie während der Corona-Pandemie bleibt gewissermaßen noch weniger, also eigentlich gar keine Zeit für andere Aufgaben. Genau dieser Sachverhalt ist leider auch Cyberkriminellen bekannt. Deshalb können die Mitarbeiter in einer digitalisierten Praxis besonders schnell und einfach zum Sicherheitsrisiko werden – ganz ohne böse Absicht.

Per E-Mail kommt ein besonders günstiges Angebot für Praxismaterial. Ein Mausklick auf die Preisliste – und schon folgt der „Lockdown“ für die Praxis! Als Dateianhang getarnte Ransomware legt in Sekundenschnelle alle Rechner lahm und verschlüsselt sämtliche Dateien. Meist folgt dann ein Erpresserschreiben, dass gegen Zahlung in Bitcoin die Herausgabe eines Passwortes verspricht, wodurch wieder der Normalbetrieb ermöglicht werden soll. In den meisten Fällen sollte man nicht darauf einzugehen, getreu dem Motto: Es gibt keine Verhandlungen mit kriminellen Erpressern. Wer bezahlt, finanziert die Arbeit von Cyberangreifern und erhält keine Garantie dafür, dass die Kriminellen den notwendigen, privaten Schlüssel wirklich zuschicken.

> »Die Fantasie und kriminelle Energie von Cyberkriminellen sollte man niemals unterschätzen, weshalb professionelle Schutzlösungen unerlässlich sind.
>
> Tim Berghoff,
> Security Evangelist bei G DATA

Bereits 2014 entdeckten Sicherheitsforscher die Schadsoftware Emotet. Sie zielte ursprünglich darauf ab, Passwörter für das Onlinebanking abzugreifen. Doch wie ein biologisches Virus mutierte auch das Computervirus Emotet immer weiter. Zuletzt konnten Angreifer immer weitere Schadsoftware nachladen und damit alle möglichen Inhalte von Computernetzwerken auslesen und manipulieren. Mit den Varianten TrickBot, QakBot und Ryuk war es Angreifern unter anderem möglich, Daten auszuspähen, Onlinebanking zu manipulieren oder Systeme zu verschlüsseln.

„Die Schadsoftware Emotet hat unter anderem das IT-System des Berliner Kammergerichts, des Uniklinikums Fürth und der Stadt Frankfurt lahmgelegt, vermutlich auch die Uni Gießen. Zwar ist sie seit einem international koordinierten Takedown vorerst lahmgelegt, aber Schadprogramme dieser Art wird es immer wieder geben“, warnt Berghoff.

IT-Sicherheit gehört dazu

Prävention alleine vermeidet zwar keine Angriffe auf die IT-Sicherheit. Doch wer die häufigsten Fehler vermeidet, reduziert die Risiken. Die wichtigste „Weiterbildungsregel“ für das gesamte Team sollte lauten: „Zum Wohle unserer Patienten und der Praxis gehört IT-Sicherheit ab jetzt auch zu unseren Aufgaben!“ Die bekannte Aussage „Das ist nicht mein Bereich!“ – sie gilt ab sofort nicht mehr! Es zahlt sich aus, wenn das gesamte Team über die „Fallstricke“ der Computerkriminellen Bescheid weiß und entsprechend umsichtig handelt.

Wichtig: Man muss wirklich kein IT-Spezialist sein. Ein paar „Basics“ tragen schon zu mehr Sicherheit bei:

Öffnen Sie niemals unbedacht E-Mail-Anhänge. Das gilt auch für Absender, die ihnen namentlich bekannt sind, denn E-Mails können manipuliert werden.

Klicken Sie Fehlermeldungen oder Updates des Betriebssystems nicht immer wieder weg. Laden Sie Updates von ihrem Betriebssystem oder ihrer wichtigsten Software kontinuierlich!

Datensicherung ist ein Muss. Erstellen Sie Backups regelmäßig – mindestens einmal täglich.

Notieren Sie Passwörter niemals – wirklich niemals! – dort, wo sie frei zugänglich sind. Wer keinen Passwortmanager (eine Software, die Passwörter verschlüsselt verwaltet) verwendet, sollte die wichtigsten PIN-Codes und Passworte wie Gold im Tresor aufbewahren.

Cyberkriminalität: Riesige Schäden

Machen Sie sich klar, dass eine „gehackte“ Praxis nicht nur für ein paar Stunden oder Tage komplett lahmlegt ist. Technische Geräte kann man reparieren oder ersetzen. Viel gravierender: Intime Patientendaten können in kriminelle Hände geraten. Das kann im Extremfall das Leben ihrer Patienten gefährden und das Renommee ihrer Praxis ruinieren! Stellen Sie sich nur einmal vor, dass am Abend alle wichtigen Nachrichtensendungen über einen entsprechenden Vorfall in ihrer Praxis berichten.

Wichtig ist: Sie können nicht alle IT-Schutzmaßnahmen selbst regeln. Arbeiten Sie deshalb mit G Data zusammen! Unsere Experten kennen sich mit dem Gesundheitsbereich und den hier geltenden Richtlinien nachweislich aus. Wir schützen Ihren Praxisbetrieb fortlaufend – während sich ihr Team auf seine Kernaufgaben konzentriert. Mit unserer cloud-basierten Managed Antivirus Software und einer fortlaufenden Überwachung und Administration Ihrer IT-Schutzkomponenten gewährleisten die G DATA Experten ein Höchstmaß an Sicherheit. Nach erfolgter Installation stellen wir sicher, dass Ihr Praxisbetrieb jederzeit geschützt ist und informieren Sie, falls von Ihrer Seite Handlungsbedarf besteht. So sparen Sie wertvolle Ressourcen, die Ihnen stattdessen voll im anspruchsvollen Praxisalltag zur Verfügung stehen.

Zusammenarbeit mit Experten

Lassen Sie Ihre IT-Systeme von Experten einrichten und passgenau konfigurieren sowie aus der Ferne überwachen. Informieren Sie bei Auffälligkeiten (Computer plötzlich „eingefroren“, Besuch eines „Servicetechnikers“, den niemand kennt) Ihren beauftragten IT-Spezialisten unverzüglich! Warten Sie nicht, bis nichts mehr geht!

Professionelles Sicherheits-management statt Softwarefrust

Staatlicherseits wird mit der Telematikinfrastruktur eine solide Basis geschaffen, um einen sicheren Austausch von Gesundheitsdaten zu ermöglichen. In vielen Fällen ist die Praxis-IT aber nicht auf die an der TI angeschlossenen Elemente beschränkt. Vom Telefonsystem bis hin zum vermeintlich privaten Tablet-PC, auf dem ausnahmsweise doch mal eine vertrauliche Information zur Bearbeitung landet, gilt es, alles im Blick zu behalten – und alles solide abzusichern.

Das gelingt nicht alleine mit der Telematikinfrastruktur. Nur mit einer Rundumlösung beschreiten Ärzte und Praxisteams den Königsweg. Mit G DATA 365 hat der Bochumer IT-Sicherheitsspezialisten G DATA genau die passende Lösung im Angebot.

Mit einem Modulkonzept, das kontinuierlich erweitert wird, legen sich Arztpraxen, MVZ, Pflegedienste und andere mittelständische Unternehmen im Gesundheitsbereich einen professionellen Schutz zu. Die gemanagte Lösung stellt ihre Praxis-IT sicher auf und macht sie verteidigungsfähig. Sämtliche Angriffsversuche werden von G DATA-Sicherheitsexperten sofort registriert, jede Modifikation ihrer Systeme proaktiv abgesichert. Die G DATA Security-Technologien sind im Hintergrund immer aktiv und funktionieren sogar dann, wenn einzelne Praxis-Rechner nicht online sind.

Die Experten von G DATA prüfen vorab, ob ihre Systeme den aktuellen Anforderungen entsprechen und wo es noch Verbesserungsbedarf gibt. Alle Systeme werden vorschriftsmäßig konfiguriert und in Betrieb genommen. Ab dann können Sie sich auf Sicherheit rund um die Uhr verlassen – an jedem Tag im Jahr. Bei Fragen steht ihnen jederzeit ein Ansprechpartner zur Verfügung. Nur ein solches, umfassendes Sicherheitsmanagement vermeidet gefährliche Sicherheitslücken und sorgt dabei für eine echte Entlastung im Team.

G DATA 365 kommt vom deutschen Cyber-Defense-Spezialisten G DATA. Vom Hauptsitz in Bochum aus koordinieren die rund 500 Mitarbeiter den Kampf gegen Cybercrime – rund um die Uhr an jedem Tag im Jahr. Das Unternehmen hat 1987 die erste Virenschutz-Software der Welt erfunden. Heute ist es ein führendes IT-Security-Unternehmen, das Unternehmen berät, Mitarbeiter in IT-Security schult, Schwachstellen in Netzwerken aufdeckt. G DATA bietet die beste Security Software mit KI-Technologien, die auch namhafte Konzerne vor Cybercrime und IT-Notfällen schützt. Als eines von nur wenigen Unternehmen in Deutschland ist das Tochterunternehmen G DATA Advanced Analytics GmbH vom BSI in die Liste qualifizierter APT-Response-Dienstleister aufgenommen worden, die hochentwickelte APT-Angriffe effektiv bekämpfen. Eine Art Ritterschlag.

Eine Publikation der

G DATA CyberDefense AG
G DATA Campus
Königsallee 178
D-44799 Bochum
Deutschland

Fotos: Adobe Stock