TELEMED @
Kommunikationslösungen

IT-SECURITY-GRUNDLAGEN

FÜR NIEDERGELASSENE ÄRZTE UND ZAHNÄRZTE

Synchronizing Healthcare

CGM CompuGroup Medical

INHALT

VORWORT

TELEMED @
Kommunikationslösungen

Die digitale Datenverarbeitung stellt äußerst hohe Anforderungen an die Sicherheit, vor allem dann, wenn es sich um die sensibelsten aller personenbezogenen Daten, die Gesundheitsdaten, handelt. Einzelne Patientendatensätze können auf den internationalen, digitalen Schwarzmärkten schnell einen vierstelligen Betrag einbringen. Was das für die Attraktivität auch kleinerer Praxen im niedergelassenen Bereich bedeutet, liegt auf der Hand. Hinzu kommt, dass spätestens seit der Einführung der Telematikinfrastruktur fast alle Praxen in Deutschland über einen Zugang zum Internet verfügen und somit zu potenziellen Zielen von Cyberkriminellen auf der ganzen Welt geworden sind. Als wäre das noch nicht genug, wachsen die Bedrohungen durch Internetkriminalität seit Jahren exponentiell an. Bereits heute werden Tag für Tag mehrere Hunderttausend neue Schadprogramme in Umlauf gebracht, und dabei geben sich die Kriminellen längst nicht mehr mit der Beschädigung von Computersystemen durch Viren zufrieden. Heute stehen Datendiebstahl und Erpressung im Fokus der Hacker. Die Folge sind häufig Praxisstillstand, hohe Lösegeldforderungen und meldepflichtige Datenschutzverstöße.

Im Zuge der voranschreitenden Digitalisierung des deutschen Gesundheitswesens hat der Gesetzgeber nun beschlossen, die IT-Sicherheit im niedergelassenen Bereich zu regulieren und konkrete Pflichtmaßnahmen zu benennen. Im „Digitale-Versorgung-Gesetz" wird der neue § 75b des SGB V beschrieben, welcher die Standesvertretungen im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) dazu verpflichtet, bis zum 30.06.2020 eine verbindliche Richtlinie für die „IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung" aufzustellen.

Um Sie als Leistungserbringer bestmöglich auf die kommende Richtlinie vorzubereiten, haben wir bei TELEMED, basierend auf unserer 25-jährigen Branchenerfahrung, dieses Whitepaper erstellt. Wir möchten Ihnen hiermit einen Ausblick geben, welche (Mindest-)Anforderungen auf Sie und Ihre Praxis zukommen, mit dem Ziel, dass Sie ein erstes Gefühl hierfür erhalten und bereits getroffene Maßnahmen besser einschätzen können.

Wichtig: Dieses Whitepaper ersetzt keineswegs die individuelle Risikoanalyse und -bewertung durch einen Fachmann vor Ort und erhebt auch keinen Anspruch auf Vollständigkeit hinsichtlich der kommenden Sicherheitsrichtlinie gemäß § 75b SGB V.

Ergänzend empfehlen wir Ihnen unbedingt auch die Lektüre und Umsetzung der Datenschutzempfehlungen Ihrer Standesvertretungen, der gematik sowie des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Insbesondere auch dann, wenn Sie planen, dieses äußerst wichtige Thema in Ihrer Praxis in Eigenregie umzusetzen.

Arthur Steinel,
General Manager TELEMED

1. SECURITY AWARENESS – RISIKOFAKTOR MENSCH

Ziel von Security-Awareness-Trainings ist es, sämtliche Praxismitarbeiter hinsichtlich der Risiken durch Schadsoftware und Co. zu sensibilisieren. Dabei wird praxisnah aufgezeigt, welcher Methoden sich Cyberkriminelle bedienen, damit die Angestellten potenzielle Bedrohungen kennen und erkennen und Risiken minimieren können. Der Effekt der Sensibilisierung hält allerdings nur eine gewisse Zeit lang an, sodass die Praxismitarbeiter anschließend wieder in ihre gewohnten Muster, z. B. bei der Bearbeitung von E-Mail-Anfragen, verfallen. Aus diesem Grund empfehlen sich regelmäßige Wiederholungen. Ein einmaliges Training ist mit Sicherheit gut für das Gewissen des verantwortlichen Praxisinhabers, bringt den gewünschten Erfolg aber nur temporär mit sich.

1.1 Regelmäßige Information

Um den positiven Effekt der Security-Awareness-Maßnahme aufrechtzuerhalten und zeitgleich effektiv und effizient über neue Bedrohungsmaßnahmen zu informieren, kann sich der Praxisinhaber beispielsweise der folgenden Tools bedienen und die so erhaltenen Informationen in planmäßigen oder außerplanmäßigen Teambesprechungen kommunizieren:

SOC (Security Operation Center)
Ein SOC ist ein Team bestehend aus Experten rund um die Themen IT und Security, welches aktiv an der Lösung von akuten Sicherheitsvorfällen arbeitet, aber auch über Sicherheitslücken und Bedrohungen informiert. Verschiedene SOCs bieten zu diesem Zweck Newsletter oder Informationsforen, mittels welcher sich Interessierte informieren (lassen) können.

RSS-Feed
Durch RSS (Really Simple Syndication) ist es möglich, schnell Informationsupdates von relevanten Websites zu erhalten. Diese können direkt in die gängigsten Mailprogramme (z. B. Microsoft Outlook) integriert und dort abgerufen werden.

Newsletter
Durch das Abonnieren von Newslettern, z. B. von Fachzeitschriften oder zuständigen Behörden, erhalten Interessierte regelmäßig Informationen über aktuelle Bedrohungen und Lösungsansätze.

Google Alerts
Mit Google Alerts ist es möglich, automatisiert Benachrichtigungen zu Inhaltsänderungen in der Suchmaschine Google zu erhalten. Diese können völlig individuell konfiguriert werden. Bei einem Alert für die Suchbegriffe „Sicherheitslücke" oder „Trojaner" wird bei jedem neuen Suchergebnis eine Benachrichtigung per E-Mail versandt. Dabei sollten die Suchbegriffe möglichst präzise formuliert werden.

1.2 Schulungsangebot

Das Schulungsangebot hinsichtlich Security Awareness ist sehr vielfältig. Wie so häufig kann auch hier online oder offline geschult werden. So können sich interessierte Praxen beispielsweise einen Trainer mit individuell gestaltetem Programm buchen oder ein angebotenes Präsenztraining besuchen. Online werden neben Webinar-Terminen häufig auch E-Learning-Plattformen für Security-Awareness-Trainings genutzt. Diese haben den Vorteil, dass Praxismitarbeiter zeitlich und räumlich unabhängig voneinander das Training absolvieren können. Nachteilig ist hingegen, dass bei dieser Trainingsform nicht individuell auf den Einzelnen und seine Fragen eingegangen wird, da es keinen Trainer, sondern nur vordefinierte Inhalte gibt.

1.3 Verhaltensregeln/Compliance

Um auch einen tatsächlichen Nutzen aus den Security-Awareness-Maßnahmen zu ziehen, ist es unerlässlich, einen Verhaltenskodex für den Umgang mit beruflich genutzter IT aufzustellen und vor allem auch dessen Umsetzung und Einhaltung zu kontrollieren. Reglementiert werden können dabei z. B. der Umgang mit E-Mails, die private Internetnutzung sowie die Nutzung privater Geräte (Smartphone etc.). Compliance ist hier vor allem auch Chefsache. Praxisinhaber sollten immer mit gutem Beispiel vorangehen, um ein entsprechendes Signal an die Belegschaft zu senden.

1.4 Passwörter

Sichere Passwörter und der Umgang mit diesen ist ein wesentlicher Bestandteil des Sicherheitskonzepts für niedergelassene Ärzte und Zahnärzte. Für die Wahl des Passwortes ist es wichtig zu verstehen, wie Passwörter i. d. R. „geknackt" bzw. herausgefunden werden:

Durch Ablesen:
Eine weit verbreitete Methode zum Merken von Passwörtern ist, diese einfach aufzuschreiben. Verschlossen, in einem Tresor o. Ä., ist dies auch legitim, allerdings werden die Passwörter häufig auch an den Bildschirm geklebt, unter die Tastatur gelegt oder in der nahegelegenen Schublade aufbewahrt. Also genau dort, wo jemand mit krimineller Energie zuerst nachsehen würde.

Durch Ausprobieren/Erraten:
Die gängigsten (und somit unsichersten) Passwörter in Deutschland werden jedes Jahr im Internet veröffentlicht. Darunter fallen z. B. die Zahlenfolgen „123456" und „123456789" oder das Wort „hallo". Bei den niedergelassenen (Zahn-)Ärzten sind bekannterweise Passwörter wie „praxis", „behandlung" oder schlicht der Name der Praxisverwaltungssoftware beliebt.

Durch Brute-Force-Attacken:
Hierbei werden durch Software-Programme in kürzester Zeit alle möglichen Passwortkombinationen ausprobiert. Die Software testet dabei zuerst die gängigsten Passwörter und anschließend verschiedene Varianten von diesen, wie z. B. „Pa$$wort" anstatt „Passwort".

Durch Verwenden der immer gleichen Passwörter:
Viele Nutzer neigen dazu, ein Passwort, das als sicher erachtet wird, für alle Anmeldungen/Dienste zu nutzen. Das Problem – auch bei einem wirklich guten Passwort – ist, dass sich die Cyberkriminellen dessen bewusst sind.

Aus diesen Informationen ergeben sich die folgenden Grundlagen für den Umgang mit Passwörtern:

- Passwörter dürfen sich nicht aus dem Kontext „erraten" lassen (Beispiel „praxis"). Dasselbe gilt natürlich auch für Passwörter mit Bezug zur Person, wie z. B. Geburtsdaten o. Ä.
- Passwörter müssen möglichst lang sein: Zwar kann mittels Brute-Force-Methode jedes Passwort ermittelt werden, aber bei entsprechender Länge (z. B. zehn Zeichen, Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen) dauert die Entschlüsselung nach heutigem Stand der Technik immerhin noch ein paar Hundert Jahre. Bei acht Zeichen sind es übrigens nur etwa 24 Tage.
- Es sollten verschiedene Passwörter für verschiedene Dienste gewählt werden.
- Passwörter müssen sich gut merken lassen, damit nicht die Notwendigkeit besteht, diese irgendwo zu notieren. Dies lässt sich beispielsweise über Eselsbrücken realisieren.

Übrigens: Regelmäßiges Ändern von Passwörtern wird mittlerweile nicht mehr empfohlen, da Nutzer, die zu einer regelmäßigen Änderung gezwungen werden, dazu neigen, eher simple Kennwörter zu vergeben, welche wiederum leichte Beute für die entsprechenden Programme sind.

Es gibt aber auch Fälle, in welchen der Passwortwechsel unerlässlich ist:

- nach dem Ausscheiden von Mitarbeitern (siehe auch Punkt „Rollen und Rechte")
- nach einer Cyberattacke, da die Gefahr besteht, dass Passwörter kompromittiert wurden

1.5 Vergabe von Rollen und Rechten

Die Vergabe von Rollen und Rechten für die Nutzung der Praxis-IT sollte restriktiv erfolgen, getreu dem Motto „so viel wie nötig, so wenig wie möglich".

Immer wieder arbeiten sämtliche Praxismitarbeiter mit ein- und demselben Benutzerkonto und dabei i. d. R. auch noch mit vollen Administrationsrechten. Hier muss eine strikte Trennung erfolgen, normale Tätigkeiten im Praxisalltag dürfen nicht mit Administratorenrechten ausgeführt werden. So kann beispielsweise verhindert werden, dass Mitarbeiter unbedacht vermeintlich harmlose Software auf den Praxis-Computern installieren, welche sich zu einem späteren Zeitpunkt als Spyware entpuppt und einen meldepflichtigen Datenschutzverstoß erzeugt. Jeder Mitarbeiter sollte also nur die Rechte erhalten, die er auch wirklich benötigt. Bei der Trennung von Benutzerkonten ist auch zwingend darauf zu achten, die Konten von ausgeschiedenen Mitarbeitern zu löschen.

1.6 Umgang mit Datenträgern

Mit Datenträgern unbekannten Ursprungs muss vorsichtig umgegangen werden, da diese potenziell Schadsoftware enthalten können. Immer wieder werden infizierte USB-Sticks, DVDs und Co. absichtlich im Umfeld von Unternehmen platziert, in der Hoffnung, dass irgendjemand diese mit dem Firmennetzwerk verbindet. Es ist aber auch durchaus möglich, dass von Patienten oder Kollegen ausgehändigte Datenträger, z. B. Röntgenaufnahmen, infiziert sind. Um das Risiko möglichst gering zu halten, empfiehlt es sich, im Rahmen des Rollen- und Rechtekonzepts (siehe Punkt 1.5) auch die Nutzung von USB-Sticks und anderen Datenträgern durch den Administrator einzuschränken.

1.7 Umgang mit E-Mails

Die E-Mail gehört zu den beliebtesten Instrumenten von Internetkriminellen. Kein Wunder also, dass in den vergangenen Jahren E-Mails immer wieder im Zusammenhang mit Angriffen auf das Gesundheitswesen genannt wurden. Das Angriffsmittel „E-Mail" wird dabei aber nicht immer gleich eingesetzt, denn eine E-Mail kann auf verschiedene Arten für niedergelassene Ärzte und Zahnärzte gefährlich werden. Folgende Varianten können beispielsweise auftreten:

1.7.1 Phishing-E-Mails:

Das Ziel von Phishing-Attacken ist der Diebstahl von Informationen bzw. Identitäten. Zu diesem Zweck erstellt der Angreifer gefälschte E-Mails und Websites, z. B. von Banken, Energieversorgern und Telekommunikationsunternehmen. Häufig wird der Empfänger darin unter irgendeinem fadenscheinigen Vorwand aufgefordert, seine Daten, wie z. B. Zahlungsinformationen, zu verifizieren. Dabei spielen die Kriminellen auch häufig mit der Angst, indem sie beispielsweise damit drohen, dass Dienste abgeschaltet werden, wenn nicht sofort reagiert wird.

Auf diese Weise erbeutete Informationen setzen die Kriminellen dann entweder ein, um sich direkt daran zu bereichern, verkaufen die Daten an andere oder nutzen sie selbst als Mittel zum Zweck für weitere kriminelle Aktivitäten.

Die große Masse der Phishing-E-Mails im Umlauf ist dabei nicht maßgeschneidert für eine bestimmte Person. Vielmehr werden die wahrscheinlichsten Szenarien genutzt, d. h. die fingierten E-Mails werden häufig im Namen des Marktführers der jeweiligen Branche verschickt, da hier die Wahrscheinlichkeit, dass sich jemand angesprochen fühlt, am größten ist. Phishing-E-Mails haben sich in der Vergangenheit häufig durch zweifelhafte Grammatik und Rechtschreibung ausgezeichnet. Leider ist dies heutzutage kein geeigneter Indikator mehr, da der Großteil der Inhalte perfekt formuliert und auch grafisch aufbereitet ist.

Maßgeschneiderte, personenbezogene Phishing-Attacken existieren natürlich auch, wobei die Cyberkriminellen hier grundsätzlich auf das Verhältnis von Aufwand und Nutzen achten. Diese Art des Angriffs wird Whaling genannt.

Achtung: Eine Datenbank mit mehreren Tausend Patientendatensätzen kann durchaus ein attraktives Ziel darstellen und den Aufwand einer maßgeschneiderten Attacke rechtfertigen.

1.7.2 Spam-E-Mails:

Bei Spam-E-Mails handelt es sich bei um Massenmails, die dem Empfänger unaufgefordert zugestellt werden und i. d. R. Werbebotschaften und dubiose Angebote transportieren. Spam-E-Mails werden dabei vom Empfänger oft hauptsächlich als nervig angesehen. Es geht aber auch eine reale Gefahr von ihnen aus, denn oft versteckt sich in Anhängen und/oder Links eine Schadsoftware, die im schlimmsten Fall den kompletten Praxisbetrieb lahmlegen und durch den Abgang von Patientendaten für einen Datenschutzverstoß sorgen kann.

1.7.3 Es gibt viele Wege, auf denen E-Mail-Adressen in die Hände von Cyberkriminellen gelangen:

- **Erratene E-Mail-Adressen:** Ein Großteil der E-Mail-Adressen wird erraten, da es E-Mail-Adressen gibt, die bei nahezu jeder Domain vorhanden sind, wie z. B. postmaster@wunschname.de oder info@wunschname.de
- **Harvester (deutsch: Erntemaschine):** Hierbei handelt es sich um kleine Programme, die Websites gezielt nach E-Mail-Adressen durchsuchen, z. B. aus Gästebucheinträgen oder dem Impressum von Websites.
- **Gewinnspiele:** Gewinnspiele, z. B. in Einkaufszentren, auf der Straße, in der Zeitung oder im Internet, eigenen sich hervorragend zum Sammeln von E-Mail-Adressen. Seien Sie sich dessen bewusst und achten Sie daher auf das Kleingedruckte auf Gewinnspielkarten.
- **Adress-Händler:** Adressdaten, u. a. auch E-Mail-Adressen, können auch von Adress-Händlern gekauft werden. Adressdaten werden von Firmen rechtmäßig aufgekauft und an Firmen für Werbezwecke weiterverkauft. Neben den rechtmäßig zum Verkauf stehenden Adressen gibt es auch die Möglichkeit, Adressen über einen digitalen Schwarzmarkt (häufig im sogenannten Darknet) zu erwerben. Dort können dann Adressdatenbanken erworben werden, die zuvor gestohlen wurden.
- **Diebstahl:** Anstatt gestohlene E-Mail-Adressen zu kaufen, kann ein Cyberkrimineller auch selbst stehlen. So können beispielsweise gestohlene Kontaktdaten von Patienten für weitere kriminelle Aktivitäten des Angreifers genutzt werden.

1.7.4 Geeignete Maßnahmen zur Risikoreduktion

Think before you click

Das ist ein Grundsatz, der zum Schutz der Praxis-IT nicht nur bei der E-Mail-Bearbeitung Beachtung finden sollte. Bevor E-Mails, Links und Anhänge angeklickt werden, sollte erst nachgedacht und bewertet werden. Oft kann man so unplausible Inhalte und Logikfehler identifizieren, welche auf Spam, Phishing und Co. hinweisen. Im Zweifel empfiehlt es sich, den vermeintlichen Absender einfach anzurufen und die Authentizität der E-Mail verifizieren zu lassen. Grundsätzlich gilt es, niemals vertrauliche Daten preiszugeben, wenn die Identität des Empfängers nicht eindeutig geklärt ist.

Konfiguration von Filtern

Viele E-Mail-Programme bieten Filter für Spam und Co. an. Diese sind häufig bereits vorkonfiguriert, können aber durch die Mitarbeit des Praxispersonals dazulernen, indem nicht erkannte Spam- und Phishing-Mails manuell als solche deklariert werden. Auch können ganze Absenderadressen blockiert bzw. ausgefiltert werden.

Einsatz von Hilfsmitteln

Häufig bringen moderne (Hardware-)Firewalls und Anti-Virus-Programme auch Tools zur Erkennung und Vermeidung von E-Mail-Bedrohungen mit, wie z. B. Spam-Filter, die mit künstlicher Intelligenz arbeiten. Zudem gibt es E-Mail-Provider und Dienste, die beispielsweise E-Mails durchleuchten und vorfiltern, bevor diese überhaupt auf den Mailserver geleitet werden.

Keine private E-Mail-Nutzung

Um das Risiko zu reduzieren, ist es sinnvoll, innerhalb des Praxisnetzwerks die private Nutzung von E-Mails einzuschränken oder idealerweise generell zu verbieten. Der Abruf von E-Mails mit privaten Geräten, wie z. B. Smartphones, sollte daher, wenn überhaupt nur über getrennte Bereiche des Netzwerks erfolgen, beispielsweise über ein Gast-WLAN.

2. TELEMATIKINFRASTRUKTUR

Durch die Einführung der Telematikinfrastruktur (TI) ist es für die niedergelassenen Ärzte und Zahnärzte in Deutschland fast unmöglich, ohne eine Internetverbindung auszukommen. All diejenigen, die bereits zuvor eine Verbindung mit dem Internet genutzt haben, sind nach der Anbindung an die TI genauso sicher online wie vorher. Vielmehr konnte gerade im Rahmen des großflächigen TI-Rollouts festgestellt werden, dass Cybersecurity im niedergelassenen Bereich bisher grundsätzlich eine eher untergeordnete Rolle spielt.

2.1 Serieller Betrieb

Diese Betriebsart zeichnet sich dadurch aus, dass sämtliche Netzwerkkomponenten hinter dem Konnektor installiert werden und somit jede Verbindung in und aus der Praxis zwangsläufig durch diesen hindurchgeleitet werden muss. Ohne die Aktivierung des sogenannten Secure Internet Service (SIS) kann keine Verbindung zum Internet aufgebaut werden, sondern lediglich die Verbindung in das Netz der Telematikinfrastruktur. Praxen, die keine Internetnutzung wünschen, können diese aber auch mit jeder anderen (klassischen) Firewall (vgl. Punkt 4) sperren.

Ist der Zugang zum Internet gewünscht, bietet die Nutzung der Firewall des Konnektors in Verbindung mit dem SIS zusätzlichen Schutz für die Praxis. Dieser ist aber alleine nicht ausreichend und ersetzt nicht die seitens Praxis zu ergreifenden technischen und organisatorischen Maßnahmen, da die gängigsten Bedrohungen wie beispielsweise E-Mails mit schadhaften Anhängen (siehe auch Punkt 4) nicht blockiert werden.

Bei der individuellen Entscheidungsfindung hinsichtlich des geeigneten Anschlussszenarios für die Telematikinfrastruktur sollte zudem berücksichtigt werden, dass eine serielle Installation Einschränkungen bei Laboranbindungen, Heimarbeitslösungen und auch der Internet-Telefonie mit sich bringen kann. Dies bedeutet vor allem für bestehende Netzwerke oft einen aufwendigen Umbau.

2.2 Paralleler Betrieb

Charakteristisch für den parallelen TI-Betrieb ist, dass der Konnektor gleichberechtigt mit den anderen Netzwerkkomponenten an einen Router oder Switch angeschlossen wird. Somit ist dieser dem Netzwerk nicht vorgeschaltet, was dazu führt, dass die integrierte Firewall nicht wirksam gegen Zugriffe von außen schützen kann. In diesem Fall sollte eine eigenständige Firewall installiert werden, um vor unerwünschten Zugriffen von außen zu schützen. Vorteil gegenüber der Nutzung der integrierten Firewall ist, dass die Nachteile des seriellen Betriebs nicht auftreten, da die Firewall individuell konfiguriert werden kann.

Seitens der gematik wird der parallele Betrieb nur für diejenigen Praxen empfohlen, welche mit Sicherheitsfunktionen gemäß den Standards des Bundesamtes für Sicherheit in der Informationstechnik ausgestattet sind. Um dieser Empfehlung nachzukommen, sollten Leistungserbringer hinsichtlich der Wahl des richtigen Firewall-Produktes die unter Punkt 4 dargestellten Informationen beachten.

3. VIRENSCHUTZ

Anti-Virus-Software hat primär die Aufgabe, die Praxiscomputer vor sogenannten Infektionen zu schützen. Wie auch in der Medizin steht hier die Prävention an erster Stelle. Um aber auch wirklich wirksam Prävention betreiben zu können, ist es notwendig, beim Virenschutz auf moderne und intelligente Software zu setzen, da der klassische Virenschutz vor allem auch im Gesundheitswesen nicht mehr ausreichend vor den vielfältigen Bedrohungen schützt.

Der klassische Virenschutz arbeitet mit einer großen Datenbank von Virensignaturen, die immer wieder aktualisiert wird. Erlangt der Hersteller also Kenntnis über eine neue Schaddatei, fügt er die Signatur seiner Datenbank hinzu und stellt den Nutzern ein Update bereit. Das Problem mit dieser Vorgehensweise besteht darin, dass es täglich mehrere Hunderttausend neue Virensignaturen gibt, Tendenz steigend, und kein Hersteller diese alle rechtzeitig identifizieren und per Aktualisierung an die jeweiligen Nutzer verteilen kann. Gleichzeitig werden Schadprogramme immer raffinierter, so gibt es beispielsweise immer mehr „dateilose Angriffe", die ihren Schadcode dort verstecken, wo er von herkömmlichen Lösungen nicht gefunden werden kann, z. B. im Arbeitsspeicher.

Daher empfiehlt sich der Einsatz von integrierten EDR-Lösungen (Endpoint Detection and Response) anstatt einer reinen, klassischen EPP-Lösung (Endpoint Protection Platform). EDR-Lösungen klassifizieren sämtliche Prozesse des Computers, nutzen Verhaltensanalysen, alarmieren und schreiten in Kombination mit der integrierten EPP-Lösung ein, um Schaden zu verhindern.

4. FIREWALL

Mittels einer Firewall kann z. B. der Datenverkehr über das Internet reguliert werden. Dabei ist vor allem die klassische Firewall zwingend abhängig vom Hinterlegen eines gut durchdachten Regelwerks durch einen Fachmann. Ziel dieses Regelwerks, der sogenannten Policy, ist es, nur wirklich benötigte Verbindungen zum Internet zuzulassen, wobei zwischen eingehenden und ausgehenden Verbindungen unterschieden wird. Eine Firewall kann also als eine Art Türsteher zwischen dem Praxisnetzwerk und dem Internet verstanden werden, der auch den Einlass nach zuvor definierten Regeln steuert.

Auf den Einsatz einer reinen Software-Firewall sollte vor allem im Gesundheitswesen verzichtet werden, da diese nur den jeweilen PC schützt und vor allem bei einem unzureichenden Rechtekonzept (siehe Punkt 1.5) einfach von Mitarbeitern umgangen werden kann. Eine dedizierte Hardware-Firewall hingegen schützt sämtliche Geräte im Netzwerk, einschließlich medizinischer Geräte wie Röntgen, Ultraschall und Co., vor unbefugtem Zugriff.

Bei Neuanschaffung einer Firewall sollte darauf geachtet werden, dass es sich um eine Next Generation Firewall oder auch sogenanntes UTM (Unified Threat Management) handelt, da diese zusätzlichen Schutz bieten. Diese Geräte weisen gemäß der aufgestellten Regeln unerwünschten Datenverkehr ab und untersuchen den erlaubten Datenverkehr, z. B. für die Nutzung von E-Mail-Diensten oder den Zugriff auf die K(Z)V-Website, auf Bedrohungen, z. B. mittels des sogenannten Sandboxing-Verfahrens. Vor allem interessant sind Geräte mit integriertem IPS (Intrusion Prevention System), da diese in der Lage sind, Angriffe auf Sicherheitslücken im Praxisnetzwerk zu identifizieren und abzuwehren.

Wichtig bei dem Einsatz von Firewallsystemen, wie auch bei jedem IT-Security-Baustein, ist die regelmäßige Pflege und Anpassung der Firewall an neue Bedrohungsszenarien. Hier ist insbesondere aufgrund der sensiblen Daten im Gesundheitswesen die Nutzung eines Managed Services empfehlenswert. *Mehr zu Managed IT-Security unter Punkt 6.*

5. UPDATES VON SOFTWARE

Bzgl. des Updatens von Anwendungen und Betriebssystem halten es viele mit dem altenbekannten Vorsatz „never change a running system", und ja, es kommt immer wieder vor, dass sich mit einem Update, das eigentlich Verbesserungen und/oder zusätzliche Features bringen sollte, neue Fehler einschleichen. Dennoch muss zwingend davon abgeraten werden, Software nicht zu aktualisieren, nur weil sie auch ohne Update alles tut, was man von ihr erwartet. Der Grund hierfür liegt in den Sicherheitsaktualisierungen, die mit den Updates eingespielt werden. Hersteller entdecken immer wieder Lücken in Ihren Systemen, die sich die Internetkriminellen zu Nutze machen. Daher kann eine ungepatchte Software zwar durchaus auch über einen längeren Zeitraum funktionieren, stellt aber u. U. ein permanentes Sicherheitsrisiko dar. Auf den Einsatz von Software, die am Ende ihres Lebenszyklus' angelangt ist und aus diesem Grund nie wieder Sicherheitsupdates erfahren wird, sollte daher gänzlich verzichtet werden. Aktuelles Beispiel ist das Betriebssystem Windows 7 von Microsoft.

Für den Umgang mit Updates können beispielsweise folgende Lösungen herangezogen werden:

- Automatische Updates: Viele Programme bieten die Möglichkeit, Updates automatisiert in einem bestimmten Turnus zu suchen und zu installieren. Vorteil ist, dass immer die sicherste Version genutzt wird. Nachteil ist, dass diese Version nicht zwingend auch die beste ist was die Funktionalität angeht und dass Updates u. U. den Betriebsablauf stören.
- Patchmanagement-Software: Mittels solcher Software kann i. d. R. für alle gängigen Programme eine individuelle Updateroutine nach Nutzerwunsch konfiguriert werden. Dabei kann bestimmt werden, welche Programme wann welche Updates erhalten. So kann beispielsweise definiert werden, dass alle sicherheitskritischen Updates für Windows täglich automatisiert um 20:00 Uhr eingespielt werden und sämtliche anderen Updates zuvor vom Administrator bestätigt werden müssen.

Im Gesundheitswesen kann immer wieder beobachtet werden, dass die Zulassungen für Medizingeräte an alte Softwarestände, die keine Sicherheitsupdates erhalten, gekoppelt sind. Da auf diesen Systemen i. d. R. aber sensible Patientendaten in irgendeiner Art und Weise verarbeitet, zwischengespeichert usw. werden, sollten diese Geräte sinnvoll vom restlichen Praxisnetzwerk getrennt werden, z. B. über eine Firewall mit den entsprechenden Beschränkungen für die Netzwerkkommunikation. Sinnvoll kann zudem die Anschaffung eines IPS (Intrusion Prevention System) sein. Dieses dient zum einen der Erkennung von Cyberattacken und kann diese zum anderen auch selbstständig abwehren, sodass Angriffe auf ungepatchte Systeme unterbunden werden können.

6. MANAGED IT-SECURITY

Sicherheitsmaßnahmen für die Praxis-IT gehören nicht zu den Dingen, die einmalig angeschafft und dann abgenutzt werden können. Da der ständige, unaufhaltsame, technologische Fortschritt immer auch auf der Seite der Internetkriminellen stattfindet, besteht die zwingende Notwendigkeit, nicht nur ein Sicherheitskonzept aufzustellen und zu implementieren, sondern dieses auch permanent weiterzuentwickeln und anzupassen. Eine Aufgabe, der die meisten Praxisinhaber schon alleine aus Zeitgründen nicht gewachsen sind, da die Praxis sich auf ihre Kernkompetenz konzentrieren muss – die Gesunderhaltung des Menschen.

Eine Alternative ist die turnusmäßige Kontrolle der Komponenten durch einen IT-Dienstleister, allerdings wird auch diese Variante häufig nicht der Dynamik der IT-Branche gerecht. Aus diesem Grund haben sich in den vergangenen Jahren immer mehr sogenannte Managed Service Provider (MSP) entwickelt. Dabei handelt es sich um IT-Dienstleister, die nicht nur auf Zuruf arbeiten oder gemäß eines Wartungsvertrags einmal jährlich gebuchte Leistungen erbringen, sondern um solche, die proaktiv die gesamte Praxis-IT oder Teile davon überwachen und instand halten. Dieses Vorgehen hilft dabei, Ausfälle der IT zu vermeiden, anstatt sie einfach nur schnellstmöglich wiederherzustellen. I. d. R. bieten diese MSP auch Managed-Security-Lösungen an und tragen damit Sorge, dass die Komponenten des Sicherheitskonzepts stets auf dem bestmöglichen Stand sind.

7. CYBERVERSICHERUNGEN

Sinn und Zwecks einer Cyberversicherung ist es, den Versicherungsnehmer vor den finanziellen Folgen eines eingetretenen Falles zu bewahren. Abgesichert werden können verschiedene Risiken für die Praxis-IT, wie z. B. der Befall mit Schadsoftware, Bedienfehler oder Ausfall der IT. Bei Eintritt eines Schadens werden dann, je nach Versicherungsvertrag, die Kosten für Datenrettung, Wiederherstellung, IT-Forensik, Patientenkommunikation und weitere Kostenfaktoren wie Rechtsberatung übernommen. Manche Versicherer kompensieren auch entgangene Umsätze durch die Betriebsunterbrechung. Zudem stellen die meisten Versicherungsunternehmen spezielle Hotlines zur Verfügung, die bei einem IT-Notfall schnell erste Hilfe leisten können.

Bei der Wahl der richtigen Cyberversicherung sollte genau hingesehen werden, da nicht alle Anbieter z. B. auch Schadenersatzansprüche von Dritten, die häufig bei Datenschutzvorfällen zum Tragen kommen, kompensieren oder Bußgelder für DSGVO-Verstöße im Zusammenhang mit der genutzten Praxis-IT übernehmen.

Auch darf eine Cyberversicherung, die alle Arten von Schäden abdeckt, nicht als Ersatz für IT-Sicherheitsmaßnahmen betrachtet werden, da

1. i. d. R. ein gewisses Maß an IT-Sicherheit Voraussetzung für das Zustandekommen des Versicherungsvertrags ist.
2. der Versicherer bei (grob) fahrlässigem Handeln die Zahlung verweigern kann.
3. temporäre oder dauerhafte Umsatzeinbußen durch Imageschäden im Zusammenhang mit Datenschutzvorfällen (z. B. durch einen Trojaner) entstehen können, die nicht durch eine Versicherungspolice abgedeckt werden.

Aus diesen Gründen wird empfohlen, vorrangig in gut aufeinander abgestimmte IT-Security-Komponenten zu investieren und das eigene Sicherheitskonzept im Bedarfsfall mittels einer Cyberversicherung abzurunden.

8. NOTFALLPLAN

Unabhängig von den getroffenen Vorkehrungen ist es unmöglich, von einer hundertprozentigen Sicherheit für die Praxis-IT zu sprechen. Daher ist es zwingend notwendig, Verhaltensregeln für den Umgang mit akuten Sicherheitsproblemen, aber auch für den begründeten Verdacht aufzustellen. Ziel ist es, bei plötzlich eintretenden IT-Notfällen Schaden für Praxis und Patienten abzuwenden oder zumindest bestmöglich zu begrenzen. Idealerweise werden alle Praxismitarbeiter hinsichtlich der Inhalte und der Einhaltung des Notfallplanes unterwiesen. Zudem sollte der Notfallplan für alle Mitarbeiter zugänglich ausgehängt werden, damit diese sich im Fall der Fälle an diesem Protokoll orientieren können. Bei einem sicherheitsrelevanten Vorfall kommt es in erster Linie auf Geschwindigkeit an, daher sollte der Plan Sofortmaßnahmen enthalten, die dazu geeignet sind, von jeder beliebigen Person eingeleitet zu werden – z. B. das Trennen der Internetverbindung durch Ziehen des Steckers, um (weiteren) Datenabgang zu verhindern.

Es ist wenig hilfreich, wenn der Plan zwar geeignete Sofortmaßnahmen enthält, diese aber einen Abschluss in Informatik voraussetzen. Ein weiterer wichtiger Punkt ist die Benennung von Ansprechpartnern inklusive deren Kontaktdaten, z. B. die des betreuenden IT-Dienstleisters. Dieser sollte auch, Eignung vorausgesetzt, für die Aufstellung des Notfallplans herangezogen und in diesen eingebunden werden. Dabei ist darauf zu achten, dass der Dienstleister auch entsprechende Reaktionszeiten (Service-Level) garantiert, da niemandem geholfen ist, wenn der IT-Dienstleister im Notfall erst Tage später reagiert. Reaktionszeiten und Leistungsumfänge lassen sich i. d. R. über sogenannte Serviceverträge regeln. Verantwortliche in den Praxen sollten aber mit Blick auf die äußerst sensiblen Daten neben dem IT-Dienstleister vor Ort auch über die Zusammenarbeit mit einem Managed Service Provider (MSP) nachdenken (siehe auch Punkt 6). Diese verfügen oft über spezielle Services oder qualifiziertes Personal für Security-Notfälle und können häufig schneller reagieren, da durch permanente Überwachung benötigte Informationen schneller zur Verfügung stehen.

9. WICHTIGE QUELLEN ZUM DATENSCHUTZ UND DATENSICHERHEIT FÜR NIEDERGELASSENE ÄRZTE UND ZAHNÄRZTE

Bundeszahnärztekammer / Kassenzahnärztliche Bundesvereinigung:
Rechtsgrundlagen und Hinweise für die Zahnarztpraxis – Datenschutz- und Datensicherheitsleitfaden für die Zahnarztpraxis-EDV:

www.kzbv.de/datenschutzleitfaden-bzaek-kzbv-2018.download.64ca6801b44abc59fb0f9b2f70f77617.pdf

Bundesärztekammer / Kassenärztliche Bundesvereinigung:
Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis:

www.kbv.de/media/sp/Empfehlungen_aerztliche_Schweigepflicht_Datenschutz.pdf

BSI:
Allgemeines zum Thema Informationssicherheit:

www.bsi-fuer-buerger.de

IT-Grundschutz-Kompendium:
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.pdf;jsessionid=26380ADCAD05CF47C7DC856ACD29FD42.1_cid351?__blob=publicationFile&v=6

gematik:

Whitepaper Datenschutz und Informationssicherheit in der Telematikinfrastruktur:
www.gematik.de/fileadmin/user_upload/gematik/files/Publikationen/gematik_Whitepaper_Datenschutz_und_Informationssicherheit.pdf

Anschluss medizinischer Einrichtungen an die Telematikinfrastruktur – ein Überblick für Dienstleister vor Ort:
https://fachportal.gematik.de/fileadmin/user_upload/fachportal/files/Service/Pruefkarten gemInfo_Anschluss_TI_DVO_V2.1.0.pdf

IT-Sicherheitsrichtlinie:

SGB V § 75b – Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung:
www.gesetze-im-internet.de/sgb_5/__75b.html

TELEMED @

Kommunikationslösungen

#fightcybercrime

GEMEINSAM FÜR MEHR IT-SICHERHEIT IM DEUTSCHEN GESUNDHEITSWESEN.

CompuGroup Medical Deutschland AG
Geschäftsbereich TELEMED
Maria Trost 21 | 56070 Koblenz
T +49 (0) 261 8000-2007
F +49 (0) 261 8000-2029
info@telemed.de

cgm.com/telemed

CGMCOM-11044_TEL_0620_SWI

Synchronizing Healthcare

CompuGroup Medical