Digitale Erpressung – eine reale Gefahr für die Praxis?

„Bei all meinen Beratungsmandaten habe ich nirgends eine dramatischere Bedrohung der wirtschaftlichen Existenz gesehen". So machte uns zm-Kolumnist Christian Henrici auf reale Fälle aufmerksam, die man üblicherweise nicht in der Welt der Zahnarztpraxen vermuten würde: Erpressung via Krypto-Ransomware, die die Praxissoftware verschlüsselt und die Daten dem Zugriff entzieht. Dass es sich bei Cybercrime nicht nur um eine theoretische Gefahr handelt, soll diese Titelgeschichte deutlich machen.

? Herr Henrici, Ransomware-Angriffe legen momentan viele Unternehmen – auch Zahnarztpraxen – lahm. Mithilfe dieser Erpressungstrojaner verschlüsseln Hacker den gesamten Datenbestand im Praxisnetzwerk und geben ihn erst gegen eine Lösegeldzahlung wieder frei. Wie wurden Sie mit diesem Thema konfrontiert?

Christian Henrici: Der hier beschriebene Fall eines Zahnarztes war der erste, der mir in diesem Maße so konkret bekannt wurde und mich dazu veranlasste, mich intensiver mit dem Thema Datenschutz und -sicherheit und der sich daraus ergebenen Kriminalisierung zu beschäftigen. Bislang war auch für mich „Sicherheit" ein Thema, das ich in fachkundigen Händen zu wissen glaubte und von dem ich dachte, mich damit nicht tiefergehend auseinandersetzen zu müssen. Ich wurde eines Besseren belehrt.

? Was ist passiert?

Im vierten Quartal vergangenen Jahres erfuhr ich von zahlreichen Fällen, in denen Zahnarzt- und Arztpraxen Opfer von Cybercrime, Datenklau und Daten-Kidnapping wurden. So unterschiedlich die Praxen auch sein mögen – eines haben sie gemeinsam: die Scheu, über ihre Fälle zu sprechen.

? Scheu? Weshalb?

Ausschlaggebend sind meines Erachtens zwei Gründe: erstens die Angst vor einem Revancheakt der Täter. Zweitens die Angst, öffentlich vom Opfer zum Täter gemacht zu werden, weil der Praxisinhaber für die Datenerfassung, -haltung und -sicherheit verantwortlich ist. Insbesondere dafür, dass mit diesen Daten vernünftig und sorgsam umgegangen wird und dass er alles in seiner Macht Stehende tut, um diese Daten zu schützen. Sollten dennoch Daten gekapert werden, besteht aufseiten des Praxisinhabers eine Fürsorgepflicht, die unrechtmäßige Kenntniserlangung von Daten durch Dritte unverzüglich der Aufsichtsbehörde sowie den Patienten und Kunden zu melden.

? Zu welchem Zeitpunkt muss der Praxisinhaber die Betroffenen denn informieren?

Die Benachrichtigung muss erfolgen, sobald angemessene Maßnahmen zur Datensicherung ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird (vgl. § 42a BDSG). „Unverzüglich" ist zwar ein dehnbarer Begriff, verdeutlicht aber die Ernsthaftigkeit, die dem Thema von behördlicher Seite gewidmet wird.

Vor diesem Hintergrund bin ich sehr dankbar, dass Dr. Michael Kann, ein Zahnarzt mit ausgeprägter IT-Affinität, sich stellvertretend für viele Kollegen bereit erklärt hat, mit mir über das Thema zu reden.

Das Fazit seiner bisherigen Erfahrungen mündet in einem klaren Appell an alle Praxisinhaber: Um die Praxis-, Patienten- und auch Mitarbeiterdaten zu sichern und sich vor hohen Kosten durch Arbeitsausfälle und/oder Lösegeldzahlungen zu schützen, sollte sich jede Praxis rechtzeitig mit den notwendigen Maßnahmen des Datenschutzes und der Datensicherheit auseinandersetzen.

? Das heißt im Klartext?

Im Klartext heißt das: Sind zum Beispiel nach einem Krypto-Ransomware Angriff die Praxisdaten nicht mehr im Zugriff, ist die Praxis hilflos. Behördenseitig kann nur selten eine rasche Wiederherstellung erreicht werden, dann nämlich, wenn die Verschlüsselungssoftware dort bekannt ist. Die Kosten, das „Problem" zu lösen, sprengen jede Vorstellungskraft und dadurch, dass es weder einen Zugriff auf elektronische Terminverwaltung noch auf die Patientendaten, geschweige denn auf die Abrechnungsdaten gibt, ist eine Weiterführung des Behandlungsalltags unmöglich. Dazu muss man sich nur mal vor Augen führen, wie man seine Patienten benachrichtigen will, wenn die Patientendaten gekapert sind.

Foto: Gorodenkoff - Fotolia.com

Sie haben ja mit vielen Praxisinhabern gesprochen. Wie handhabt die Mehrheit den Datenschutz und die Datensicherheit?

Erstens: Eine große Anzahl von Zahnarztpraxen mit Internetzugang nutzt ein nicht ausreichend gesichertes System.

Zweitens: Mittels randomisierter Brute-Force-Attacken – das sind automatisierte Dauerattacken auf der Suche nach Passwörtern – auf RDP-Server wurden viele Zahnarztpraxen angegriffen und Daten gekapert, wodurch es zu erheblichen Lösegeldzahlungen kam.

Drittens: Von neun IT-Firmen, mit denen ich gesprochen habe, haben sich lediglich zwei über einen gewissen Standard hinaus mit Cybercrime und Abwehrmaßnahmen beschäftigt.

Wie interpretieren Sie diese Situation?

Die Gefahrenlage ist leider nur wenigen Praxisinhabern wirklich bewusst. Die Frage, wie die eigene Praxis geschützt werden kann, was zu tun ist, damit eine vernünftige Sicherheit gewährleistet ist, muss sich allerdings jeder Praxisinhaber stellen.

Wie haben Sie und Ihr Team reagiert?

Wir haben auf Basis der unbefriedigenden Recherche Anfang Dezember eine Security-Task-Force gegründet und nach den besten IT-Spezialisten gefahndet, die es im Markt gibt. Dabei haben wir mit ehemaligen Hackern gesprochen und uns mit IT-Spezialisten zusammengesetzt, die über die notwendige Expertise in diesem Bereich verfügen. Danach haben wir das Team aus verschiedenen Disziplinen und Firmenzugehörigkeiten gebildet.

Was empfehlen Sie der Zahnarztpraxis?

1. Vergewissern Sie sich, ob der für Ihre IT-Sicherheit zuständige Mitarbeiter beziehungsweise das zuständige Unternehmen alle notwendigen Maßnahmen zum Schutz Ihrer technischen Infrastruktur ergriffen hat.
2. Lassen Sie den Ist-Zustand Ihrer Praxis im datenschutzrechtlichen Zusammenhang von einer externen Stelle unabhängig von Ihrem IT-Dienstleister überprüfen. Auf diese Weise können Sie grobe Verstöße gegen die geltenden Sicherheitsrichtlinien minimieren oder gar eliminieren. Achtung: Ihre Dienstleister stehen Ihnen beratend zur Seite, die Haftung liegt jedoch allein bei der Praxis, da diese für die Datenhaltung verantwortlich ist. Sie reduzieren hiermit allerdings das Risiko einer Einschätzung fahrlässiger Handhabe seitens der Justitia.
3. Vereinbaren Sie mit Ihrem IT-Dienstleister regelmäßige Kontrollen im Hinblick auf die Aktualität der ergriffenen Maßnahmen und Ihrer eingesetzten Programme beziehungsweise Anwendungen.

Wie schätzen Sie diese Bedrohung ein?

In meiner mittlerweile 15-jährigen Tätigkeit im Dentalmarkt habe ich nirgends eine derartige Existenzgefahr wie bei diesem Thema gesehen.

Das Interview führte Claudia Kluckhuhn.

Foto: privat

Christian Henrici ist Hauptgesellschafter der OPTI Zahnarztberatung GmbH und verfügt über die Erfahrung von über 1.400 Mandaten aus den vergangenen 15 Jahren.
henrici@opti-zahnarztberatung.de

Diese Regeln müssen Sie beachten!

Thies Harbeck

Die Begriffe „Datenschutz" und „Cyber-Kriminalität" bestimmen aktuell die Medienlandschaft. Passend dazu bilanziert das Bundeskriminalamt (BKA) im Bereich Cybercrime eine – wie in kaum einem anderen Deliktbereich – kontinuierlich steigende Entwicklung. Längst sind es nicht mehr Einzeltäter, die im Keller eine Schadsoftware entwickeln, mittlerweile sind professionelle Gruppen mit Geschäftsleitungen und Kundenservice aktiv.

Foto: krass99 - Fotolia.com

Wenn die Datenschutz-Grundverordnung (DSGVO) ab dem 25. Mai 2018 in der Europäischen Union anwendbar wird, heißt das nicht, dass das deutsche Bundesdatenschutzgesetz (BDSG) gegenstandslos wird. Vielmehr bildet die DSGVO den erweiterten Rahmen, der in den einzelnen Mitgliedsstaaten gewissermaßen individualisiert werden kann. In vielen Punkten entspricht das BDSG bereits den neuen EU-Richtlinien und wird ebenfalls zum 25. Mai angepasst.

Ein Zeichen dafür, dass wir in Deutschland gut aufgestellt sind? Nein! Umfragen – unter anderem von Bitkom Research – zeigen, dass sich lediglich 15 bis 20 Prozent aller deutschen Unternehmen sicher sind, dass sie den Datenschutzanforderungen umfänglich entsprechen. Als eines der größten Probleme wird dabei der Mangel an praktischen Umsetzungshilfen genannt.

Verantwortlich ist immer der Praxisinhaber

Die Bundeszahnärztekammer (BZÄK) hat ein knapp vierseitiges Merkblatt veröffentlicht, das die Kernpunkte des neuen Gesetzespapiers gelungen zusammenfasst. Wichtig ist, dass sich auch der Praxisinhaber mit dem Thema intensiv befasst, denn die Delegation an vermeintlich Wissende – dazu gehören auch die IT-Systembetreuer – verlagert nicht die Verantwortung, die sich aus den gesetzlichen Entwicklungen und Anpassungen für die alltägliche Arbeit in der Zahnarztpraxis ergibt. Dies gilt insbesondere für die zusätzlichen Regelungen, die im Rahmen der ärztlichen Schweigepflicht, des Patientenschutzes oder der Mitarbeiterschulung zu beachten sind.

Echter Experte oder doch Trittbrettfahrer?

Ganz offensichtlich wurde mit dem Thema Datenschutz in den vergangenen Jahren fahrlässig umgegangen. Erst die neue Gesetzeslage – die Anzahl der Neuerungen ist überschaubar – und insbesondere die drastisch gestiegenen Höchststrafen bei Verstößen sorgen für Aufmerksamkeit. Waren es gemäß § 43 Abs. 2-3 BDSG Geldbußen bis zu 300.000 Euro, sieht die DSGVO nun Strafen in Höhe von bis zu 20 Millionen Euro vor. Eine Steigerung um das 66,7-Fache!

Neben den persönlichen Daten Ihrer Patienten und Mitarbeiter schützen Sie durch eine korrekte Anwendung des Datenschutzgesetzes vor allem auch Ihre Praxis und Ihre berufliche und private Existenz. Das sind Werte, bei denen es keine zwei Meinungen geben sollte.

Die Grundlage einer hohen Datensicherheit bildet im heutigen Zeitalter der nach wie vor rasant fortschreitenden Digitalisierung eine den aktuelen Standards entsprechende technische Infrastruktur (TI). Da die wenigsten Zahnarztpraxen über eigene Techniker oder Datenschutzexperten verfügen, sind sie auf die Hilfe sogenannter Experten angewiesen. Hier überrascht die hohe Anzahl von Trittbrettfahrern, die sich die Angst der Unternehmen vor Cyber-Angriffen mit unprofessionellen Beratungs- und Sicherheitsangeboten zunutze machen.

Grundsätze beim Gebrauch der Praxis-EDV

Auch wenn die Anforderungen der elektronischen Datenverarbeitung immer komplexer werden und die Masse online verfügbarer Daten weiter zunehmen wird, gibt es einige grundlegende Regeln, um den alltäglichen Gebrauch der Praxis-EDV sicher zu gestalten. In § 630f BGB ist klar definiert, dass der Behandelnde verpflichtet ist, eine Patientenakte mit sämtlichen wesentlichen Maßnahmen derzeitiger und künftiger Behandlungen inklusive der Ergebnisse zu führen. Wie aber kann der Inhalt geschützt werden? Die BZÄK hat in Zusammenarbeit mit der Kassenzahnärztlichen Bundesvereinigung (KZBV) bereits 2015 einen Leitfaden dazu veröffentlicht, in dem die wichtigsten Grundsätze aufgeführt sind:

Das sagt der Experte

„Da draußen herrscht Krieg!“

Schützen kann sich der Zahnarzt nur durch ein Maßnahmenpaket. Dabei darf kein einzelner Punkt vernachlässigt werden.

Firewall/UTM

Eine Kontrolle der Inhalte des Datenverkehrs durch ein sogenanntes Unified Threat Management, kurz UTM, erhöht die Sicherheit enorm. Während eine Firewall den Datenverkehr zwischen einem Rechner und dem Internet beobachtet und unaufgefordert von außen eingehende Daten abblockt, schaut ein UTM in alle Datenpakete hinein. Damit ist das UTM in der Lage, sowohl eingehende E-Mails wie auch besuchte Webseiten direkt zu untersuchen und sowohl gefährliche (Viren, Schadsoftware, …) als auch unerwünschte Inhalte (Spam, bestimmte Dateitypen wie .exe, .com, …) herauszufiltern. Die Sinnhaftigkeit solcher Maßnahmen erkennt man schon daran, dass es zum Beispiel bei einem Unternehmensnetzwerk wie dem der KZBV täglich mehrere zehntausend Angriffe gibt. Es klingt dramatisch: Aber da draußen herrscht Krieg.

Die Gegenwehr – ein UTM inklusive Firewall und Servicepaket – kostet nicht die Welt, etwa 1 bis 2 Euro am Tag fallen für eine Praxis an. Ein UTM schützt das interne Netz effektiv. Aufbau und Konfiguration dieser Infrastruktur sollten jedoch nur versierte Zahnärzte selbst vornehmen und ansonsten an einer EDV-Unternehmen abgeben.

Sensibilität

Es ist wichtig, dass das komplette Praxisteam die Notwendigkeit der IT-Sicherheitsmaßnahmen versteht. Denn Passwörter wie 123456 und das gedankenlose Öffnen von unaufgefordert erhaltenen E-Mails oder darin enthaltenen Dateianhängen können beinahe existenzgefährdende Folgen haben. Hier gilt: Unaufgefordert erhaltene E-Mails von unbekannten Absendern sollten unverzüglich gelöscht werden. Denn häufig enthalten beispielsweise Office-Dokumente (.doc, .docx) sogenannte Makros, die nach dem Öffnen des Dokuments auf dem Client-Computer selbsttätig aus dem Internet Schadsoftware herunterladen können, weil Firewalls in der Regel eine derartige Datenanfrage nicht blockieren. Da die Ausführung von Makros auf dem Client-Computer in der Regel nicht deaktiviert ist, stellen solche Dateianhänge eine latente Gefahr dar.

Schulung

Da im Notfall – das Netzwerk der Praxis wurde trotz allen Vorsichts- und Schutzmaßnahmen Opfer eines Verschlüsselungsangriffs – lediglich eine funktionierende intakte Datensicherung die letzte Möglichkeit zur Rettung der Daten darstellt, kommt dem Thema Datensicherung eine entscheidende Rolle zu. So sollten die Personen, die für die Datensicherung verantwortlich sind, ausreichend geschult sein. Gerne wird hier der externe EDV-Dienstleister auch die Schulungsmaßnahme übernehmen.

Back-up-Strategie

Eine stichprobenartige Überprüfung der gesicherten Daten auf Lesbarkeit und Vollständigkeit ist ebenso eine Selbstverständlichkeit wie die Frage der Aufbewahrung der Datensicherung. Diese sollte auf keinen Fall in der Praxis aufbewahrt werden,

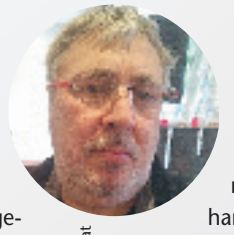

Foto: privat

andernfalls ist sie nach einem Brand, einem Wasserschaden oder nach einem Einbruch nicht mehr nutzbar oder nicht mehr vorhanden.

Nach erfolgter Sicherung, zum Beispiel auf einer externen Festplatte, sollte diese auf jeden Fall räumlich getrennt von der Praxis aufbewahrt werden. Es ist daher notwendig, mindestens zwei Sätze (Festplatten) zu nutzen. Während die eine angeschlossen ist, um als Sicherungsmedium zu dienen, wird die zweite räumlich getrennt aufbewahrt. Tag für Tag werden dann die beiden Sätze gewechselt.

Virenschutz

Ein guter, regelmäßig aktualisierter Virenschutz ist unerlässlich. Am besten wird er sowohl an zentraler Stelle auf dem Server als auch auf allen Client-Rechnern installiert. Es ist regelmäßig zu überprüfen, ob die Virendefinitionen auf dem neuesten Stand sind. In der Regel sind die Virendefinitionen tagesaktuell und erfolgen gegebenenfalls auch mehrfach täglich.

Wenn die Betroffenen einen Angriff bemerken, ist es für Schutzmaßnahmen in der Regel zu spät. Dann gilt die Devise: „Schnell alle Stecker raus!“ Alle Netzwerkverbindungen zwischen Router und Server sowie zwischen Server und Client-Rechnern müssen unverzüglich getrennt und die Rechner heruntergefahren werden. Anschließend sollte das EDV-Partnerunternehmen kontaktiert werden.

Siegfried Reiser ist Leiter der Abteilung EDV-Inhouse/Kommunikationssysteme der Kassenzahnärztlichen Bundesvereinigung.

Nutzung und Qualität von Kennwörtern

Wie im privaten Umfeld sollte man sensible Daten nicht mit dem Passwort „1234“ schützen. Als sinnvoll und schwer zu knacken erweisen sich Kombinationen aus kurzen Sätzen gepaart mit Sonderzeichen (Beispiel: Dies/iSt&EIN_Test).

Virenschutz

Auch wenn der Rechner nicht mit dem Internet verbunden ist, bildet ein zuverlässiger Virenschutz die Basis sicheren Arbeitens. Der Datenaustausch mittels USB-Stick oder CD sollte idealerweise auf Rechner außerhalb des Praxissystems beschränkt werden.

Administrationsrechte

Jeder Mitarbeiter sollte nur so viele Rechte erhalten, wie er für seine Arbeit benötigt. Damit schützen Sie einerseits die sensible Datenstruktur der Praxis, andererseits entlasten Sie den Mitarbeiter. Ein Rechte- und Rollenkonzept gibt Aufschluss über die entsprechenden Erfordernisse.

Datensicherung (Back-ups)

Auch wenn die Cloud viele Vorteile mit sich bringt, gibt die Praxis ihre Datensicherung damit in einen Bereich, der nicht der eigenen Kontrolle unterliegt. Regelmäßige,

IT-Sicherheitsbeauftragter Tobias Thiede

Hacking as a service

Seit ungefähr 2,5 Jahren ist Krypto-Erpressung in Deutschland ein Thema – nicht nur für große Firmen, sondern auch für kleinere Unternehmen wie Zahnarztpraxen. Das liegt auch daran, dass all unsere Geräte – Smartphones, Kreditkarten, MRT – mittlerweile miteinander vernetzt sind.

Diese kriminelle Szene tut nichts anderes, als mit gekaperten Daten Geld zu erpressen. Das BKA verzeichnet eine kontinuierliche Steigerung im Bereich Cybercrime. Die Dunkelziffer ist hoch, aber Experten gehen davon aus, dass der weltweite Umsatz in diesem Markt höher ist als im Drogenhandel. Ungefähr 70 Prozent der Schadsoftware – Stand Mitte 2017 – dient der Datenverschlüsselung. Daten, das sind Unternehmensdaten, Patientendaten, aber auch Urlaubsfotos. Dabei wird nicht wie früher ein Gebiet abgegrast, sondern flächendeckend attackiert.

Das Raffinierteste derzeit? Zielgerichtete Bewerbungen. Dabei suchen die Hacker bei der Arbeitsagentur nach offenen Jobs und schicken der Firma daraufhin eine Bewerbung auf die real ausgeschriebene Stelle. Im Anhang befinden sich Zeugnisse in einer Excel-Datei, die im Hintergrund schadhafte Makros enthält. Im schlimmsten Fall wird der Rechner der Personalabteilung verschlüsselt. Die Frage, wer welche Anhänge öffnen darf, sollte daher auch in der Zahnarztpraxis beantwortet werden.

Viele Attacken laufen über extern erreichbare Dienste wie zum Beispiel den VPN-Tunnel, der in der Zahnarztpraxis klassischerweise für externe Abrechnungskräfte eingerichtet wird. Ist ein VPN-Zugang nicht über Zertifikate oder andere Methoden, sondern lediglich durch Benutzernamen oder Kennwort gesichert, dann sind diese Zugänge gefährdet.

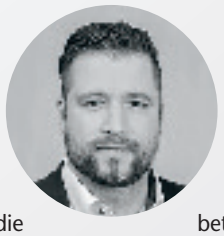

Foto: privat

In den häufigsten Fällen finden die Verbrecher das Kennwort über automatische Scans heraus, die ihnen den Weg zu einem offenen VPN-Zugang weisen. Diese sogenannten Brut-Force-Angriffe verschicken tausende Anfragen mit zig Benutzername-Passwort-Kombinationen. Wer keine automatische Sperre nach dreimaliger Falscheingabe eingerichtet hat, eröffnet dem Angreifer somit unendlich viele Möglichkeiten, so lange herumzuprobieren, bis er das System geknackt hat. Man muss sich den Vorgang als automatisierten Prozess vorstellen: Wie ein Wörterbuch geht das Programm eine Liste mit Millionen von Kombinationen durch. Das heißt, es handelt sich nicht um zielgerichtete Attacken, sondern um Massenangriffe. In 95 Prozent der Fälle ist auch die Zahnarztpraxis Opfer eines solchen Massenangriffs.

Zielgerichtete Attacken – Datenspionage – richten sich indessen eher gegen große Unternehmen oder politische Strukturen wie den Bundestag. Hacking ist heute ein Service: Im Regelfall bieten Hacker im Darknet die Schadsoftware plus gestohlene E-Mail-Adressen im Paket an. Der Angreifer muss also gar kein spezielles Know-how mehr haben.

Erfahrungsgemäß wird man mit einem Pop-up-Fenster darauf hingewiesen, dass man angegriffen wurde („Wir haben Ihre Daten verschlüsselt. Überweisen Sie xx Bitcoins auf folgendes Bitcoin-Konto!").

Die alten Karteikarten sind hinterher oft der einzige Weg, um auch ohne Zugriffsmöglichkeit auf die digitalen Daten der Informationspflicht nachzukommen und Patienten und betroffene Dritte über den Diebstahl zu benachrichtigen.

Doch wie kann der Praxischef präventiv tätig werden? Hier sollte der Fokus immer auf dem Betriebssystem beziehungsweise dem Rechner liegen. Die Zahnarztsoftware läuft ja nur auf einem Computer. Sie ist ein Programm. Da die meisten flächendeckenden Angriffe sich aber nicht direkt gegen die PVS wenden, sondern – wie etwa bei Kryptotrojanern – darauf abzielen, alles zu verschlüsseln, sollte man in erster Linie das Betriebssystem selbst schützen – über Updates, der Trennung vom Internet, einem Installations- und Ausführungsverbot bestimmter Programme (Wird Office – denken Sie an die Makros! – in der Praxis wirklich auf jedem Computer benötigt?) und Dokumente.

Ein zweiter Faktor – wie ein Zahlencode oder ein Zertifikat – erhöht zudem im Vergleich zur einfachen Authentifizierung mit Benutzername und Kennwort die Sicherheit und schützt doppelt vor einem Angriff auf einen VPN-Dienst.

Am Ende sollten Sie sich immer vor Augen führen: Verantwortlich für die Absicherung des IT-Systems und damit haftbar ist der Betreiber, also der Praxisbesitzer– und das sind Sie!

Tobias Thiede
IT-Sicherheitsbeauftragter
bei der BFS health finance in Dortmund

dezentral gelagerte, physische Back-ups sind noch immer die sicherste Variante. Ursprünglich dienten die physischen Back-ups auf Kassette dem „BDÜ"-Schutz – der Absicherung gegenüber Brand, Diebstahl und Überschwemmung. Dazu empfehlen sich tägliche Sicherungen auf unterschiedlichen Datenträgern – für jeden Arbeitstag einen. In der heutigen Zeit ist der Faktor Cyber nicht länger außer Acht zu lassen und sollte als vierter Bestandteil ergänzt werden.

■ regelmäßige Sicherheits- und Programmupdates

Aktuelle Betriebssysteme sind die zwingende Voraussetzung sicheren Arbeitens. Darüber hinaus muss jede Software regelmäßig aktualisiert werden. Programme, die Sicherheitslücken aufweisen oder nicht zwangsweise benötigt werden, sollten deinstalliert werden.

■ Schulung der Mitarbeiter (Awareness)

Das Bewusstsein der Mitarbeiter für die heikle Thematik personenbezogener Daten ist von immenser Bedeutung. Immer wieder kommt es durch Unwissenheit zu Verstößen. Datenschutzbeauftragte sind in Deutschland gemäß Art. 37 DSGVO i.V.m. § 38 BDSG (neu) zwar erst ab einer Mitarbeiteranzahl von zehn Personen, die mit der Verarbeitung personenbezogener Daten beschäftigt sind, vorgesehen, aber auch für kleinere Praxen sehr sinnvoll. Lassen es die eigenen Kapazitäten nicht zu, sich intensiv

mit dem Thema zu beschäftigen, kann die Praxis auf externe Dienstleister zurückgreifen und sogar einen externen Datenschutzbeauftragten im Rahmen eines Dienstleistungsvertrags bestimmen (Art. 37 Abs. 6 DSGVO).

Die Bestellung eines Datenschutzbeauftragten allein reicht jedoch nicht aus, er muss sich auch seiner Aufgaben und Pflichten zur Erfüllung der Datenschutzrichtlinien bewusst sein. Dazu gehört unter anderem auch die Aufklärung der Mitarbeiter, die sich gern hinter ihrer Unwissenheit verstecken. Selbige schützt bekanntlich nicht vor der Strafe – außerdem haftet die Praxis für das Fehlverhalten der Mitarbeiter.

Klassiker für Verstöße: der Offline-Bereich

Auch wenn im Zusammenhang mit dem Datenschutz vermehrt die Begriffe EDV und Cyber-Kriminalität fallen, sind es doch immer wieder die klassischen „Offline-Bereiche", in denen es in Zahnarztpraxen regelmäßig zu Datenschutzverstößen kommt: Mitarbeiter verwenden schwache Passwörter, rufen gefährliche Webseiten auf oder öffnen infizierte E-Mail-Anhänge. Regelmäßige Schulungen und aktive Trainings helfen der Praxis, die Mitarbeiter fit zu machen.

die ärztliche Schweigepflicht

Datenschutz heißt, den Einzelnen vor Beeinträchtigungen in seinem Persönlichkeitsrecht zu schützen. Die ärztliche Schweigepflicht ist eine Konkretisierung dieser Maßgabe durch das in § 203 StGB definierte Patientengeheimnis. Mitarbeiter sind auf das Datengeheimnis zu verpflichten und sollten eine entsprechende Erklärung unterzeichnen.

Erstkontakt an der Rezeption (Datenerfassung)

Insbesondere bei Neupatienten sind in der Regel in größerem Umfang Daten für die korrekte Erfassung und Behandlung vonnöten. Diese sollten in einem persönlichen Gespräch in einem geschlossenen Raum oder schriftlich über den Anamnesebogen eingeholt werden. Offene Gespräche an der Rezeption sind nicht angemessen.

das Behandlungszimmer

Nicht gesicherte PCs sind der einfachste Einstieg in das sensible System der Zahnarztpraxis. Mit wenigen Klicks kann ein destruktiv gesinnter „Patient", der im Zimmer allein gelassen wurde, die komplette Praxis stilllegen. Ebenso dürfen analoge Daten (KVs, HKPs) nicht ungesichert greifbar sein.

Kontakt über Telefon, E-Mail und Fax

Auch wenn durch die Abfrage von Wohnort oder Geburtsdatum eine scheinbare Sicherheit erzeugt werden kann, sollten über Terminvereinbarungen und -verschiebungen hinaus keine telefonischen Auskünfte erteilt werden. Gleiches gilt für E-Mails und Faxe.

externe Dritte

Werden Patientendaten an externe Dienstleister ausgelagert, ist stets ein Vertrag zur Auftragsdatenvereinbarung gemäß Art. 28 DSGVO zu schließen. Ein Vertrag zur Auftragsdatenverarbeitung muss durch die Einwilligung des Patienten genehmigt werden. Insbesondere im Hinblick auf die verschärfte gesetzliche (strafrechtliche) Grundlage ab Mai sollte sich spätestens jetzt aber jeder Praxisinhaber die Frage stellen, ob er und seine Praxis gut aufgestellt sind. Wer diese Frage nicht beantworten kann, sollte auf die Hilfe externer Berater zurückgreifen, die die Praxis beispielsweise im Rahmen einer simulierten Datenschutzbegehung prüft. Ebenso wie das Qualitätsmanagement muss auch Datenschutz als fester Prozess in der Praxis integriert werden.

Foto: privat

Thies Harbeck ist Geschäftsführer der OPTI Zahnarztberatung GmbH.

ZM-ONLINE

Kann und Thiede im Video

Zahnarzt Dr. Michael Kann berichtet über seine Erlebnisse. Der TI-Experte gibt Tipps.