Mike Amelang

Datenhygiene: Warum Datenschutz und Cyberschutz unerlässlich sind

PRAXISMANAGEMENT Wo Daten generiert werden – und das erfolgt heutzutage ja allgegenwärtig – müssen sie geschützt werden. Das trifft auch und besonders für Zahnarztpraxen zu, die, wenn nicht schon komplett, doch zunehmend digital aufgestellt sind. Welche Schritte unbedingt zu beachten sind, um eine konsequente „Datenhygiene“ zu garantieren, erläutert der folgende Beitrag.

Handfeuerwaffe: © peteri – stock.adobe.com

Das Internet befeuert uns stündlich mit Millionen von automatisierten oder gezielten Angriffen. Beachtlich ist die Tatsache, dass die **CYBERKRIMINALITÄT** mittlerweile sogar die Umsätze der Drogenkriminalität weltweit übertroffen hat.

Die Digitalisierung in der Zahnarztpraxis läuft. Aus dem klassischen Praxismarketing ist ein Onlinemarketing mit Social-Media-Auftritten bei Facebook, Instagram und YouTube geworden. Vor Jahren noch undenkbar, veröffentlichen Zahnärzte heute Filme und Postings. Zudem verlagert sich das Thema Fortbildung seit Jahren in Webinare und wird zum E-Learning. Die Telematik wird ausgebaut. Patienten buchen Arzttermine online, und Such- oder Bewertungsportale sind eine Selbstverständlichkeit. Gleichermaßen entwickeln sich digitale Behandlungsmöglichkeiten, und Behandlungen wie Patientendaten werden auf dem Praxiscomputer gespeichert. Und tagtäglich werden interaktiv Daten mit Laboren, Behandlern und anderen Partnern ausgetauscht.

Die beschriebenen Aktivitäten zeigen deutlich: Es werden immer umfangreicher Daten verarbeitet, gespeichert und versandt. Die Digitalisierung ist Realität. Wer A sagt, muss auch B tun. Jetzt gilt es, die neuen, mit der Digitalisierung verbundenen Herausforderungen auch zu meistern.

Leitfaden zur Datenhygiene

Viele Praxisinhaber ignorieren (immer noch) Haftungen, Pflichten und Risiken der Digitalisierung. Zur Erinnerung: Seit 25. Mai 2018 haftet der Praxisinhaber bei Datenschutzverletzungen. Der Geschädigte hat nun einen eigenen, gerichtlich durchsetzbaren Rechtsanspruch (Schadenersatz). Wer die gesetzeskonformen Datenschutzpflichten verletzt, hat nunmehr mit empfindlichen Geldbußen zu rechnen. Ein aus der Datenschutzverletzung entstandener Schaden kann existenzzerstörend sein.

Im Gespräch mit Praxisinhabern wird deutlich, dass schlichtweg ein Leitfaden zur Datenhygiene fehlt. Kammern, Verbände, Öffentlichkeit haben es nicht vermocht, für Klarheit zu sorgen. Der Begriff der Datenhygiene passt vortrefflich. So definiert die Deutsche Gesellschaft für Hygiene und Mikrobiologie den Begriff Hygiene als „Erkennung, Behandlung und Prävention von Infektionskrankheiten“. Bei Wikipedia wird bereits das Eindringen von Schadsoftware in einen Computer als Infektion bezeichnet. Fasst man im Ergebnis die Begrifflichkeiten und die Zielsetzung zusammen, so handelt es sich bei der Datenhygiene letztlich

um die Beachtung des Datenschutzes (Prävention, Erkennung) und Cyberschutzes (Behandlung). Doch es mangelt an der Datenhygiene.

Die Frage ist nicht, ob es zu einem Cyberangriff kommt, sondern wann und wie?

Blickwechsel. Zum Jahresbeginn 2019 wurde ein Cyberangriff auf Bundespolitiker bekannt. Ein 20-jähriger Computer-Nerd aus Hessen drang in die Systeme der Politiker ein und entwendete Daten. Diese Geschichte ist ein lehrreiches Beispiel und zeigt viele Aspekte der fehlenden Datenhygiene auf. Glücklicherweise wurde dieser Datenskandal an die Öffentlichkeit getragen und aufgeklärt. Normalerweise ist die Dunkelziffer von Cyberattacken und Datenschutzverletzungen hoch, die Aufklärungsrate gering. Aus Scham veröffentlicht kaum eine geschädigte Praxis erlittene Datenschutzverletzungen. Doch es gibt unzählige Praxen, die bereits erfolgreich attackiert wurden und große Schäden (Verschlüsselung, Erpressung, Ausfall) erlitten.

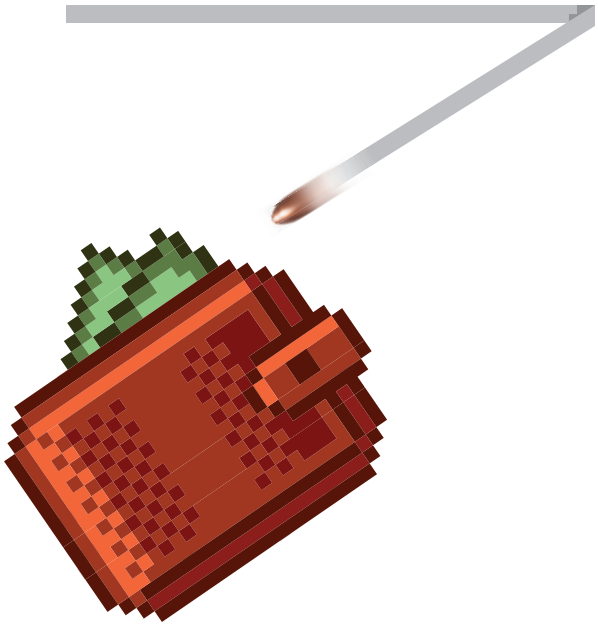

Illustration: © La Gorda – stock.adobe.com

Es ist wohl einfacher, jemanden **ANONYM ÜBER DAS INTERNET** zu erpressen, als einzubrechen und auszurauben …

Der Vorgang in Berlin zeigt, dass es eine hundertprozentige Sicherheit nicht geben kann. Wir müssen eine offene Fehlerkultur akzeptieren. Im Zeitalter der Datenströme ist die Frage nicht, ob es zu einem Cyberangriff oder einer Datenschutzverletzung kommt, son-

dern wann und mit welchen Auswirkungen. Denn das rastlose Internet befeuert uns stündlich mit Millionen von automatisierten oder gezielten Angriffen. Beachtlich ist die Tatsache, dass die Cyberkriminalität mittlerweile sogar die Umsätze der Drogenkriminalität weltweit übertroffen hat. Es ist wohl einfacher, jemanden anonym über das Internet zu erpressen, als einzubrechen und auszurauben oder aufwendig Drogen herzustellen und zu verkaufen.
Hinzu kommt auch menschliches Versagen. Anerkannte Untersuchungen zeigen, dass rund ein Viertel aller Datenschutzverletzungen durch absichtliche oder versehentliche Aktivitäten von Mitarbeitern erfolgte. Der Mensch ist immer noch ein wichtiger Bestandteil der Datensicherheit.

Datenhygiene in der Praxis

Der ernüchternde Befund des Ist-Zustands enthält zwei Denkansätze: 1. Der Praxisinhaber behält seinen Glauben und ignoriert die Grundlagen effektiven Datenschutzes oder 2. Der Praxisinhaber setzt die Datenhygiene um. Es gilt, in Zukunft zwingend auf Prävention, Erkennung für Datenschutzmaßnahmen und Behandlung von Cyberinfektionen zu achten. Datenschutz muss aktiv gelebt werden. Voraussetzung ist, dass man weiß, was zu tun ist.
Es wird Zeit, sich Beratungskompetenz in die Praxis zu holen. Es reicht nicht mehr, sich auf andere Dienstleister (IT) oder Dritte (Kammern) zu verlassen, die Patienten zu informieren und die Homepage im Impressum anzupassen. Die DSGVO ist vollständig zu erfüllen, Passwörter sind regelmäßig zu tauschen und sicher zu machen, Daten sollten überlegt in Speichermedien überführt werden. Updates sollten regelmäßig ausgeführt und abgelaufene Software gelöscht werden. Ein Notfallszenario und die Sensibilisierung zum Datenschutz muss regelmäßig eingeübt sein. Ein Dreivierteljahr nach verpflichtender Umsetzung der DSGVO sind viele Praxen noch weit entfernt, wenigstens die gesetzeskonformen Rechenschafts- und Dokumentationspflichten zu erfüllen. Gerade kleine Praxen haben keinen Ansprechpartner für den Datenschutz und sind zu diesem Thema blind wie Milchglas und für Cyberangriffe offen wie ein Scheunentor.

Schaden eingetreten – Wer zahlt dafür?

Nach einem Cyberangriff oder einer Datenschutzverletzung ist die Aufregung meist groß. Was ist zu tun? Wer kann helfen? Wer bezahlt eigentlich den ganzen Schaden? Aber was heißt eigentlich „Schaden“? Ein Informationsschaden liegt vor, wenn die Rechte Dritter (Mitarbeiter, Patienten, Partner) verletzt werden. Wenn deren Daten verschlüsselt, entwendet, veröffentlicht wurden. Auch der Eigenschaden des Praxisinhabers gehört dazu (Ausfall, Erpressung, Reputationsschaden). An dieser Stelle zeigt sich auch ein allgemeiner Irrtum. Der Datenschaden realisiert sich nur zu einem geringen Teil innerhalb der Praxis-Computeranlage (Speichermedien). Daher kann der eigene IT-Dienstleister auch kaum Hilfe geben. Der wirkliche und teure Schaden (Ausfall, Schadenersatz, Erpressung) wirkt außerhalb der Computer. Kein IT-Dienstleister kann eine einhundertprozentige Sicherheit garantieren. Ist der Schaden eingetreten, so verlangt die DSGVO einen klaren Schadenfolgeprozess. Neben einer ordnungsgemäßen Meldung des Schadens an die Behörde bedarf es einer hochkomplexen IT-Forensik, einer Information der Geschädigten und natürlich der Behandlung des Schadens.
Der Schaden der angegriffenen Bundespolitiker wird natürlich wieder vom Bund bzw. Steuerzahler beglichen, zumal der 20-Jährige wohl kaum zahlen können wird. Der geschädigte Normalmensch oder Praxisinhaber wird in einem solchen Fall alle amtlich geforderten Aktivitäten selbst erledigen müssen und auf dem Schaden sitzen bleiben. Denn die bestehenden Praxisversicherungen gelten für diese neue Art von Schäden nicht.
Im Sinne der Datenhygiene erfolgt nun die notwendige Behandlung und Heilung durch eine Cyberschutzabsicherung. Denn nur Cyberschutz bietet ein umfangreiches Maßnahmenpaket im Schadenfall und beinhaltet die Abwehr von Schäden, damit die Praxis schaden- und kostenfrei weiterarbeiten kann.

Fazit

Wer die Datenhygiene in der Zahnarztpraxis aktiv angeht und die Bausteine Prävention (DSGVO), Erkennung (Sensibilisierung im täglichen Umgang) und Heilung (Cyberschutz) beherzigt, wird ruhiger schlafen und entspannter arbeiten, da er trotz offener Fehlerkultur weiß, es kann so schlimm nicht werden. Jeder Praxisinhaber tut gut daran, sich beraten zu lassen.

INFORMATION

Mike Amelang
Jurist und Datenschutzbeauftragter
Tel.: 030 39886465
info@amelang.berlin
www.amelang.berlin

Infos zum Autor

YunMed

PEEK Natur

Hochleistungskunststoff in der reinsten Form

ANGEBOT
129,- €
für jede Ronde
Höhe 16, 20 oder 25 mm

Bestellen Sie jetzt direkt bei Ihrem Vertriebs- und Servicepartner FDZ:
bestellungen@fdz-deutschland.de
www.fdz-deutschland.de

Alle Preise verstehen sich netto zzgl. MwSt. Das Angebot gilt nur in Deutschland bis zum 30.04.2019. Das Angebot ist einmalig pro Kunde für die erste Bestellung und für maximal drei Ronden gültig. Preisänderungen und Lieferbedingungen vorbehalten. Es gelten die allg. Geschäftsbedingungen.

FDZ Fräs- und Dienstleistungszentrum GmbH Deutschland