Und plötzlich steht die Praxis still – Cyberkriminalität und Datensicherheit

Der übliche Arbeitsplatz bietet rund 10 bis 15 Angriffspunkte für Cyberkriminelle: E-Mail, Internet, Telefon, ungesicherte USB-Schnittstellen, freier Blick auf den Bildschirm usw. So banal diese Angriffspunkte klingen, so ausgefeilt sind mittlerweile die Techniken der Cyberkriminellen, um solche Schwachstellen auszunutzen. Selbst bei perfekter technischer Umsetzung bleibt der „Faktor Mensch" als zunehmendes Ziel krimineller Aktivitäten. Nur gut geschulte Mitarbeiter sind in der Lage, Gefahren zu erkennen und die Praxis effektiv vor Angriffen zu schützen. Die Brisanz und Notwendigkeit zum Schutz der sensiblen Praxis- und Patientendaten rückt die neue Europäische Datenschutz-Grundverordnung (EU-DSGVO) ins Rampenlicht.

Cyberkriminalität und der Schutz der Daten gehen uns alle an! Praxisinhaber und IT-Verantwortliche können nur die technischen Voraussetzungen für eine möglichst effektive Abwehr schaffen. Die Vielfältigkeit der Angriffe, die mithilfe von Internet, informationstechnischen Systemen oder deren Daten verübt werden oder auf diese gerichtet sind (kurz Cyberkriminalität), erfordert jedoch eine Sensibilisierung aller Personen, die mit Systemen und Daten umgehen. Der Rahmen der EU-DSGVO setzt hier klare Vorgaben, um die getroffenen technischen und organisatorischen Maßnahmen zum Schutz der Daten aufzuzeigen. Auch wenn die gesetzliche Vorgabe den Eindruck von Bürokratie hinterlässt – der kritische Blick auf die eigene Praxis zeigt Schwachstellen und Lücken auf, die in erster Linie aus Eigeninteresse der Praxis geschlossen werden sollten. Simone Uecker kennt die Sicherheitslücken aus Praxen, die sie in der Umsetzung der EU-DSGVO betreut und verrät ihre Tipps zum Schutz der Praxis. Denn welche Praxis kann bei Totalverlust ihrer Daten heute noch arbeiten?

Der kritische Blick auf die eigene Praxis

Wenn wir verstehen, warum Cyberkriminelle überhaupt Daten angreifen, können wir durch die Augen der Cyberkriminellen einen kritischen Blick auf die eigene Praxis und die eigenen Verhaltensweisen werfen. Vermehrt kommen Datenverschlüsselungen des gesamten Datenbestandes durch Schadsoftware vor, mit denen die Verantwortlichen zu beträchtlichen Lösegeldern erpresst werden sollen. So legte ein derartiger Angriff im Mai 2017 mehrere britische Krankenhäuser lahm. Operationen mussten verschoben und Patienten an andere Häuser verwiesen werden.
Auch Betrugsmaschen ähnlich dem „Enkeltrick", nur im professionellen Umfeld angewandt, zielen auf finanzielle Vorteile für die Angreifer ab. Neben finanziellen Zielen beabsichtigen Cyberkriminelle oft den Identitätsdiebstahl, indem gezielt persönliche Daten auf vielfältige Weise ausgespäht und schließlich wie ein Puzzle zu einer Identität zusammengesetzt werden. Die umfangreichen und sensiblen persönlichen Patientendaten in der Praxis können hierbei also genauso zum Ziel werden.
Beim Durchleuchten der Praxis auf mögliche Schwachstellen werden all jene Punkte beachtet, an denen Daten entwendet oder Daten bzw. Schadsoftware eingebracht werden können, also alle Schnittstellen, Kommunikations- und Transportwege. Genau diese kritischen Punkte gilt es, bewusst zu machen und zu schützen, z. B. USB-Schnittstellen sperren, Virenschutz auf allen PCs und Aktualisierungen sicherstellen, E-Mail-Kommunikation durch Verschlüsselung gegen Datenverlust schützen, Back-up-Medien verschlüsseln und sicher transportieren, Kommunikation mit externen Back-up-Servern verschlüsseln, verschlüsselte Datenübermittlung aus Online-Kontaktformularen auf der Praxiswebsite, Internet nur für vertrauenswürdige Seiten freigeben, Pop-up- und Werbe-Blocker nutzen.

Der Netzwerkplan – Technische Maßnahmen dokumentieren

Der Praxisrundgang gibt erste Einblicke in mögliche Angriffspunkte in der Praxis. Ein detaillierter Netzwerkplan, also eine grafische Darstellung der informationstechnischen Einrichtungen der Praxis (PCs, Server etc.), erlaubt dem Profi eine strukturierte Analyse. Der Netzwerkplan stellt übrigens auch ein Schlüsseldokument im Datenschutzmanagementsystem dar, um die technischen Maßnahmen der Praxis darzustellen. „Hier fällt mein erster Blick auf die Firewall und die Verbindungen von außen in das Praxisnetzwerk. Sie möchten mir nicht glauben, wie viele Firewalls ungesicherte Türen offen lassen", erklärt Simone Uecker. Hardware-Firewalls sind heute vielfach bereits Standard, doch damit diese Systeme echten Schutz bieten, sollte die Konfiguration kritisch hinterfragt werden. Gängige Praxis ist es, dass sich IT-Dienstleister einen freien Zugang durch die Firewall zu Server und Praxisnetz offen halten, um im Support-Fall schnell Unterstützung zu bieten oder auch mal während Schließzeiten der Praxis Wartungen durchzuführen. „Aus Sicht des Kundenservice ist dieses Vorgehen verständlich, doch aus Sicht der Datensicherheit und des Datenschutzes können wir dies nicht gutheißen", warnt Simone Uecker. Der zweite Blick fällt auf das Thema Systemtrennung. Während es zu Beginn der Digitalisierung üblich war, z. B. nur einen einzelnen PC mit dem Internet zu verbinden, ist das mit dem aktuellen Stand der Technik nicht mehr zeitgemäß. In der Kombination mit einer sauber konfigurierten Firewall lässt sich die Trennung eines „Internet-PC" für E-Mail und Internet vom Praxisnetzwerk realisieren, trotzdem bleibt der Onlinezugriff an den erforderlichen Arbeitsplätzen erhalten. Wird der Internet-PC von Schadsoftware oder Verschlüsselung befallen, kann dieser schnell und einfach neu konfiguriert werden – ganz ohne Ausfallzeiten der gesamten Praxis-IT und somit Stillstand im Praxisbetrieb.

Back-up – Ihre beste „Lebensversicherung"

Bei aggressiven Cyberattacken, die z. B. den gesamten Datenbestand verschlüsseln und in der Folge Lösegeld zur Entschlüsselung fordern (sogenannte Ransomware), hilft meist nur, auf die letzte Datensicherung zurückzugreifen. Trotz Lösegeldzahlung geben die Erpresser meist den Schlüssel nicht preis – Daten und Geld sind verloren. Das Back-up der Praxisdaten bleibt also die beste Lebensversicherung für den Fall der Fälle (nicht nur im Schutz gegen Cyberangriffe, sondern auch bei Brand, Systemausfall oder Festplattencrash). Dies gilt jedoch nur, wenn auf eine sehr

aktuelle Datensicherung zurückgegriffen werden kann und das Back-up auch wirklich alle Daten der Praxis umfasst.

Hier zeigt sich in der Beratungspraxis jedoch oft gefährliches Unwissen und damit Unverständnis, dass die aufwendigen Back-up-Maßnahmen in der Praxis nicht effektiv sein sollen. Wenn die externe Festplatte oder NAS auch nach der Sicherung angesteckt und somit Teil des Netzwerks bleibt oder nur auf interne Festplatten gespiegelt wird, wird auch die Sicherung von der Verschlüsselungsattacke betroffen sein. Zudem enthalten Back-ups in der Regel nicht alle Anwendungsdaten, meist um die Datenmenge und erforderliche Zeit für die Erstellung des Back-ups zu reduzieren. Hier sollten mehrschichtige Back-up-Konzepte angedacht werden, um eine Mischung aus Effizienz und Vollständigkeit zu erzielen.

Die Praxis zeigt auch, dass vielfach versäumt wird, den erfolgreichen Abschluss der Sicherung mittels Protokoll oder Benachrichtigung zu kontrollieren. Ein kritischer Blick auf den tatsächlichen Umfang der eigenen Datensicherung, regelmäßige Kontrolle und die genaue Dokumentation des Back-up-Prozesses inklusive Erfolgskontrolle sind also notwendig, um sich nicht in trügerischer Sicherheit zu wiegen.

Selbstcheck Praxen

Organisatorische Maßnahmen schulen – Praxisteam steht an vorderster Front

Die beste technische Ausstattung der Praxis ist nur so sicher wie die Menschen, die sie nutzen. Durch hoch entwickelte Algorithmen in Antivirus-Software, die in kürzester Zeit auch die neuesten Schadprogramme entdecken, richten sich mehr und mehr Angriffe auf die Nutzer vor dem Bildschirm.

Können Sie zuverlässig eine Spammail mit Schadsoftware im Anhang von einem tatsächlichen Hinweis zur verspäteten Zahlung Ihres Telefonanbieters unterscheiden? Siegt nicht doch die Neugierde auf die Daten des neuen Bewerbers und der Anhang wird ganz ohne Virenscan und kritischem Blick auf Warnhinweise geöffnet? „Ich hätte niemals erkannt, dass es sich hier um einen Angriffsversuch Cyberkrimineller handelt“, bekommt Simone Uecker von erschrockenen Kursteilnehmern oft zu hören, wenn eine Windows-Systemwarnung über ihren Bildschirm flackert und die Beraterin damit ein seriös wirkendes, reales Beispiel eines Angriffs simuliert. „Wir müssen lernen, die Tricks Cyberkrimineller zu enttarnen“, ist der Aufruf der Beraterin ans Praxisteam.

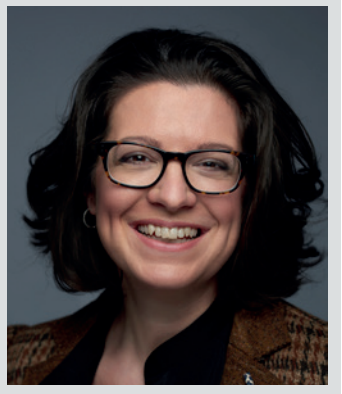
Wer die Methoden und Vorgehensweisen von Cyberkriminellen kennt, kann lernen, schnell und intuitiv verdächtige E-Mails oder Anrufe zu identifizieren und nicht in die Falle zu tappen. Zugleich müssen alle Mitarbeiter wissen, wie sie sich verhalten sollen, wenn es doch zum Angriff kommt – keiner darf Warnzeichen ignorieren, lieber einmal zu vorsichtig, als im falschen Moment nicht zu reagieren!

Die digitale Welt dreht sich so schnell, dass es hier mit einer einmaligen Schulung nicht getan ist. Ideal ist es, wenn nach einer intensiven Grundschulung des Praxisteams zumindest ein interessierter Mitarbeiter am Ball bleibt und das Team regelmäßig informiert. „Das Internet ist Freund und Feind zugleich“, bestätigt Simone Uecker. Zwar geht vom weltweiten Datennetz die größte Bedrohung aus, doch es ist auch die umfangreichste und aktuellste Informationsquelle zum Thema Cybersicherheit. So bietet die Verbraucherzentrale NRW eine ständig aktualisierte Übersicht von Phishing-Mails. Bei verdächtigen Mails kann diese Seite helfen, die schwarzen Schafe zu identifizieren. Außerdem empfiehlt die Beraterin Tools wie Google Alerts, um mit wenig Aufwand einen aktuellen Überblick über Themen rund um Cyberkriminalität zu behalten.

Fazit

Datensicherheit ist in Zeiten trickreicher Cyberattacken längst keine technische IT-Aufgabe mehr. Das gesamte Praxisteam ist gefordert, mit offenen Augen und Ohren durch die Praxis zu gehen und mit aktuellem Wissen um mögliche Angriffe zur „Human Firewall“ der Praxis zu werden. Wer sich bereits mit der Umsetzung der Europäischen Datenschutz-Grundverordnung befasst, sollte die Gelegenheit ergreifen und nicht nur Papierarbeit leisten, sondern einen ehrlichen und kritischen Blick auf seine technischen und organisatorischen Maßnahmen zur Datensicherheit in der Praxis werfen. Firewall, echte Systemtrennung zwischen Praxisnetz und Internet, Back-up & Co. bieten viele Stolperfallen und sind vielfach unzureichend konfiguriert, ohne dass Betreiber davon wissen. Die Praxis kann von effizienten Maßnahmen und echter Datensicherheit – auch im Fall von Brand oder Festplattencrash – nur profitieren. KN

KN Kurzvita



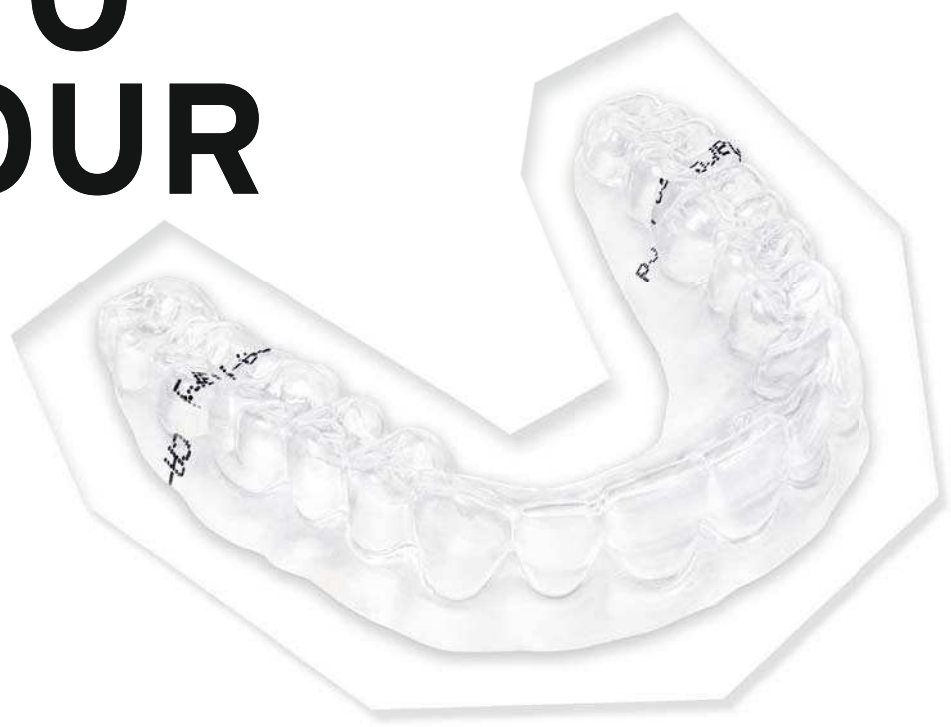
Mag. (FH) Simone Uecker
[Autoreninfo]

KN Adresse

Mag. (FH) Simone Uecker
4MED Consult
Amselweg 8
82194 Gröbenzell
Tel.: 0176 62279280
info@4med-consult.de
www.4med-consult.de

CLEAR ALIGNER

START TO LOVE YOUR SMILE.



44 Mio Reichweite

82.000 Webseitenbesucher

18.000 Arztsuchen

Werden auch Sie ein Teil unserer Kampagne!

Profitieren Sie jetzt von unserer aufmerksamkeitsstarken Kampagne „Start to Love your Smile“: Erhalten Sie unser kostenloses, innovatives Marketing-Kit und lassen Sie sich auf unserer hochfrequentierten Kampagnen-Seite listen!

Informationen wie Sie teilnehmen können erhalten Sie unter:

Kampagne@ca-digit.com

CA DIGITAL