Zum aktuellen Thema weltweiter Cyberattacke vom 12.05.2017

Wie man die Zahnarztpraxis gegen

Foto: Natalia Merzlyakova - Fotolia

Stellen Sie sich vor, Sie kommen morgens in die Praxis, fahren die EDV-Systeme hoch und nichts funktioniert mehr: Kein Zugriff auf die Patientenakten, keine Verbindung zu externen Anbietern, die Diagnosen der Patienten sind verschlüsselt und digitale Röntgenbilder stehen nicht zur Verfügung. – Sie wurden das Opfer einer Cyberattacke. – Alles nur Angstmacherei?

Wana Decrypt0r 2.0 legt Krankenhäuser lahm

Genau dies geschah am 12.05.2017 in zahlreichen Krankenhäusern des englischen National Health System. Angestellte konnten sich nicht an Computern in den Kliniken anmelden. Sie wurden durch ein Popup aufgefordert, ein Lösegeld zu zahlen, um wieder Zugang zu den Daten zu erhalten. Ebenso davon betroffen waren an das Netzwerk angeschlossene Geräte wie Drucker, Kartenlesegeräte oder bildgebende Verfahren. Der Angriff fand zeitgleich weltweit statt. So war z. B. in Deutschland die Deutsche Bahn betroffen, bei der die Anzeigetafeln noch Tage nach dem Angriff nicht richtig funktionierten.

Auswirkungen eines Hackerangriffs auf eine Praxis

In Abhängigkeit des Digitalisierungsgrades einer Zahnarztpraxis hätte ein solcher Angriff unterschiedliche Folgen. Praxen mit niedrigen Digitalisierungsgrad kommen noch glimpflich davon, diese können Daten, wie Patienteninformationen oder Termineinträge der letzten Tage manuell nachtragen, sobald die EDV wieder funktioniert. Anders verhält es sich bei Praxen mit hohem Digitalisierungsgrad. Sobald die vernetzte Dentaleinheit, inkl. intraoraler Kamera, Patientenakte und Röntgenbildern nicht zur Verfügung steht, kann es zu einem tagelangen Praxisausfall kommen.

Wie Sie Ihre Praxis gegen Cyberangriffe schützen

Experten sind sich einig, dass nach diesem „erfolgreichen Hackerangriff“ der nächste Versuch einer Cyberattacke nur noch eine Frage der Zeit ist. Im aktuellen Fall ging es um eine Lösegelderpressung. Doch was, wenn sensible Patientendaten mit Diagnosen abgegriffen und veröffentlicht werden? Hier kommt schnell der Straftatbe-

Cyberangriffe schützt

Marcus Tausend

stand des § 203 StGB ins Spiel. Dies führt zwangsläufig auch zu einer Aufwands- und Kostenbelastung und möglicherweise auch zu einem Reputationsschaden für die Zahnarztpraxis. Höchste Zeit also, sich mit dem Thema Cybersicherheit in der Praxis zu beschäftigen. Der professionelle Schutz der Praxis vor Cyberangriffen minimiert die Gefahr eines erfolgreichen Cyberangriffs, beschleunigt die Wiederherstellung der Systeme und unterstützt den Inhaber bei finanziellen Belastungen wie beispielsweise dem Ausfall der Praxis.

Sicheres Praxis-EDV-Management und -Bewusstsein unerlässlich

Die Cybersicherheit in der Praxis beginnt neben einer systematisch aufgestellten IT-Infrastruktur immer mit dem Gefahren-Bewusstsein des Inhabers. Diese Managementaufgabe beinhaltet die Aufstellung eines detaillierten Notfallplans für den Fall einer Cyberattacke und die Sensibilisierung aller Mitarbeiter durch entsprechende Schulungen. Im Falle eines Angriffs geht es dann darum, die gelernten Strategien sofort umzusetzen, um den möglichen Schaden für die Praxis zu minimieren.

Ein sicheres IT-System beinhaltet folgende Punkte:

- Virenschutz auf Servern und Systemen mit aktuellen Virensignaturen
- Firewall-Strukturen an allen Netzübergängen zu externen Netzen
- Abgestuftes Rechtekonzept mit administrativen Kennungen ausschließlich für IT-Verantwortliche und
- Regelmäßige, mindestens tägliche Datensicherung auf separierten Systemen oder Datenträgern

Cyberversicherung – wenn doch mal was passiert

Doch auch das beste Management- und EDV-System bietet keinen 100-prozentigen Schutz. Gute Anti-Viren-Programme können jedoch die Dauer zwischen dem Auftreten einer neuen Schadsoftware und dem sicheren Schutz dagegen verkürzen. Hier setzen sog. Cyberversicherungen an; ein ganz neuer Bereich der Absicherungen in Deutschland. Erst im April 2017 hat sich der Gesamtverband der Versicherungswirtschaft (GDV) auf eine einheitliche Vertragsgrundlage festgelegt. Anglo-amerikanische Versicherer mit langjähriger Erfahrung auf dem Gebiet „Cyberrisk“ machen heute noch einen Großteil der Risikoträger aus.

Tilo Schneider

Fremd- und Eigenschäden

Die Deckung wird in Fremd- und Eigenschäden unterteilt. Bei Fremdschäden erfolgt eine Erstattung des Schadens aufgrund von Verstößen gegen die Cyber-Sicherheit, den Datenschutz, Persönlichkeitsrechte und Geheimhaltungspflichten. In modernen Berufshaftpflichtversicherungen ist dieser Baustein bereits integriert.
Die Absicherung bei Eigenschäden bietet neben der Kostenerstattung umfangreiche Assistance-Leistungen für notwendige PR-Maßnahmen, oder um der Forderung im Zusammenhang mit angedrohter oder bereits erfolgter Erpressung und vor allem der Unterbrechung des Praxisbetriebes durch Ausfall der IT-Systeme nach einem Angriff zu entgehen.
Erfahrene Krisendienstleister, ein Rechtsbeistand und ein IT-Sicherheitsexperte unterstützt die Praxisinhaber nach einem Cyberangriff. Sie übernehmen das Krisenmanagement, sorgen durch IT-Forensiker dafür, dass die Schadenursache schnell identifiziert und beseitigt wird, schließen Sicherheitslücken und stellen Daten und Computersysteme wieder her. Darüber hinaus fungieren sie als rechtliche Vertretung z. B. ggü. Aufsichtsbehörden. Die Übernahme der gesetzlich vorgeschriebenen Information an alle von „Ihrem“ Cyber-Schaden Betroffenen (Patienten oder sonstige Dritte) runden diese Serviceleistungen ab.

Bange machen gilt nicht!

Das Thema Cybersicherheit wird zunehmend an Bedeutung gewinnen. Praxisinhaber sollten sich deshalb so früh wie möglich damit auseinandersetzen. Berücksichtigen sie die beschriebenen Maßnahmen, können sie Schäden durch Cyberkriminelle verhindern oder zumindest den entstandenen Schaden in Grenzen halten. Ihre IT-Dienstleister oder Versicherungs-Experten helfen sicher gerne dabei.

Autoren:

Marcus Tausend - Tausend Finanz GmbH
zertifizierter Berater Heilwesen mit Fokus auf Zahnarzt-Praxen
E-Mail: info@cyberrisk-praxis.de und info@zahnarzt-schutz.de
URL: www.zahnarzt-schutz.de

Tilo Schneider - croniq Ingenieurgesellschaft mbH
zertifizierter IT-Sicherheitsbeauftragter nach ISO 27001
E-Mail: tilo.schneider@croniq.de
URL: www.croniq.de