PRAXIS-IT // Hackerangriffe, Cybercrime, Internetkriminalität: Was nach spannender Unterhaltung wie „Krieg der Sterne“ oder „Matrix“ klingt, ist in Zeiten der zunehmenden Digitalisierung zur bitteren Realität geworden, die Zahnarztpraxen und andere Einrichtungen des Gesundheitswesens zunehmend bedroht.

PRAXISHACKING – BEDROHUNGEN ERNST NEHMEN

Mark Peters, Bettina Ritter / Heidelberg

Aber was ist „Cyberkriminalität“ eigentlich? Wie erkenne ich, dass meine Praxis Opfer eines Angriffs geworden ist? Und vor allem: Was können mein Team und ich tun, damit es nicht zu einem Schaden kommt? Solche und viele weitere Fragen stellen sich Niedergelassene immer häufiger.

Die Zahl der Cyberangriffe auf (Zahn-) Arztpraxen, Kliniken und weitere Akteure im Gesundheitswesen (bspw. auch Software-Hersteller) steigt seit Jahren stark an. Da die Methoden, mit denen die Attacken erfolgen, immer perfider werden, und die Täter zunehmend an Professionalität gewinnen, sollten Praxisinhaber unbedingt jetzt aktiv werden und in den Schutz ihrer EDV investieren. Erfahrungsgemäß ist der Schaden, wenn es passiert, beträchtlich. Neben den finanziellen Verlusten durch Verdienstausfall, die Zahlung von Lösegeld und/oder die Anschaffung neuer Rechner und Peripherie, entsteht auch ein erheblicher Imageschaden, denn welcher Patient vertraut noch seinem Zahnarzt, wenn dieser höchst sensible Gesundheitsdaten nicht zuverlässig schützt?

Wie erfolgen nun üblicherweise Cyberattacken? Für Zahnarztpraxen dürften vor allem diese drei Angriffsarten relevant sein:

– Zusendung sogenannter „Phishing-Mails“: Nach dem Öffnen des Anhangs (meist eine PDF-Datei) oder dem Anklicken eines in der E-Mail enthaltenen

Links installiert sich im Hintergrund eine Schadsoftware, die dann beispielsweise Daten ausspioniert.
- **Ransomware:** Hierbei handelt es sich um Schadprogramme, die den Zugriff auf bestimmte Programme (beispielsweise die Praxisverwaltungssysteme) oder sogar das komplette IT-System verschlüsseln. Nach der Zahlung von Lösegeld (englisch: „ransom") werden die Daten dann wieder freigegeben – oder auch nicht.
- Mit Schadsoftware bespielte **USB-Sticks** oder **CD-ROMs**: Es sind bereits Fälle bekannt geworden, in denen Zahnärzte ihre EDV infiziert haben, indem sie einen USB-Stick, den sie bei einer Fortbildungsveranstaltung als „Give-away" mitgenommen und, mit ihrem Rechner verbunden haben. Ähnliches ist auch schon mit CD-ROMs passiert, auf denen angeblich Röntgenaufnahmen enthalten waren.

Da die strafrechtliche Verfolgung der Täter äußerst schwierig ist, da diese oft aus dem Ausland operieren und Angriffe nicht immer gleich zu identifizieren sind, sollten Maßnahmen getroffen werden, die die Praxis davor schützen, dass eine Attacke – und dazu wird es früher oder später auf jeden Fall kommen – für die Täter zum Erfolg führen kann.

Um zu erfahren, ob zumindest ein Mindestmaß an Sicherheit vorhanden ist, sollten Sie als Praxisinhaber die folgenden Fragen alle mit „Ja" beantworten können:
- Habe ich die Anforderungen, die sich aus der IT-Sicherheitsrichtlinie nach § 75b SGB V ergeben, vollumfänglich umgesetzt?
- Sind meine Angestellten und ich sensibilisiert für dieses Thema?
- Sind das Betriebssystem, die Anti-Viren-Software, das Praxisverwaltungssystem, der TI-Konnektor und der Router auf aktuellem Stand (regelmäßiges Einspielen von Updates, Aktualisierung der Firmware etc.)?
- Sind die Rechner so aufgestellt, dass kein schneller Zugriff auf USB-Anschlüsse möglich ist?
- Werden regelmäßig (zumindest wöchentlich, besser jedoch täglich) Backups vom Praxisverwaltungssystem erstellt und die Datenträger an einem sicheren Ort außerhalb der Praxis aufbewahrt?
- Werden die Passwörter regelmäßig geändert und bestehen diese aus mindestens zwölf Zeichen (mit Groß- und Kleinschreibung und Sonderzeichen, keine Trivialnamen)?
- Habe ich einen Quick-Penetrationstest für Zahnarztpraxen durchgeführt?

Neben diesen Aspekten gibt es natürlich noch mehr Möglichkeiten, die Praxis vor Cyberattacken abzusichern. Am besten sprechen Sie hierfür in einem ersten Schritt Ihren IT-Dienstleister an.

Sollte es trotz aller Vorsichtsmaßnahmen doch zu einem Vorfall kommen, sind unbedingt die folgenden Punkte zu befolgen:
- Arbeit am IT-System sofort einstellen
- Praxis mit dem Hinweis auf eine „technische Störung" schließen
- IT-Dienstleister und die ZAC (Zentrale Ansprechstelle Cybercrime) informieren
- Sachverhalt und Beobachtungen dokumentieren
- Weitere Maßnahmen am System nur nach Anleitung durch Experten ergreifen
- Strafanzeige stellen
- Die Kassenzahnärztliche Vereinigung und gegebenenfalls die Kollegen vor Ort informieren
- Meldung der Datenschutzverletzung innerhalb von 72 Stunden
- Gegebenenfalls BSI Digitalen Ersthelfer anrufen

Wenn Sie über eine Cyberschutz-Versicherung verfügen, dann ist der Schadenfall umgehend zu melden. Die Versicherung wird dann alle weiteren Schritte, unter anderem die Beauftragung von IT-Forensikern, koordinieren.

PRAXISMANAGEMENT
BUBLITZ-PETERS
GMBH & CO. KG
Rohrbacher Straße 28
69115 Heidelberg
Tel.: +49 6221 438500
info@bublitz-peters.de
www.bublitzpeters.de