Gastbeitrag von Mark Peters

Praxishacking: Bedrohung ernst nehmen

Hacker-Angriffe, Cybercrime, Internetkriminalität: Was nach spannender Unterhaltung wie „Krieg der Sterne“ oder „Matrix“ klingt, ist in Zeiten der zunehmenden Digitalisierung zur bitteren Realität geworden, die Arztpraxen und andere Einrichtungen des Gesundheitswesens bedroht.

Dass Ihr Bildschirm so ein Bild zeigt, kann verhindert werden.

Was ist „Cyberkriminalität“? 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 Fragen kennt jeder Praxisinhaber.

In den vergangenen Jahren haben mindestens vier Prozent der Arztpraxen einen Schaden durch einen Cyberangriff erlitten, Tendenz stark steigend. Trotzdem ist ein Großteil der niedergelassenen Ärztinnen und Ärzte weiterhin davon überzeugt, dass ihre Praxis-EDV-Systeme ausreichend vor möglichen Angriffen geschützt sind. Die Realität sieht jedoch anders aus.

INVESTITIONEN SCHÜTZEN VOR ANGRIFFEN

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 Arzt, wenn dieser höchst sensible Gesundheitsdaten nicht zuverlässig schützt?

Wie erfolgen nun üblicherweise Cyberattacken? Für Arztpraxen 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 Schad-Software, die dann beispielsweise Daten ausspioniert.

Infobox

Die KV Hessen bietet zum Thema „Cyberkriminalität auf dem Vormarsch“ Fortbildungen an. Anmelden können Sie sich unter **www.kvhessen.de/fortbildungsprogramm**

Hier die nächsten Termine:

- Freitag, 19.03.2021, 16.00–18.00 Uhr als Online-Kurs
- Mittwoch, 15.09.2021, 15.00–19.00 Uhr in Espenau
- Freitag, 26.11.2021, 15.00–19.00 Uhr in der KV Frankfurt

- Ransomware: Hierbei handelt es sich um Schadprogramme, die den Zugriff auf bestimmte Programme (beispielsweise die Praxisverwaltungssysteme) oder sogar das komplette IT-System verschlüsseln. Nach Zahlung von Lösegeld (englisch: „ransom"), heutzutage üblicherweise in Bitcoins, werden die Daten dann wieder freigegeben – oder auch nicht.

- Mit Schad-Software bespielte USB-Sticks oder CD-ROMs: Es sind bereits Fälle bekannt geworden, in denen Ärzte ihre EDV infiziert haben, indem sie einen USB-Stick, den sie bei einer Fortbildungsveranstaltung als „Give-Away" mitgenommen haben, mit ihrem Rechner verbunden haben. Ähnliches ist auch schon mit CD-ROMs passiert, auf denen angeblich Röntgenaufnahmen enthalten waren.

Geht es bei Angriffen auf große Unternehmen und staatliche Einrichtungen oft um (Wirtschafts-) Spionage, so dürften Arztpraxen vornehmlich zur Erpressung von Lösegeld ausgesucht werden.

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:

- 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) Back-ups vom Praxisverwaltungssystem erstellt und die Datenträger an einem sicheren Ort außerhalb der Praxis aufbewahrt?

- Werden die Passwörter regelmäßig geändert und bestehen diese aus mindestens acht Zeichen (mit Groß- und Kleinschreibung und Sonderzeichen, keine Trivialnamen)?

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.

Mark Peters von der Praxismanagement Bublitz-Peters GmbH & Co. KG in Heidelberg ist ein externer Datenschutzbeauftragter, Auditor mit Heidelberger Cyberschutz-Rating-Zertifizierung und geprüfter IT-Grundschutz (BSI)-Praktiker.

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, Tel. 0611 83-8377 zac.hlka@polizei.hessen.de) informieren
- Sachverhalt und Beobachtungen dokumentieren
- Weitere Maßnahmen am System **nur nach Anleitung durch Experten** ergreifen
- **Strafanzeige** stellen
- Die Kassenärztliche Vereinigung und gegebenenfalls die Kollegen vor Ort informieren
- **Meldung der Datenschutzverletzung** innerhalb von 72 Stunden

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. ■

Mark Peters

Weitere Informationen unter:

Bundesamt für Sicherheit in der Informationstechnik:
www.bsi.bund.de

Allianz für Cybersicherheit:
www.allianz-fuer-cybersicherheit.de

Zentrale Ansprechstelle Cybercrime
www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html