RATGEBER // Der folgende Artikel widmet sich dem aktuell brisanten Thema der Cyberkriminalität. Es ist wichtig zu wissen, auf welchem Weg die eigene Praxis angegriffen werden kann, wie Praxisinhaber und Angestellte sich vor einem Angriff schützen können und wie sie reagieren sollten, falls es zu einem Schaden kommt.

CYBERSICHERHEIT IN DER ZAHNARZTPRAXIS

Mark Peters / Heidelberg

Hacker-Angriffe, Cybercrime, Internetkriminalität: Was zunächst nach spannender Unterhaltung im Stile von „Krieg der Sterne" oder „Matrix" klingt, ist in Zeiten zunehmender Digitalisierung leider zur bitteren Realität geworden, die immer mehr Arztpraxen und andere Einrichtungen des Gesundheitswesens bedroht.

Die Praxis-IT und der damit verbundene Cyberschutz sind ein komplexes Feld. Cyber-Sicherheit umfasst alle Aspekte der Sicherheit in der Informations- und Kommunikationstechnik, sowie den so genannten Cyber-Raum. Dieser beinhaltet alle mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik sowie die darauf basie-

rende Kommunikation, Anwendungen und Informationen.

Internetkriminalität kann Menschen überall, wo Computer, Smartphones und andere IT-Geräte benutzt werden, treffen. Demnach werden Straftaten, bei denen die Täter moderne Informationstechnik nutzen, allgemein als Cyberkriminalität bezeichnet. Dies kann zum Beispiel ein Betrugsversuch sein, der das potenzielle Opfer per E-Mail statt per Post erreicht.

In den vergangenen Jahren haben mindestens vier Prozent der Arztpraxen einen Schaden durch einen sogenannten Cyberangriff erlitten – Tendenz: stark steigend. Trotzdem ist ein Großteil der niedergelassenen Ärztinnen und Ärzte weiterhin davon überzeugt, dass die Systeme zur elektronischen Datenverarbeitung (EDV) in ihrer Praxis ausreichend vor möglichen Angriffen geschützt sind. Die Realität sieht jedoch häufig anders aus, wie die skizzierte Entwicklung zeigt.

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-Anlagen investieren. Erfahrungsgemäß ist der Schaden, wenn es zu einem Angriff gekommen ist, beträchtlich. Neben den finanziellen Verlusten durch Verdienstausfälle, die Zahlung von Lösegeld und/oder die Anschaffung neuer Rechner und der zugehörigen Peripherie, entsteht auch ein erheblicher Imageschaden: Denn welcher Patient vertraut einem Arzt, der höchst sensible Gesundheitsdaten nicht zuverlässig schützt?

Wie erfolgen Cyberattacken üblicherweise?

Für Arztpraxen sind vor allem die folgenden drei Angriffsarten relevant:

- Phishing-Mails: Nach dem Öffnen des Email-Anhangs, meist eine PDF-Datei, oder dem Anklicken eines in der Email enthaltenen Links, installiert sich im Hintergrund eine Schad-Software, die dann beispielsweise Daten auf dem Rechner oder System ausspioniert.
- Ransomware: Hierbei handelt es sich um Schadprogramme, häufig als Trojaner bekannt, die den Zugriff auf bestimmte Programme (beispielsweise die Praxisverwaltungssysteme) oder sogar das komplette IT-System verschlüsseln. Sie können auf USB-Sticks und CDs, durch E-Mail-Anhänge, das Surfen auf unsicheren Internetseiten oder den Download ungeprüfter kostenloser Programme aus dem Internet ins System gelangen. Nach Zahlung eines Lösegelds (englisch: „ransom") werden die Daten dann in der Regel wieder freigegeben.
- 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 als „Give-Away" mitgenommen haben, mit ihrem Rechner verbunden haben. Ähnliches ist auch schon mit CD-Roms passiert, auf denen angeblich Röntgenaufnahmen enthalten sein sollten. Daher ist es unbedingt empfehlenswert, die Quelle eines solchen Datenträgers genau zu kennen und als vertrauenswürdig einstufen zu können.

Während es bei Angriffen auf große Unternehmen und staatliche Einrichtungen oft um (Wirtschafts-) Spionage geht, werden Arztpraxen vorrangig Ziel von Erpressungsversuchen mit Lösegeldforderung (siehe Infobox).

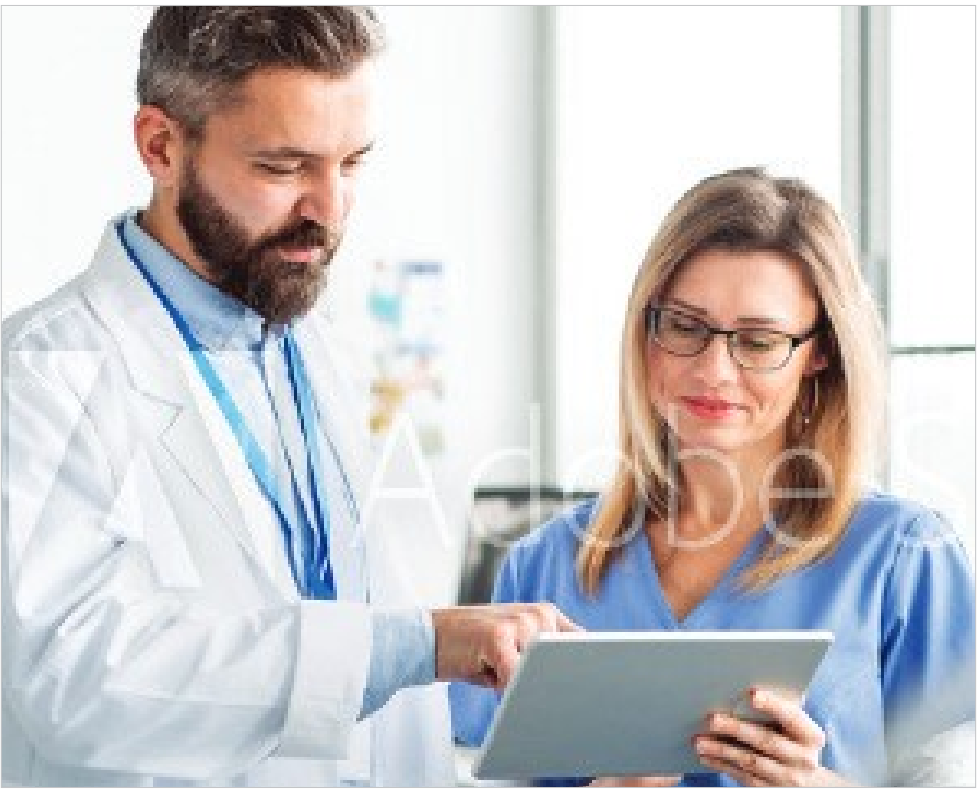
Beispiel einer Email-Erpressung vom 20.10.2020

Ich grüße dich!

Ich habe schlechte Nachrichten für dich.
10.12.2019 – An diesem Tag habe ich mich in dein Betriebssystem gehackt und vollen Zugriff auf dein Konto erhalten. Das Passwort muss nicht geändert werden, meine Malware fängt es jedes Mal ab.
Wie war es: Es gab eine Sicherheitslücke in der Software des Routers, mit dem Sie an diesem Tag verbunden waren. Ich habe mich zuerst in diesen Router gehackt und dort meinen Schadcode abgelegt. Als Sie ins Internet gingen, wurde mein Trojaner auf dem Betriebssystem Ihres Geräts installiert. Danach habe ich eine vollständige Sicherung Ihres Laufwerks erstellt (Websitesverlauf, alle Dateien, Telefonnummern und Adressen all Ihrer Kontakte).
Vor einem Monat wollte ich Ihr Gerät sperren und um etwas Geld bitten, um es zu entsperren. Aber ich habe mir die Websites angesehen, die Sie regelmäßig besuchen, und es hat mir wirklich Spaß gemacht, Ihre Lieblingsressourcen zu sehen. Ich spreche von Websites für Erwachsene.
Ich bin der festen Überzeugung, dass Sie diese Fotos Ihren Verwandten, Freunden oder Kollegen nicht zeigen möchten. Ich denke, 399 EUR sind ein sehr kleiner Betrag für mein Schweigen.
Ich akzeptiere Geld nur in Bitcoins. Meine BTC-Brieftasche:
3LbyjEJCLPd54tbP3RsAAswbREPWfkFAJt
Sie wissen nicht, wie Sie eine Bitcoin-Brieftasche auffüllen sollen? Schreiben Sie in eine Suchmaschine „Wie kaufe ich BTC?". Es ist einfacher als Geld auf eine Kreditkarte zu senden! Für die Zahlung haben Sie genau 24 Stunden Zeit. Keine Sorge, der Timer startet, sobald Sie diesen Brief öffnen. Ja, ja … es hat bereits begonnen!
Nach der Zahlung zerstören sich mein Virus und Ihre schmutzigen Fotos mit Ihnen. Wenn ich den angegebenen Betrag nicht von Ihnen erhalte, wird Ihr Gerät blockiert und alle Ihre Kontakte erhalten ein Foto mit Ihren „Freuden".

Sei mir nicht böse, jeder hat seinen Job.
Abschied.

PS: Ich garantiere, dass ich Sie nach der Zahlung nicht wieder stören werde, weil Sie nicht mein einziges Opfer sind. Dies ist ein Ehrenkodex für Hacker.



Die strafrechtliche Verfolgung der Täter wird durch den weltweiten Aktionsradius erschwert. Zudem sind Angriffe in der Regel nicht leicht zu identifizieren. Daher sollten Maßnahmen getroffen werden, die die Praxis vor einer Attacke schützen.

Schutz für die Praxis

Um zu erfahren, ob zumindest ein Mindestmaß an Sicherheit vorhanden ist, sollten die folgenden Fragen alle mit „Ja" beantwortet werden können:

- Sind meine Angestellten und ich sensibilisiert für dieses Thema oder bedarf es eventuell einer Schulung?
- Sind das Betriebssystem, die Anti-Viren-Software, das Praxisverwaltungssystem, der TI-Konnektor und der Router auf dem aktuellen Stand (regelmäßiges Einspielen von Updates, Aktualisierung der Firmware etc.)?
- Sind die Rechner so in der Praxis lokalisiert, dass Externen kein schneller Zugriff auf USB-Anschlüsse gewährt wird?
- Werden regelmäßig (zumindest wöchentlich, besser jedoch täglich) Sicherungskopien (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 viele weitere Möglichkeiten, die Praxis vor Cyberattacken abzusichern. Am besten sprechen Sie hierfür in einem ersten Schritt Ihren IT-Dienstleister an.

Im Schadensfall

Sollte es trotz aller Vorsichtsmaßnahmen doch zu einem Vorfall kommen, sind unbedingt die folgenden Punkte zu befolgen:

- Die Arbeit am IT-System ggf. sofort einstellen.
- Den Cyberschutzbeauftragten der Praxis informieren.
- Cyberabwehrnetzwerk-Praxismanagement Bublitz-Peters informieren.
- Die 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 zuständige Kassenärztliche Vereinigung und gegebenenfalls die Kollegen vor Ort informieren.
- Die Datenschutzverletzung innerhalb von 72 Stunden melden.

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

Da dieser Artikel nur einen kurzen Abriss über die Thematik geben kann, sei zum Schluss noch an folgende Stellen verwiesen:

- 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
- Praxismanagement Bublitz-Peters: www.cyberschutzzertifizierung.info

MARK PETERS
Praxismanagement Bublitz-Peters GmbH & Co. KG
Externer Datenschutzbeauftragter
Auditor Heidelberger Cyberschutz-Rating Zertifizierung
Geprüfter IT-Grundschutz (BSI)-Praktiker
Heidelberg