PATIENTENKARTEI

CYBER-ATTACKE auf die Praxis: WAS NUN?

Ein Beitrag von Dr. Tobias Witte

RECHT /// Die Vorweihnachtszeit mag ein friedvolles Miteinander aller suggerieren, Gefahren aber bleiben Gefahren: Für viele Praxisinhaber scheint das Thema IT-Sicherheit im Alltag nicht ganz oben auf der Agenda zu stehen. Spätestens jedoch, wenn Hacker sich Zugriff auf die Praxis-IT verschaffen und die Patientenkartei kapern, wird das Thema blitzartig real.

Infos zum Autor

Mithilfe sogenannter Ransomware (Erpressersoftware) kann es digitalen Kriminellen gelingen, die wertvollen Patientendaten gleichsam zu entführen: Diese werden verschlüsselt, der Praxisinhaber hat plötzlich keinen Zugriff mehr, die Hacker sehr wohl. Was folgt, ist eine waschechte Erpressung: Die Hacker verlangen teils horrende Lösegeldzahlungen und drohen an, im Falle der Nichtzahlung oder beim Einschalten der Polizei die Daten nicht wieder freizugeben oder diese sogar im Darknet gewinnbringend zu verkaufen oder dort öffentlich zu machen.

Reales Gefahrenpotenzial

Hackerangriffe auf (Zahn-)Arztpraxen treten immer häufiger auf und werden stets gefährlicher. Davon betroffen sind jedoch nicht nur Großunternehmen, auch kleinere Praxen können zur Zielscheibe eines solchen Cyberangriffs werden. Eine Studie des Branchenverbands Bitkom beziffert den Schaden für die deutsche Wirtschaft durch Cyberkriminalität auf jährlich 223 Milliarden Euro. Ist das Erbeuten von Daten an sich stets für die betroffenen Unternehmen ein großes Problem, so verschärft sich dies im Gesundheitswesen nochmals aufgrund der besonderen Sensibilität von Gesundheitsdaten vor dem Hintergrund der Datenschutz-Grundverordnung (DSGVO) sowie der zahnärztlichen Schweigepflicht und des zahnärztlichen Berufsrechts.

Die wichtigsten Sofortmaßnahmen im Überblick

Daher bietet es sich für Praxisinhaber an, sich bereits frühzeitig mit einer solchen potenziellen Situation auseinanderzusetzen und einen Notfallplan zu haben, um im Ernstfall vorbereitet zu sein und den Schaden minimieren zu können. Es gibt bestimmte Maßnahmen, die Betroffene nach einem Hackerangriff durchführen (lassen) sollten:

Schadensbegrenzung_ Zuerst ist die eigene IT-Abteilung bzw. der IT-Dienstleister, falls vorhanden, zu kontaktieren und auf den Ernst der Lage hinzuweisen. Sie sollten sich am Anfang darauf konzentrieren, dass durch den Cyberangriff kein weiterer Schaden entstehen kann. Sind Internetaccounts betroffen, vor allem E-Mail-Clients, so sind schnellstmöglich die kompromittierten Passwörter zu ändern, falls technisch noch möglich. Insbesondere bei kompromittierten E-Mail-Accounts ist Vorsicht geboten. Diese fungieren oft als zentrale Schaltstelle, um Passwörter anderer Dienste per E-Mail zurückzusetzen. Überprüfen Sie bzw. lassen Sie überprüfen, ob möglicherweise neue Passwörter für verknüpfte Konten beantragt wurden. Diese sollten vorsichtshalber in jedem Fall geändert werden, denn der Hacker könnte diese E-Mails bereits gelöscht haben. Ein neues Passwort sollte jeweils gewissen Qualitätsanforderungen genügen, es sollte möglichst lang sein und aus einer Kombination von

C:\>DEL
YOU HAVE BEEN HACKED_

Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Selbiges gilt für Serverzugänge und sonstige Log-ins.

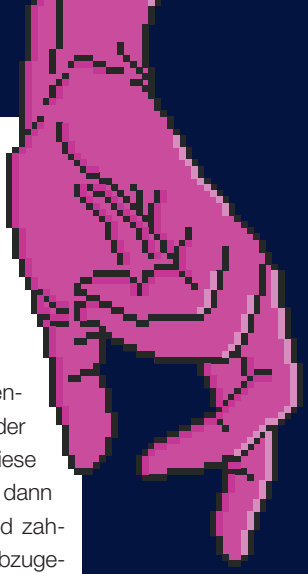
Bewusst offline gehen – und löschen_ Die Rechner bzw. Server mit der Patientenkartei sollten Sie sofort ausschalten und vom Internet trennen. Dadurch kann zunächst vermieden werden, dass das Schadprogramm weiterarbeiten kann und zusätzliche Daten übertragen werden. Dies dient der Schadensbegrenzung. Daraufhin ist es ratsam, alle auf diesem Gerät verwendeten Passwörter zu ändern, diese könnten bereits vom Angreifer abgefragt worden sein. Anschließend kann die Festplatte des Geräts nach einer fachmännischen Begutachtung gelöscht und das System neu installiert werden. Da Sie nicht wissen, ob der Angriff weiter gestreut ist bzw. in welchem Umfang sich der Angriff ereignet hat, ist es wichtig, die Festplatte vollständig zu löschen. Davor kann versucht werden, etwaige wichtige Daten zu retten, allerdings birgt dies die Gefahr der weiteren Verbreitung der Schadsoftware. Hier kann nur ein IT-Fachmann helfen. Es wird anschließend ganz elementar auf – hoffentlich in jeder Praxis vorhandene – Back-ups ankommen.

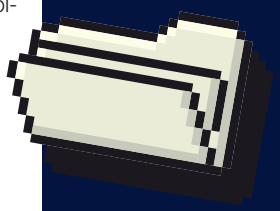
Meldepflichten beachten_ Der erfolgte Angriff kann erhebliche rechtliche Auswirkungen auf Ihre Compliance-Vorgaben mit sich bringen. Höchstwahrscheinlich müssen datenschutzrechtliche Meldepflichten eingehalten werden. Diese sind in einer solchen Situation zweigeteilt: Es gibt zum einen die Meldepflicht an die Datenschutz-Aufsichtsbehörde nach Art. 33 DSGVO mit dem Inhalt, möglichst unverzüglich, spätestens aber binnen 72 Stunden nach Kenntnis von der Attacke, die Behörde zu informieren. Zum anderen gibt es eine Benachrichtigungspflicht gegenüber den betroffenen Dritten nach Art. 34 DSGVO – also den Patienten. Hier wird es für Praxisinhaber höchst schmerzhaft: Das Gesetz verpflichtet dazu, die Patienten in so einem Fall unverzüglich über das Datenleck zu informieren. In diesem Bereich entstehen sodann komplexe Folgeprobleme, etwa aufgrund der Frage, wie man ein Rundschreiben an alle betroffenen Patienten aus der Praxis umsetzen soll, wenn die Patientendaten gekapert wurden und ein Zugriff im schlimmsten Fall auch auf Back-ups nicht mehr möglich ist. Hier gilt es, sich möglichst schnell fachkundig rechtlich beraten zu lassen. Bei beiden Meldepflichten existieren darüber hinaus gesetzliche Vorgaben an den genauen Inhalt der zu meldenden Informationen. Ein Verstoß entgegen dieser Meldepflichten ist bußgeldbewehrt.

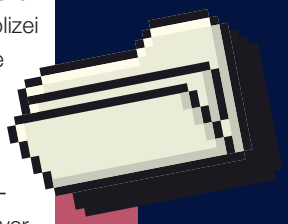
Lösegeld zahlen?_ Wenn sich die Patientendaten technisch durch Ihre IT-Abteilung oder aber externe Dienstleister, die auf Fälle wie diese spezialisiert sind, nicht entschlüsseln lassen, dann stellt sich die Frage: Soll man das Lösegeld zahlen? Dazu ist keine generelle Empfehlung abzugeben, es kommt auf die konkreten Umstände des Einzelfalls an. Sehr hilfreich können hier aber sogenannte Cyber-Versicherungen sein: Je nach Ausgestaltung und Police decken diese die unterschiedlichsten Schäden, die mit einer solchen Ransomware-Attacke einhergehen, konsequent ab. Dies kann die IT-Kosten für die Wiederherstellung des Systems, die Anwaltskosten im Zusammenhang mit der Rechtsverfolgung und sogar das Lösegeld selbst umfassen. Ist eine solche Versicherung vorhanden, ist diese ebenfalls schnellstmöglich nach Bekanntwerden der Attacke zu informieren. Lösegeldzahlungen in derartigen Ransomware-Fällen sind ferner sogar steuerlich absetzbar.

Strafanzeige erstatten_ Es ist im Einzelfall durchaus empfehlenswert, Anzeige bei der Polizei oder Staatsanwaltschaft zu erstatten. Manche Versicherungen setzen eine solche Anzeige für die Deckungsteilung der Schäden voraus.

Ursachenforschung und Fehlerbehebung_ Im Nachgang der hoffentlich glimpflich verlaufenen Cyberattacke gilt es, nach den Ursachen des Problems zu suchen, Schwachstellen in der IT auszumachen und daraus zu lernen. Dabei sollte der eigene Datenschutzbeauftragte, falls vorhanden, ebenso miteinbezogen werden wie die interne oder extern IT-Abteilung. Höchstwahrscheinlich müssen im Nachlauf der Attacke die technischen und organisatorischen Maßnahmen der Praxis – wie Passwortmanagement, Back-ups, Firewall, Virenschutz, Mitarbeitersensibilisierung, Verschlüsselung und vieles mehr – überarbeitet werden. Häufig entstehen Sicherheitslücken aus Unachtsamkeit des Personals, sodass in vielen Fällen eine Schulung für die Mitarbeiter sinnvoll ist.







DATEN LÖSCHEN?

Und die Moral von der Geschicht …

… am falschen Ende sparen lohnt sich nicht: Gut beraten ist, wer jetzt, falls noch nicht geschehen, in seine IT-Sicherheit investiert. Im Jahr 2024 wird das Thema mit der Umsetzung der EU-Cybersicherheitsrichtlinie NIS2 ohnehin für viele Praxen nochmals an Bedeutung gewinnen.
Häufig sind die Kosten dafür weniger hoch, als man denkt, da bereits mit einfachen Mitteln wie Firewall, Virenschutz und vernünftigem Passwortmanagement viel gewonnen ist. Dies betrifft auch die angesprochenen Cyber-Versicherungen, die vor einem Hackerangriff ein gutes Gefühl der Sicherheit vermitteln und danach bares Geld sparen helfen.

Damit Sie im Falle einer Cyberattacke auf die Praxis schnell die richtigen Entscheidungen treffen können, haben wir die wichtigsten To-dos in unserer Checkliste zusammengefasst.

INFORMATION ///

Dr. Tobias Witte
Rechtsanwalt & Partner
Fachanwalt für Medizinrecht
Fachanwalt für IT-Recht
Justiziar | Datenschutzbeauftragter
www.kwm-law.de

CHECKLISTE CYBERATTACKE

Betroffene Geräte in der Praxis ausschalten, **physisch vom Netzwerk und vom Internet trennen.**

IT-Dienstleister informieren und diesem jedwede technische Arbeit vor Ort umgehend ermöglichen (Datensicherung, Back-ups, Wiederherstellung etc.).

In Betracht kommende **Passwörter in Absprache mit IT-Dienstleister ändern** – E-Mail-Accounts, Log-ins der Praxis-EDV, Social Media usw.

Versicherung und Rechtsanwalt informieren.

Prüfen, ob von der Praxis aus E-Mails im Namen des Inhabers an Dritte verschickt wurden **(Identitätsdiebstahl)**.

Lösegeldzahlung?

Prüfung und Umsetzung der Meldepflicht **an die Behörde** (unter Einbeziehung des Rechtsanwalts).

Prüfung und Umsetzung der Meldepflicht **an die Patienten** (unter Einbeziehung des Rechtsanwalts).

Strafanzeige erstatten.

Das eigene IT-System in der Praxis auf Schwachstellen **überprüfen und verbessern.**