Praxis

Cybercrime rollt auf Ärzte zu

Datenschutz. Da Kliniken und Krankenanstalten die Sicherung von sensiblen Daten meist zentral lösen, trifft das höchste Risiko die niedergelassenen Ärzte. Dieses Risiko besteht vorwiegend im Verlust oder ungewollter Veröffentlichung von Patientendaten. Der Schaden daraus ist immer finanzieller Natur, der mitunter den Ruin des Arztes bedeuten könnte.

Von Andreas Reinthaler

Die Digitalisierung hat uns bereits fest im Griff und sie bringt uns Vor- wie auch Nachteile. Die positiven Beispiele sind z. B. die relativ schnelle und einfache Abrechnung mit den Krankenkassen, ein geringer Verwaltungsaufwand, schneller Zugriff auf Patientendaten und die Vernetzung mit anderen behandelnden Stellen. Die Nachteile sind hohe Kosten für Anschaffung, Problemen bei der Datenübertragung, unzureichende Sicherheit und allgemeine Gefahr im Gesundheitswesen wie Diebstahl von Patientendaten. Im Folgenden lesen Sie, wo die Gefahren für einen Datenmissbrauch lauern.

Alarm in der Praxis – aktuelle Faktenlage

So gut wie keine Praxis ist bei der Mail-Verschlüsselung up-to-date (Statistik Branchenreport GDV 2018).

- 88 Prozent empfinden steigende Cyberkriminalität als Nachteil der Digitalisierung.
- 78 Prozent der Arztpraxen wären ohne funktionierende IT-Systeme deutlich eingeschränkt.
- 80 Prozent meinen, sie wären ausreichend gegen Cyberkriminalität geschützt.
- 33 Prozent der Ärzte planen keine weiteren Investitionen in die ITSicherheit.

Auch die weiterführende Statistik ist erschreckend:

- 17 Prozent der Ärzte haben automatische Sicherheitsupdates und aktuelle Systeme.
- 18 Prozent machen mindestens zweimal pro Woche eine Sicherungskopie.
- 20 Prozent haben Administratoren-Rechte nur bei einem Administrator.
- 20 Prozent schützen auch Systeme, die über das Internet erreichbar sind (Webseite, App).
- 20 Prozent verhindern aktiv Zugriffe und Manipulationen auf Sicherungskopien.
- 20 Prozent schützen und aktualisieren Systeme vor Schadsoftware (Viren, Würmer, usw.).
- 21 Prozent haben Sicherungskopien auch physisch getrennt vom System (Safe).
- 18 Prozent verlangen Mindestanforderung an Passwörter (Länge, Zeichen usw.).
- 38 Prozent statten jeden Nutzer mit eigenem Zugang und Passwort aus.
- 45 Prozent testen regelmäßig die Wiederherstellung aus Sicherheits- Backups.

Angesichts dieser Zahlen müsste jedem Arzt sofort Angst und Bang werden und in der Sekunde jeder seinen IT-Experten mit der 100-prozentigen Absicherung beauftragen. Das nicht zu tun, gilt als grob fahrlässig.

Welche konkreten Online-Risiken haben Ärzte?

Als übliches Praxisbeispiel gilt mittlerweile ein Hacker-Angriff . Dabei greifen Hacker das IT-System einer Arztpraxis mit einer „Brute-Force-Attacke" an. Sie verschaffen sich über ein geknacktes Passwort Zugang zum System und kopieren die Patientendaten. Dann wird die Zahlung von Lösegeld erpresst, um auf eine Veröffentlichung der Daten zu verzichten.

Auswirkungen der Hacker-Angriffe:

1. Angriff. Die Arztpraxis erhält per Mail einen Erpresserbrief. Die Kriminellen behaupten, im Besitz aller Patientendaten zu sein. Als Beleg senden sie kompromittierende Daten über z. B. fünf Patienten, die tatsächlich in der betroffenen Praxis in Behandlung waren. Sie drohen damit, die Daten zu veröffentlichen, wenn der Arzt nicht bereit ist, ein hohes Lösegeld zu zahlen.

2. Informationen an Patienten und Behörden. Nach Rücksprache mit Polizei und Staatsanwaltschaft zahlt der Arzt kein Lösegeld. Er muss aber die Datenschutzbehörde und seine Patienten über den Verlust der sensiblen Daten informieren. Um sicher zu gehen, dass er seinen Pflichten in vollem Umfang nachkommt, holt er sich Hilfe bei einem Rechtsanwalt. Die Patienten sind nach der Information verunsichert und haben intensiven Gesprächsbedarf.

Die Kosten für solch einen Zeitaufwand wirken sich finanziell deutlich aus:

- Informationszeit mit/für Patienten: 4.000 Euro
- Anwaltskosten: 2.000 Euro

3. Security-Initiative. IT-Spezialisten suchen und schließen die Schwachstelle, die den Tätern Zugriff auf die Daten erlaubte. Die Systeme werden desinfiziert und gehärtet.

- Kosten für IT-Forensik: 5.000 Euro

4. Betriebsunterbrechung. Bis die Schwachstellen geschlossen sind und weitere Datendiebstähle verhindert werden, bleibt die Arztpraxis geschlossen. Auch die Abrechnung mit den Krankenkassen ist derzeit unmöglich.

- Kosten für zwei Tage Betriebsunterbrechung: 5.000 Euro

5. Datenmissbrauch. Die Hacker veröffentlichen die Gesundheitsdaten einiger Patienten. Die Betroffenen beauftragen Rechtsanwälte mit der Löschung der unrechtmäßig veröffentlichten Daten und verlangen vom Arzt Schadenersatz.

- Schadensersatz: 20.000 Euro nach Art. 82 DSGV0

6. Vertrauenskrise. Nachdem die lokale Presse über den Datendiebstahl berichtet hat, wenden sich zahlreiche Patienten von der Praxis ab, der Patientenstamm schrumpft deutlich.

- Krisenkommunikation: 1.000 Euro
- Umsatzrückgang: nicht gedeckt

7. Aufarbeitung. Die Datenschutzbehörden verhängen aufgrund des Datenverlustes ein hohes Bußgeld.

- Bußgeld: nicht gedeckt

Länge des Passworts wesentlich

Brute-Force-Attacken sind Versuche eines Computer-Programms, das Passwort eines anderen Programms zu knacken, indem alle möglichen Kombinationen ausprobiert werden. Daher ist die Länge eines Passworts maßgeblich für die Sicherheit von Daten.

Mit den aktuellen Rechnergeschwindigkeiten können Kriminelle zirka 2,15 Milliarden Passwörter pro Sekunde generieren. Ein Passwort mit z. B. sieben Kleinbuchstaben, hat 8.031.810.176 (ca. 8 Mrd.) verschiedene Kombinationen. Ein Hacker benötigt somit nicht einmal vier Sekunden, um alle Kombinationen zu verwenden.

Je länger und vielfältiger ein Passwort gewählt wird, umso größer sind die Chancen auf den Schutz. Folgende Zugriffsbeispiele von Passwörtern mit ausschließlich Kleinbuchstaben zeigen in etwa die Gefahr:

- 7 Zeichen: 3,74 Sekunden
- 8 Zeichen: 97 Sekunden
- 9 Zeichen: 42 Minuten
- 10 Zeichen: 18,5 Stunden
- 11 Zeichen: 19,8 Tage
- 12 Zeichen: 514 Tage
- 13 Zeichen: 36,5 Jahre
- 14 Zeichen: 952 Jahre
- 15 Zeichen: 24.766 Jahre

Achtung: Das ist allerdings jeweils die Maximaldauer für eine Entschlüsselung, denn in der Praxis sind die Werte durch 1.000 zu dividieren. Das bedeutet, dass Passwörter mit Kleinbuchstaben erst ab zirka zwölf bis 14 Zeichen uninteressant für Hacker sind. Andererseits potenziert sich die Rechen- und Speicherleistung von Computer-Chips nahezu jährlich, womit ein langes Passwort keinesfalls als Sicherheitsmaßnahme allein genügt.

Weitere Maßnahmen bzw. Informationen für die Praxis

- Sichere Passwörter. Länge und Anzahl der möglichen Kombinationen, Passwort-Manager, Zwei-Faktoren-Authentifizierung (Passwort + Code auf Smartphone)

Unter den folgenden Links kann getestet werden, ob z. B. E-Mails bereits geleakt wurden:
https://haveibeenpwned.com/
https://sec.hpi.de/ilc/search

- Mailverwaltung: Sicherheitseinstellungen, Sicherheits-Updates, nur vertrauenswürdige Mails öffnen (Absender und Betreff prüfen).
- Datensicherung: alle Gerätedaten sollten gesichert sein, Back-up soll vom Hauptsystem erstellt und nicht mit Hauptsystem verbunden sein, Backups auf Funktion regelmäßig testen.
- Wartung von Sicherheitsupdates: IT- Systeme, Virenprogramme etc.

Was leistet eine Cyber-Versicherung?

Diese Versicherung ist speziell auf die Bedürfnisse von kleinen und mittleren Unternehmen zugeschnitten und richtet sich damit unter anderem besonders an Ärzte. Die Versicherung übernimmt nicht nur die Kosten durch Datendiebstähle, Unterbrechungen des Praxisbetriebs und den Schadenersatz an Dritte, sondern steht den Kunden im Ernstfall mit einem umfangreichen Service-Angebot zur Seite. Nach einem erfolgreichen Angriff schickt und bezahlt die Versicherung Experten für IT-Forensik, vermittelt spezialisierte Anwälte und Krisenkommunikatoren. So hilft sie, den Schaden für betroffene Ärzte so gering wie möglich zu halten. Im Folgenden der Deckungsumfang (auszugsweise):

- **Haftpflichtversicherung.** Versicherungsschutz besteht für Ansprüche Dritter, z. B. im Zusammenhang mit Verstößen gegen die Geheimhaltungspflichten, Verletzungen von Bestimmungen des Datenschutzes etc., aber auch für von Behörden verhängte Strafen und Bußgelder.
- **Vertrauensschadenversicherung.** Versicherungsschutz besteht für unmittelbare Schäden durch Dritte oder kriminelle Mitarbeiter aufgrund von vorsätzlichen, unerlaubten Handlungen, insbesondere Vermögensdelikten wie z. B. Diebstahl, Raub, Betrug, Fake President Fraud etc.
- **Eigenschadenversicherung.** Versicherungsschutz für eigene Schäden und Kosten bei z. B. unvorhergesehenen Ausfällen des Computersystems durch fehlerhafte Bedingung, Datenerpressung etc. Betriebsunterbrechung infolge eines Ausfalls des IT-Systems, Lösegelder für die Freischaltung der IT bei Erpressungsversuchen, Computer-Forensik etc.

Der Bericht basiert auf einen Vortag des Autors, den er am 13. Europäischen Medizin-Rechtstag 2019 in Wien gehalten hat.

Andreas Reinthaler ist Spezialist für Risikoprävention und Risikoabsicherung bei Ärzten, Wien. © Privat