MEDletter

> Ausgabe 1 / 2025
> Informationen für Ärzte und medizinische Fachberufe

Cyberangriff – und was nun?

In der heutigen digitalen Welt sind Arztpraxen zunehmend Ziel von Cyberangriffen. Diese Angriffe können nicht nur denPraxisbetrieb stören oder komplett lahmlegen, sondern auch Datenwiederherstellung. das Vertrauen der Patienten beeinträchtigen und erhebliche finanzielle Schäden verursachen. Daher ist es essenziell, sowohl präventive als auch reaktive Maßnahmen zu ergreifen Betriebsunterbrechungsschadens.
und proaktiv den passenden Versicherungsschutz zu wählen.

Beispielsfall
Ein Fall aus Bayern verdeutlicht die potenziellen Auswirkungen eines Cyberangriffs auf eine Zahnarztpraxis:

Eine Gemeinschaftspraxis mit vier Zahnärzten und 18 Mitarbeitern wurde Opfer eines Trojaner-Angriffs. Die Schadsoftware verbreitete sich über einen E-Mail-Anhang mit Erpressern, inkl. Übernahme des Lösegelds als Ultima Ratio. dem Betreff „Terminvorschläge für eine professionelle Zahnreinigung“.
Nach Öffnen der Datei verschlüsselte der Trojaner die IT-Systeme und per E-Mail wurde ein Lösegeld in Höhe von 10 Bitcoins (ca. 220.000 Euro) gefordert.
Trotz Zahlung des Lösegelds wurde zwar der Code zur Entschlüsselung der Daten übergeben. Jedoch waren die in erster Linie personenbezogenen Daten bereits abgezogen und im Darknet veröffentlicht worden. Infolge des Angriffs musste die Praxis zwei Wochen vollständig schließen und kämpfte auch danach noch mit einer erheblichen Verringerung / Reduzierung des Patientenstamms.
Der Gesamtschaden für die Bereiche IT, Datenwiederherstellung und Erpressung sowie Betriebsunterbrechung belief sich auf rund eine halbe Million Euro.

In diesem Fall wurden zum Glück ein Großteil der Kosten von der Cyberversicherung abgedeckt.

Eine Cyberversicherung bietet finanziellen Schutz vor den Folgen von Cyberangriffen.

Versicherungsschutz
Von der Cyberversicherung werden folgende Bereiche typischerweise abgedeckt:

Eigenschäden:
Deckung der Kosten für die Soforthilfe, IT-Forensik und Datenwiederherstellung.

Rechtsberatung und Übernahme des entstandenen Betriebsunterbrechungsschadens.

Zusätzlich gewährt die Cyberversicherung Unterstützung bei der Kommunikation mit den Datenschutzbehörden sowie den Patienten, Kunden und Mitarbeitern.

Sollte es tatsächlich zu einem Verfahren bei der Datenschutzbehörde kommen, ist auch die Übernahme von Bußgeldern möglich, sofern rechtlich zulässig.

Übernahme und Hilfestellung bei der Verhandlung mit den Erpressern, inkl. Übernahme des Lösegelds als Ultima Ratio.

Das Darknet Monitoring ist ebenfalls Teil einer umfassenden Versicherungsdeckung.

Drittschäden:
Die Cyberversicherung betreibt die Haftungsabwehr von Ansprüchen Dritter, in der Regel der Patienten, aufgrund von Datenschutzverletzung oder Sicherheitslücken.

Sofern entsprechend geltend gemachte Schadenersatzansprüche berechtigt sind, werden diese seitens der Cyberversicherung ebenfalls übernommen.

Was tun im Schadenfall

- **System isolieren:**
  Trennen Sie betroffene Geräte sofort vom Netzwerk, um eine weitere Ausbreitung des Angriffs zu verhindern.
- **Eigenen IT-Experten kontaktieren:**
  Konsultieren Sie Ihren IT-Dienstleister, der den Umfang des Angriffs bewerten und die Wiederherstellung der Systeme übernehmen kann.
- **Hotline der Cyberversicherung anrufen:**
  Diese kann Ihnen direkt die passenden Dienstleister für das Krisenmanagement und die Soforthilfe zur Verfügung stellen, beantwortet erste Fragen und unterstützt Sie im Schadenfall.
- **Meldung an die Ermittlungsbehörden:**
  Informieren Sie bei einem Hackerangriff mit Lösegeldforderung immer die Polizei. Dort gibt es / existieren inzwischen eigene Cyberabteilungen für solche Fälle.
- **Patienten unterrichten:**
  Benachrichtigen Sie betroffene Patienten so weit wie möglich über den Vorfall.
- **Meldung bei der Datenschutzbehörde:**
  Informieren Sie die zuständigen Datenschutzbehörden über den Vorfall, insbesondere wenn sensible Patientendaten betroffen sind. Bei einer Cybererpressung muss man immer davon ausgehen, dass die Daten nicht nur verschlüsselt, sondern auch abgezogen worden sind.

Prävention

Damit es am besten gar nicht zu einem solchen Schaden kommt, oder dieser deutlich geringer ausfällt, raten wir zu folgenden präventiven Sicherheitsmaßnahmen:

- **Personalschulung:**
  Hauptursache bzw. Haupteinfallstor für Cyberangriffe ist menschliches Versagen. Schulen Sie Ihr Personal regelmäßig im sicheren Umgang mit IT- Systemen und in der Erkennung von Phishing-Versuchen.
- **Regelmäßige Updates:**
  Stellen Sie sicher, dass Software und Betriebssysteme stets auf dem neuesten Stand sind, um Sicherheitslücken zu schließen, das betrifft auch Diensthandys und -laptops. Gerade die mobilen Arbeitsgeräte werden hier oft vergessen und stellen ein leichtes / ideales Einfallstor für Angreifer dar.
- **Starke Passwortrichtlinien:**
  Verwenden Sie komplexe Passwörter und ändern Sie Sie diese regelmäßig. Implementieren Sie, wo möglich, eine Multi-Faktor-Authentifizierung.
- **Datensicherung:**
  Erstellen Sie regelmäßig Back-ups und bewahren Sie diese sicher und idealerweise offline oder in der Cloud auf.
- **Firewall und Antivirus-Software:**
  Nutzen Sie aktuelle Sicherheitssoftware und konfigurieren Sie Firewalls entsprechend, um unbefugten Zugriff zu verhindern.

Fazit

In jedem Fall ist es für Arztpraxen unerlässlich, sowohl präventive Sicherheitsmaßnahmen zu implementieren als auch einen umfassenden Versicherungsschutz zu wählen. Beide Maßnahmen in Kombination gewährleisten einen effektiven Schutz vor den vielfältigen Risiken der Cyberkriminalität und sichern den Praxisbetrieb langfristig ab.

Autorin

Meike Ackermann, Rechtsanwältin,
HDI

HDI Versicherung AG
HDI-Platz 1
30659 Hannover
www.hdi.de/medletter