Steigende Cybergefahr für Arztpraxen
Mit ausgewogenen Sicherheitskonzepten vorbeugen

Cyber-Angriffe sind allgegenwärtig, variantenreich und vor allem branchenunabhängig. Das schnelle Geld verdienen Kriminelle zumeist mittels der Cyber-Erpressung. Dabei werden menschliche Schwächen gezielt ausgenutzt.

Die Bedrohungslage

Zwar sind Cyberrisiken branchenunabhängig, aber in den vergangenen Monaten sind insbesondere Krankenhäuser und Arztpraxen verstärkt in das Visier Cyber-Krimineller geraten. Einerseits, weil die enorme Arbeitsbelastung infolge der Corona-Pandemie perfekt für sog. Cyber-Erpressungen genutzt werden kann, und anderseits, weil Patientendaten für Kriminelle weiterhin von sehr hohem Wert sind. Sie lassen sich für viel Geld weiterverkaufen. Genutzt werden die Daten dann zur Vorbereitung weiterer krimineller Aktivitäten oder aber auch zu wirtschaftlichen/werblichen Zwecken.

Die Cyber-Erpressung

Trotz der Vielzahl an Angriffsvarianten, sticht eine Methode heraus: Die Cyber-Erpressung. Hiermit verdienen Kriminelle das schnelle Geld, und Sie profitieren dabei von einer Sicherheitslücke, die nie ganz geschlossen werden kann - die Rede ist vom Menschen bzw. dem Anwender.

Was passiert bei einer Cyber-Erpressung? Die Täter tarnen Schadsoftware als vermeintlich harmlosen E-Mail-Anhang, etwa als Bewerbungsunterlage, Bestellbestätigung, vermeintliche Beschwerde oder einfach als interne Mail. Dabei soll die Neugier des Empfängers geweckt werden, damit dieser den Anhang anklickt und so die Erpressung aktiviert. Die Schadsoftware verschlüsselt dann die Daten der Opfer. Übrig bleibt die Nachricht über den Angriff, verbunden mit der Aufforderung, einen bestimmten Betrag (in Bitcoin) für die angekündigte Entschlüsselung der Daten zu zahlen.

Die Lösegelder können frei gewählt und individuell angepasst werden. Damit das Geschäftsmodell auch weiterhin funktioniert, ist die Höhe regelmäßig so bemessen, dass die Opfer noch bereit sind zu bezahlen. Der Ausgang ist dennoch ungewiss; nicht immer funktionieren die Systeme anschließend wieder.

IT-Sicherheit als Gesamtkonzept verstehen

IT-Sicherheit ist Chefsache, das normiert inzwischen auch die Richtlinie zur IT-Sicherheit in der vertragsärztlichen Versorgung (§ 75b SGB V). Sie legt technische Anforderungen fest und beschreibt das Mindestmaß der zu ergreifenden Maßnahmen, um IT-Sicherheit in Arztpraxen zu gewährleisten. Versicherungslösungen können bzw. sollen insoweit Bestandteil eines ausgewogenen Sicherheitskonzeptes sein.

Ausgereifte Sicherheitskonzepte basieren immer auf einer modernen IT-Infrastruktur. Dabei ist auf folgende Punkte zu achten:

- Automatische Updates / Aktuelle Antivirensoftware
- Strukturierte Vergabe von Nutzer- und Administratorrechten
- Nutzung komplexer Passwörter
- Regelmäßige Datensicherung

Cyber-Präventionstraining

Ganz entscheidend aber ist bereits die Sensibilisierung der Mitarbeitenden. Hilfreich sind insoweit Cyber-Präventionstrainings. Dies sind kompakte, kurzweilige Video-Trainings, die Grundlagen zur Cyber- und Datensicherheit vermitteln.

Solche Trainings sind zumeist schon Bestandteil umfassender Cyber-Versicherungslösungen. Die Versicherungsprämien orientieren sich an der Praxisgröße sowie der gewünschten Versicherungssumme und beginnen bereits bei rund 400,- EUR. Die Cyber-Versicherung ist sozusagen das Back-Up für die IT. Hierüber werden im Krisenfall vielzählige Kostenpositionen ersetzt.

- IT-Dienstleistungen
- Informationskosten zur Benachrichtigung von Behörden und Patienten
- Schadensersatzforderungen der Dateninhaber
- Rechtsanwaltskosten
- Lösegelder
- PR-Maßnahmen
- Ertragsausfälle

Fazit

Das Thema IT-Sicherheit wird längst nicht mehr allein dem individuellen Sicherheitsempfinden überlassen. Ganz gezielt werden Praxisinhaber in die Pflicht genommen, sorgsam mit Patienten- und Gesundheitsdaten umzugehen und Vorkehrungen zum Schutz derselben zu treffen.

Fernab der technischen Bemühungen zeigt sich, dass die beste Prävention darin besteht, sich innerhalb der Praxis über Cyberrisiken auszutauschen. Denn nur wer die Gefahren überhaupt kennt, kann sie erfolgreich umschiffen.

Prüfen Sie daher bei seltsam anmutenden Mails, ob es den Absender überhaupt gibt oder dessen Telefonnummer tatsächlich funktioniert, und achten Sie auf Rechtschreibfehler und den verdächtigen, dringlichen Tonfall.

Vorankündigung für ein Cyber-Webinar für BDA-Mitglieder

Cyber-Risiken erfolgreich abwehren
Webinar am 08.04.2022; 17 - 18.00 Uhr
Für BDA-Mitglieder kostenfrei

Die Gefahren des digitalen Zeitalters, insbesondere Cyber-Angriffe, treffen längst auch das Gesundheitswesen. Es ist also Zeit Vorsorge zu treffen.

Nähere Informationen samt Link zur Anmeldung folgen in Kürze.

Stand: Februar 2022