Cyberversicherung – sinnvoll oder nicht?

Immer mehr Versicherer bieten als Zusatzversicherung sogenannte „Cyberpolicen“ an, die Schäden absichern, die durch Cyberkriminalität entstehen. Viele Niedergelassene stehen vor der Frage, ob sie eine solche Police benötigen und was beim Vertragsabschluss zu beachten ist. Im Gespräch mit Auf den PUNKT. beantwortet IT-Experte Mark Peters die wichtigsten Fragen.

Der Abschluss einer Cyberversicherung sollte wohlüberlegt sein. Bei Interesse empfiehlt es sich, Vergleichsangebote anzufordern und sich die Zeit zu nehmen, alle AGB aufmerksam zu lesen.

Herr Peters, vorab Hand aufs Herz – das wird hier jetzt keine versteckte Werbung für ein Produkt, oder?

Mark Peters: Natürlich nicht! Ich selbst verkaufe oder empfehle keine spezielle Versicherung. Meine Unabhängigkeit als IT-BSI-Grundschutzpraktiker ist mir sehr wichtig. Mein Wissen stammt aus Gesprächen mit Versicherungen im Rahmen meiner Kundenbetreuung, aus verschiedenen Policen, die mir von Ärzten zur Sichtung zugesendet wurden, und dem Dokument „BSI – Die Lage der IT-Sicherheit in Deutschland 2020“.

Wie hoch ist denn überhaupt das Risiko für Praxen, einem Cyberangriff zum Opfer zu fallen?

Mark Peters: Auch und vor allem Arzt- und Therapeutenpraxen sind mittlerweile tatsächlich ein beliebtes Ziel von Hackern, da sie oftmals (noch) nicht über ein entsprechendes Sicherheitssystem verfügen. Es wurden aber auch schon große Unternehmen im Gesundheitssektor erfolgreich angegriffen. Wichtig zu wissen ist: Die herkömmlichen Inventar- und Haftpflichtversicherungen decken üblicherweise Schadensfälle, die durch einen Hacker-Angriff entstehen, nicht ab.

Da liegt der Gedanke, eine Cyberversicherung abzuschließen, durchaus nahe. Welche Vorbereitungen sollte man dafür treffen?

Mark Peters: Aus meiner Sicht sollte man sich zunächst folgende Frage stellen: Deckt meine eigene, bestehende Ärzte/Therapeuten-Berufshaftpflicht Fremdschäden (Haftpflicht) und Datenschutzvorfälle ab? Wenn ja, ist in der Regel alles in Ordnung. Wenn diese Frage mit „Nein“ beantwortet wird, ist eine Bedarfsermittlung allein wegen der sensiblen Patientendaten unumgänglich. Ich habe dazu eine Checkliste erstellt (siehe Infokasten).

Checkliste zur Bedarfsermittlung für eine Cyberschutzversicherung

1. Wird die vorhandene Antivirensoftware permanent aktualisiert?
2. Ist eine Soft- und Hardware-Firewall im Einsatz?
3. Sind alle Mitarbeitenden in der Lage, Phishing-E-Mails und andere potenzielle Bedrohungen zu erkennen?
4. Gibt es einen Notfallplan, falls Kriminelle das System erfolgreich angreifen konnten?
5. Werden die Daten regelmäßig (am besten täglich) gesichert?
6. Werden Updates zeitnah aufgespielt?
7. Werden Passwörter regelmäßig geändert?
8. Sind die Rechner vor unberechtigten Zugriffen geschützt (Sperrung des Bildschirms, Inaktivierung der USB-Anschlüsse etc.)?
9. Gibt es eine/-n Cyberschutz-Beauftragte/n?

Fehler beim Abschluss der Versicherung vermeiden und folgende Fragen eindeutig klären:

1. Wie hoch ist die maximale Versicherungssumme?
2. Wer ist der Versicherer?
3. Wie hoch ist die Jahresprämie inklusive Versicherungssteuer?
4. Welche Bausteine sind im Versicherungsumfang enthalten?
5. Wie hoch ist die Selbstbeteiligung?
6. Welche Anforderungen muss ich erfüllen?
7. Wer ist mitversichert?

Was leisten Cyberversicherungen denn überhaupt?

Mark Peters: Meine Erfahrungen haben gezeigt, dass der Auslöser eines Versicherungsfalles folgendermaßen formuliert sein sollte: „Unbefugte Nutzung von IT-Systemen inklusive Bedienfehlern". Je nach Vertrag sichern die Versicherungen den finanziellen Schaden eines Angriffs ab (Betriebsausfall, Neuanschaffungskosten, gegebenenfalls auch die Zahlung von Lösegeld etc.), stellen IT-Experten zur Verfügung und übernehmen Bußgeldzahlungen im Rahmen von Datenschutzverletzungen.

Und welche Leistungen sind vom Versicherungsnehmer zu erbringen?

Mark Peters: Die Obliegenheiten können mitunter sehr anspruchsvoll sein. Hier kommen unter Umständen zunächst hohe Investitionskosten auf den Inhaber zu. Fragen Sie sich, ob Sie die Anforderungen vollumfänglich erfüllen können. Ist das nicht der Fall, kann es passieren, dass die Versicherung im Schadensfall nicht einspringt. Außerdem lohnt es sich auf jeden Fall, mehrere Angebote miteinander hinsichtlich der Anforderungen zu vergleichen und eine Kosten-Nutzen-Rechnung aufzustellen.

Mark Peters von der Praxismanagement Bublitz-Peters GmbH & Co. KG in Heidelberg ist ein externer Datenschutzbeauftragter, Auditor mit Heidelberger Cyberschutz-Rating-Zertifizierung und geprüfter IT-BSI-Grundschutzpraktiker.

Um die Sicherheit Ihres EDV-Netzwerks zu erhöhen und den Anforderungen der IT-Sicherheitsrichtlinie gerecht zu werden, brauchen Sie keine Cyberschutzversicherung. Sie können die Unterstützung eines IT-BSI-Grundschutzpraktikers in Anspruch nehmen oder auch die neue Richtlinie eigenverantwortlich umsetzen. Mein Tipp: Schließen Sie nur dann eine Cyberversicherung ab, wenn Sie die Anforderungen des Versicherers erfüllen können. Andernfalls zahlen Sie hohe Versicherungsbeiträge, sind im Schadensfall aber nicht abgesichert.

Wie viele Anbieter gibt es denn eigentlich?

Mark Peters: Mittlerweile bieten fast alle großen Versicherer Cyberpolicen an, aber es gibt auch einige Spezialisten am Markt. Aktuell dürften es mehr als 30 Anbieter sein. ■

Die Fragen stellte
Cornelia Kur

Was leistet eine Cyberversicherung NICHT?

- Sie schützt nicht vor den Folgen von Urheberrechtsverletzungen, wenn jemand beispielsweise ohne Erlaubnis geschützte Bilder auf seiner Internetseite verwendet.
- Sie entbindet Praxisinhaber nicht von ihrer Verantwortung, das Praxisnetzwerk entsprechend der IT-Sicherheitsrichtlinie abzusichern.
- Vor allem schützt eine Cyberversicherung nicht vor Angriffen auf das System und dem Imageverlust, den die Praxis hierdurch vielleicht erleidet.

Infobox