PRAXIS-IT // Immer mehr Versicherer bieten als Zusatzversicherung sogenannte „Cyberpolicen" an, um Schäden, die durch Cyberkriminalität entstehen, abzusichern. Viele niedergelassene Zahnärzte stehen vor der Frage, ob eine solche Zusatzversicherung tatsächlich sinnvoll ist. Und wenn ja, was ist dann bei Vertragsabschluss zu beachten? Anbei erhalten Sie Antworten zu den häufigsten Fragen rund um das Thema „Cyberpolicen".

CYBERVERSICHERUNG – SINNVOLL ODER NICHT?

Mark Peters, Bettina Ritter / Heidelberg

Wie hoch ist das Risiko für Praxen, einem Cyberangriff zum Opfer zu fallen?
Praxisinhaber schätzen das Risiko, Opfer einer Hackerattacke zu werden, immer noch als gering ein. Aktuelle Zahlen zeigen jedoch, dass es sich hierbei um eine tragische Fehleinschätzung handelt. Tatsächlich sind niedergelassene Zahnärzte mittlerweile ein beliebtes Ziel von Cyberkriminellen, da diese oftmals (noch) nicht über ein entsprechendes Sicherheitssystem verfügen. Es wurden aber auch schon große Unternehmen im Gesundheitssektor (zum Beispiel Kliniken) erfolgreich angegriffen. Wenn dann lebenswichtige Systeme lahmgelegt werden, kann dies für Patienten auch tödliche Folgen haben.


© Follow Focus/Shutterstock.com

Wie viele Anbieter gibt es?
Inzwischen bieten fast alle großen Versicherungsgesellschaften Cyberpolicen an. Aktuell dürften es mehr als 25 Anbieter sein.

Was leisten Cyberversicherungen?
Je nach Vertrag sichern die Versicherungen den finanziellen Schaden eines Angriffs ab (Betriebsausfall, Neuanschaffungskosten, ggf. auch die Zahlung von Lösegeld etc.), stellen den Kontakt zu IT-Experten her und übernehmen Bußgeldzahlungen im Rahmen von Datenschutzverletzungen.

Was leisten Cyberversicherungen nicht?
Das Vorhandensein einer Cyberpolice schützt nicht vor den Folgen von Urheberrechtsverletzungen, wenn Sie beispielsweise ohne Erlaubnis geschützte Bil-

der auf Ihrer Internetseite verwenden. Sie entbindet Praxisinhaber nicht von ihrer Verantwortung, das Praxisnetzwerk entsprechend der IT-Sicherheitsrichtlinie abzusichern. Vor allem schützen Cyberversicherungen nicht vor Angriffen auf Ihr System und dem Imageverlust, den die Praxis bei Bekanntwerden hierdurch erleidet.

Welche Vorbereitungen sollten vor Abschluss einer Cyberversicherung getroffen werden?

Die folgende Checkliste bietet einen ersten Überblick über die Anforderungen:

1. Wird die vorhandene Antiviren-Software permanent aktualisiert?
2. Ist eine 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?
10. Wurden die Auflagen gemäß der IT-Sicherheitsrichtlinie (§ 75b SGB V) umgesetzt?
11. Liegt eine Konformitätsbescheinigung gemäß der jährlichen Evaluationspflicht (§ 75b SGB V) vor? Beispiel ITe@sy Praxismanagement

Welche Leistungen sind vom Versicherungsnehmer zu erbringen?

Die Obliegenheiten können mitunter sehr anspruchsvoll sein. Hier kommen unter Umständen zunächst hohe Investitionskosten auf die Praxis zu. Fragen Sie sich vor Vertragsabschluss, ob Sie die Anforderungen vollumfänglich erfüllen können. Ist das nicht der Fall, kann es passieren, dass die Versicherung im Schadensfall nicht einspringt.

Es lohnt sich auf jeden Fall, mehrere Angebote miteinander hinsichtlich der Anforderungen zu vergleichen.

Welche Konditionen sollten miteinander verglichen werden?

Die folgende Checkliste soll Ihnen helfen, Fehler beim Abschluss der Versicherung zu vermeiden:

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

Es bestehen bereits mehrere Versicherungen, unter anderem eine Inventarversicherung. Ist die Praxis damit nicht ausreichend vor einem Cyberangriff geschützt?

Üblicherweise decken die herkömmlichen Inventar- und Haftpflichtversicherungen Schadensfälle, die durch einen Hackerangriff entstehen, nicht ab.

Natürlich konnten an dieser Stelle nicht alle Fragen beantwortet werden. Am besten wenden Sie sich an einen Versicherungsmakler Ihres Vertrauens. Es lohnt sich auf jeden Fall, mehrere Versicherungsangebote miteinander zu vergleichen und eine Kosten-Nutzen-Rechnung aufzustellen.

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.

Quelle: Heidelberger Cyberschutz-Rating, ITe@sy Cyberschutz-Versicherung

PRAXISMANAGEMENT
BUBLITZ-PETERS
GMBH & CO. KG
Rohrbacher Straße 28
69115 Heidelberg
Tel.: +49 6221 438500
info@bublitz-peters.de
www.bublitzpeters.de