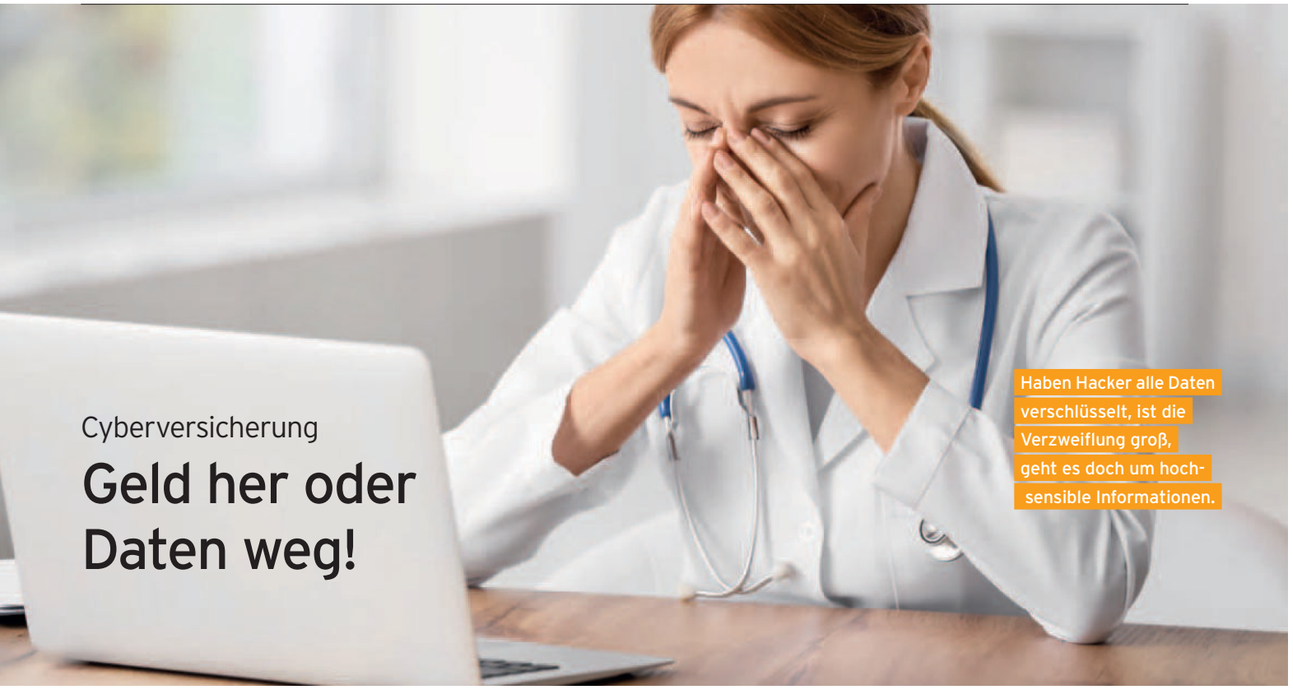


Cyberversicherung

Geld her oder Daten weg!

Haben Hacker alle Daten verschlüsselt, ist die Verzweiflung groß, geht es doch um hochsensible Informationen.

Ein Cyberangriff kann jeden treffen, den Praxisbetrieb lahmlegen, Patientendaten abgreifen und Vertrauen kosten. Doch viele Ärztinnen und Ärzte verdrängen das Risiko. Wie eine Cyberversicherung die Folgen mildern kann und warum ein maßgeschneidertes Produkt so wichtig ist.

Es trifft mich selbst bestimmt nicht, wir sind viel zu klein und nicht interessant genug für Hacker, außerdem sind wir ja ausreichend geschützt – was viele Praxisinhaberinnen und -inhaber in puncto Cyberkriminalität denken, lässt sich durch Zahlen belegen. Laut Branchenreport „Cyberrisiken von Ärzten und Apotheken“ des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV) aus dem Jahr 2019 meint jede zweite Artpraxis, sie sei zu klein, um Ziel eines Hackerangriffs zu werden (siehe Zahlen rechts). Ein Drittel der damals Befragten wollte daher nicht weiter in die IT-Sicherheit investieren.

Beim Thema Cyberkriminalität richtet sich die Wahrnehmung oft auf große oder mittelständische Firmen, die von global agierenden Hackerbanden lahmgelegt werden. Doch für Cyberkriminelle ist es auch lukrativ, massenhaft Kleinbeträge zu erpressen – frei nach dem Motto: Kleinvieh macht auch Mist. Ärzte sind dabei ein lohnendes Ziel. Sie sind besonders gut erpressbar, da sie zur Geheimhaltung verpflichtet sind und in der Regel über ausreichend Liquidität verfügen. Gelangen sensible Patientendaten an die Öffentlichkeit, ist der Imageschaden groß. Oft müssen Ärztinnen und Ärzte in Deutschland auch mit einem Bußgeld vonseiten der Datenschutzbehörden rechnen, von Schadensersatzforderungen ihrer Patienten ganz zu schweigen. Doch das ist noch nicht alles. Werden Daten verschlüsselt, liegt für Tage der Praxisbetrieb lahm, Patienten können nicht behandelt, E-Mails nicht beantwortet werden. Sind die Daten weg, erschwert das zudem die Abrechnung mit der Kassenärztlichen Vereinigung oder macht diese völlig unmöglich.

GEFÄHRLICHER IRRGLAUBE

56 %
der Ärzte denken, ihre Praxis sei zu klein, um in den Fokus von Cyberkriminellen zu geraten.

80 %
der Ärzte glauben, dass ihre Computersysteme umfassend geschützt seien.

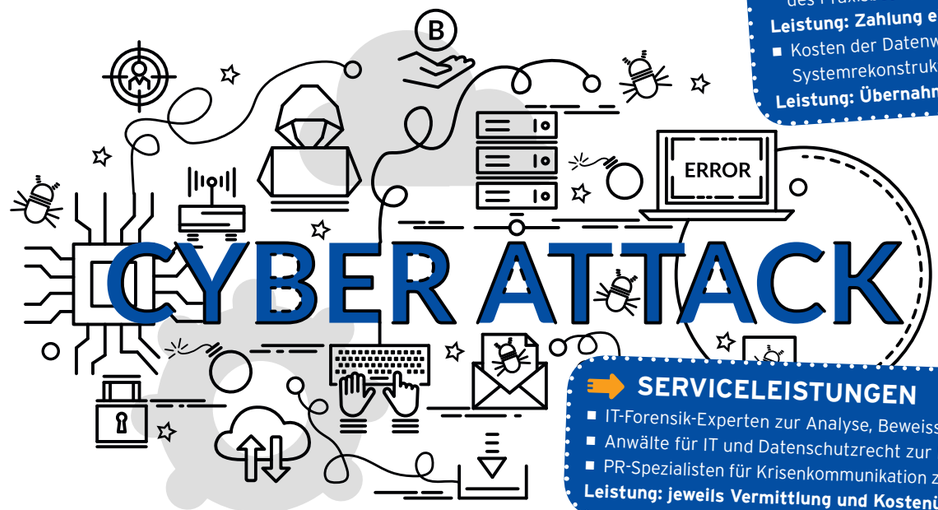
45 %
der Ärzte meinen, dass ihre Daten für Cyberkriminelle nicht interessant genug seien.

Quelle: Branchenreport „Cyberrisiken von Ärzten und Apotheken“ des Gesamtverbands der Deutschen Versicherungswirtschaft, 2019

Plötzlich sind alle Daten weg

Doch wie funktioniert das Ganze? Ransomware-Angreifer (von englisch ransom: Lösegeld) dringen in das Praxis-Netzwerk ein, stehlen Daten und verschlüsseln alles mit einer Software, für die nur sie den Zugang haben. Für die Freischaltung fordern sie ein Lösegeld, meist in der Digitalwährung Bitcoin. Zusätzlich drohen sie, die gestohlenen Daten zu veröffentlichen. Dahinter stecken meist Gruppen von Cyberkriminellen, die mithilfe von Botnets (eine Gruppe automatisierter Schadprogramme) Computer infizieren, meistens über verseuchte Word-Dateien, die als Anhang per E-Mail verschickt werden. Das Botnet macht sich dann in den Computern der Betroffenen breit und nutzt diese, um weitere Rechner zu infizieren. Über die Botnets verändern die Kriminellen regelmäßig ihre Schadsoftware, damit diese von den Virenprogrammen nicht entdeckt wird. Andere Kriminelle können das Botnet sogar mieten.

DAS LEISTET EINE CYBERVERSICHERUNG



EIGENSCHÄDEN
- Wirtschaftliche Schäden durch Unterbrechungen des Praxisbetriebs

Leistung: Zahlung eines Tagessatzes
- Kosten der Datenwiederherstellung und Systemrekonstruktion

Leistung: Übernahme der Kosten

DRITTSCHÄDEN
- Schadenersatzforderungen von Patienten wegen Datenmissbrauchs

Leistung: Entschädigung und Abwehr unberechtigter Forderungen

SERVICELEISTUNGEN
- IT-Forensik-Experten zur Analyse, Beweissicherung und Schadenbegrenzung
- Anwälte für IT und Datenschutzrecht zur Beratung
- PR-Spezialisten für Krisenkommunikation zur Eindämmung des Imageschadens

Leistung: jeweils Vermittlung und Kostenübernahme

Quelle: Branchenreport „Cyberrisiken von Ärzten und Apotheken“ des Gesamtverbands der Deutschen Versicherungswirtschaft, 2019

Die Sorglosigkeit ist groß

Der Branchenverband Bitkom berechnete den gesamtwirtschaftlichen Schaden durch Cyberkriminalität schon 2019 auf mehr als 100 Milliarden Euro. Die Frage ist inzwischen nicht mehr, ob ein solcher Angriff stattfindet, sondern wann. Doch die Sorglosigkeit in Arztpraxen ist groß. Der Branchenreport des GDV offenbarte, dass in rund 90 Prozent der getesteten Arztpraxen mehrere Benutzer dieselbe Zugangskennung mit sehr einfachen oder gar keinen Passwörtern nutzten – ein klassisches Einfallstor für Cyberkriminelle. Aber auch sogenannte Phishing-Mails, E-Mails mit Dateianhängen, in denen eine Schadsoftware steckt, sind äußerst beliebt. Viele Kriminelle suchen gar nicht mehr nach Sicherheitslücken in veralteten Betriebssystemen, sondern wählen gezielt die Schwachstelle Mensch. Die Schäden können immens sein. Eine Cyberversicherung kann hier eine sinnvolle Ergänzung zu umfassenden technischen und organisatorischen Maßnahmen darstellen.

Der GDV hat 2017 unverbindliche Musterbedingungen für eine Cyberversicherung entwickelt und damit für viele Versicherer den Anstoß gegeben, dieses Produkt in ihr Portfolio aufzunehmen. Eine Cyberversicherung übernimmt in der Regel nicht nur die Eigenschäden, die durch den Diebstahl der Daten entstehen, sondern kommt auch für Schäden Dritter auf. Was im Falle einer Cyberattacke ebenfalls enorm wichtig ist: Die Assekuranz steht dem Versicherungsnehmer auch mit Experten für IT-Forensik, Anwälten und Krisenkommunikatoren zur Seite (siehe Grafik oben).

Im Detail können die Leistungen jedoch sehr unterschiedlich sein. Die Analyse- und Ratingagentur Franke und Bornberg aus Hannover hat sich die Versicherungsbedingungen verschiedener Versicherer genauer angesehen und festgestellt, dass es schon in der Terminologie keine Einheitlichkeit gibt. Einige Versicherer sprechen von „Netzwerksicherheitsverletzung“, andere schlicht von „Cyberangriff“ – und jeder versteht im Detail etwas anderes darunter. Schwierig sei nach Angaben der Agentur auch, zu erkennen, welche Sicherheitsvorkehrungen vonseiten der Versicherungsnehmer erwartet werden, um im Ernstfall die Versicherung in Anspruch nehmen zu können. In den Versicherungsbedingungen ist oft von „gängigen“ oder „branchenüblichen“ Standards die Rede. Eine Definition fehle aber meist, was reichlich Platz für Auslegung lasse. Als unabdingbare Voraussetzung für eine gute Cyberversicherung definiert die Agentur übrigens die Mitversicherung des Krisenmanagements. Der Grund: Zwar leisten die Assekuranzen erste Hilfe durch IT-Forensiker, PR-Experten und spezialisierte Juristen. Das Management dieser hoch spezialisierten Fachleute bleibe in den meisten Fällen aber dem Betroffenen überlassen – das kann schwierig werden, wenn die Nerven blank liegen.

Für die TI haftet die gematik

Sorgen machen sich viele Ärztinnen und Ärzte seit Langem um die Sicherheit der Telematikinfrastruktur (TI) sowie die Frage, wer für Datenlecks in diesem Bereich haftet. Hier gibt es Entwarnung: Mit dem dritten Digitalisierungsgesetz soll nun klar geregelt werden, dass die gematik für den Betrieb der TI verantwortlich ist. „Das ist für uns eine wichtige Verbesserung“, betonte KBV-Vorstandsmitglied Dr. Thomas Kriedel in einem Video-Interview. Auch die mit der TI verbundene Datenschutz-Folgeabschätzung soll vom Gesetzgeber vorgenommen werden. Dabei soll auch klargestellt werden, dass beispielsweise bei Ausfällen nicht mehr der Arzt haftet.

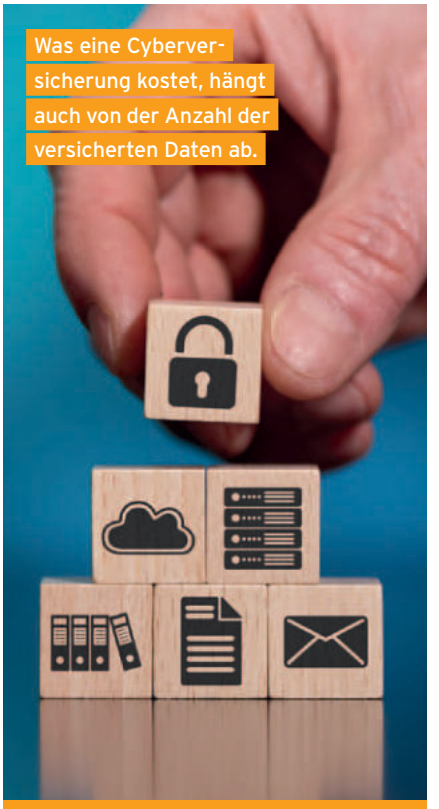
Die Agentur Franke und Bornberg hat 148 Tarife von 33 Versicherern für kleine und mittelständische Unternehmen »

genauer unter die Lupe genommen und bewertet. Für Praxisinhaber erscheint es jedoch kaum machbar, sich durch die verschiedenen Versicherungsbedingungen zu wühlen, um das für sie passende Produkt zu finden. Die Beratung durch einen unabhängigen Versicherungsmakler ist daher fast ein Muss. Wir haben bei einem nachgefragt, worauf es bei einer guten Cyberversicherung für Niedergelassene wirklich ankommt.

Der Teufel steckt im Detail

„Hier spielen verschiedene Faktoren eine Rolle", sagt Stephan Curt, unabhängiger Versicherungsmakler aus Leipzig. „Es kommt unter anderem darauf an, wie viele Patientendaten die Praxis hat, wie viele IT- und Telekommunikationsgeräte angeschlossen sind, ob in der Praxis mit Kreditkarte gezahlt werden kann, aber auch darauf, wie viele Mitarbeiter beschäftigt sind und ab welcher Schadenssumme es für den Arzt oder die Ärztin existenzbedrohend wird, um nur einige zu nennen." Ein guter Makler fragt diese Punkte mithilfe eines Tools ab, wird aber zum Beispiel auch wissen wollen, ob der Arzt ein eigenes Labor betreibt (zusätzliche IT und personenbezogene Daten) oder noch Bereitschaftsdiensteinsätze fährt (Abrechnung mit Kreditkarte bei Selbstzahlern oder Privatpatienten) – Punkte, die der Arzt oder die Ärztin von sich aus vielleicht gar nicht als wichtig einstuft.

Curt rät zudem, die Versicherungssumme bei einer Arztpraxis nicht zu gering zu bemessen, das Risiko einer Unterversicherung ist groß. „100.000 Euro reichen aus meiner Sicht nicht aus. Eine gute Police sollte außerdem das Lösegeld bezahlen und keine Sublimits, also Obergrenzen für einzelne Bausteine enthalten", mahnt der Experte. So gebe es Policen, die zwar eine Versicherungssumme von einer Million Euro haben, Lösegelder aber nur bis 50.000 Euro übernehmen oder die Kosten für die Wiederherstellung der IT deckeln. Das hält der Makler nicht für empfehlenswert. Weitere Faktoren sind die Selbstbeteiligung oder die Wartezeiten bei der Betriebsunterbrechung: „Manche Policen sehen vor, dass die Versicherung erst dann einspringt, wenn das Cyberproblem nicht innerhalb von acht Stunden geklärt werden kann. Dauert es länger, zahlt die Versicherung aber von der ersten Minute an", erklärt Curt.



Was eine Cyberversicherung kostet, hängt auch von der Anzahl der versicherten Daten ab.

DAS KOSTET EINE CYBERVERSICHERUNG

Modellrechnung* für eine Hausarztpraxis

- **Jahresumsatz der Praxis:** 300.000 €
- **Anzahl der Patientendaten:** 3.000
- **Anzahl der Beschäftigten:** 5
- **Vorhandene IT- und Telekommunikationsgeräte:** 10
- **Back-up:** alle 14 Tage
- **Geschätzter Zeitraum, bis nach einem Cyberangriff alles reibungslos funktioniert:** 5 Tage
- **Geschätzte Einschränkung durch den Ausfall der IT:** 80 %
- **Kreditkartenzahlung:** 0
- **Schadenssumme, ab der die Praxis in ihrer Existenz gefährdet wäre:** 40.000 €
- **Selbstbeteiligung:** 1.000 €
- **Kosten einer Cyberversicherung:** zwischen 700 und 900 € im Jahr

* Berechnung: Versicherungsmakler Stephan Curt, CV-Curt versichert® GmbH & Co. KG aus Leipzig, 2021 (Modellrechnung stark vereinfacht)

Wichtig: Eine gute Cyberversicherung tritt in der Regel auch schon beim Verdacht eines Cyberangriffs ein. „Den muss der Arzt innerhalb von 72 Stunden dem Landesdatenschutzbeauftragten melden. Dieser entscheidet, ob und wie die potenziell betroffenen Patienten zu informieren sind. Je nach Bundesland kann es passieren, dass dazu ein Einschreiben mit Rückschein erforderlich ist. Bei Portokosten von 5,50 Euro und 3.000 Patientendaten entsteht dem Arzt allein dadurch ein Schaden von 16.500 Euro." Dieses Geld würde eine gute Versicherung übernehmen – im Gegensatz zu Bußgeldern für Datenschutzverstöße. Bei den Bußgeldern wird aber ein anderer Aspekt wichtig, den die Versicherung abdeckt: die Einschaltung eines Fachanwalts für IT- und Datenschutzrecht. „Dieser kann mit dem Datenschutzbeauftragten verhandeln und vielleicht erreichen, dass ein Bußgeld gemindert oder davon ganz abgesehen wird", weiß der Versicherungsexperte.

Maßgeschneidert ist besser

Wichtig ist aus Sicht des Experten auch, sich spezielle Deckungskonzepte der Versicherer für die Gesundheitsbranche anzusehen, denn nicht jede Branche braucht jeden Baustein. „95 Prozent der Arztpraxen ermöglichen beispielsweise keine Kreditkartenzahlung, sie haben nur ein normales EC-Terminal. Daher benötigen sie den Baustein ePayment nicht. Warum sollten sie dann dafür bezahlen?", gibt Curt zu bedenken. „One fits all" ist daher nicht der richtige Weg. Auch die Frage, wie lange ein Versicherer seine Cyberversicherung schon im Portfolio hat, ist nicht unwichtig. „Viele Versicherungen springen derzeit auf den Zug auf, haben aber noch keine oder wenig Erfahrung in der Abwicklung und den Prozessen. Der Kunde braucht aber eine Versicherung, die die Infrastruktur hat und auf ein Netzwerk guter IT-Forensiker, Fachanwälte und Fachfirmen zurückgreifen kann – und das muss wachsen."

Bleibt die Frage, was eine Cyberversicherung kostet. Das hängt natürlich von der Praxisgröße ab. Curt sagt: „Einen hohen dreistelligen bis niedrigen vierstelligen Betrag" (siehe auch Kasten links).

Ina Reinsch

Foto: thodonal - stock.adobe.com