Medletter

> Ausgabe 1 / 2023
> Informationen für Ärzte und medizinische Fachberufe

Ja ist denn schon wieder Cyber?

Für Arzt- und Psychotherapeutenpraxen gelten nunmehr verbindliche Anforderungen an die IT-Sicherheit. Die Vertreterversammlung der Kassenärztlichen Bundesvereinigung hatte dazu im Dezember 2020 die gesetzlich vorgeschriebene IT-Sicherheitsrichtlinie verabschiedet. Sie trat bereits Anfang 2021 offiziell in Kraft. Bedarf es nun noch einer zusätzlichen Cyberversicherung nach dem Beschluss der IT-Richtlinie in einer vertragsärztlichen bzw. vertragspsychotherapeutischen Praxis?

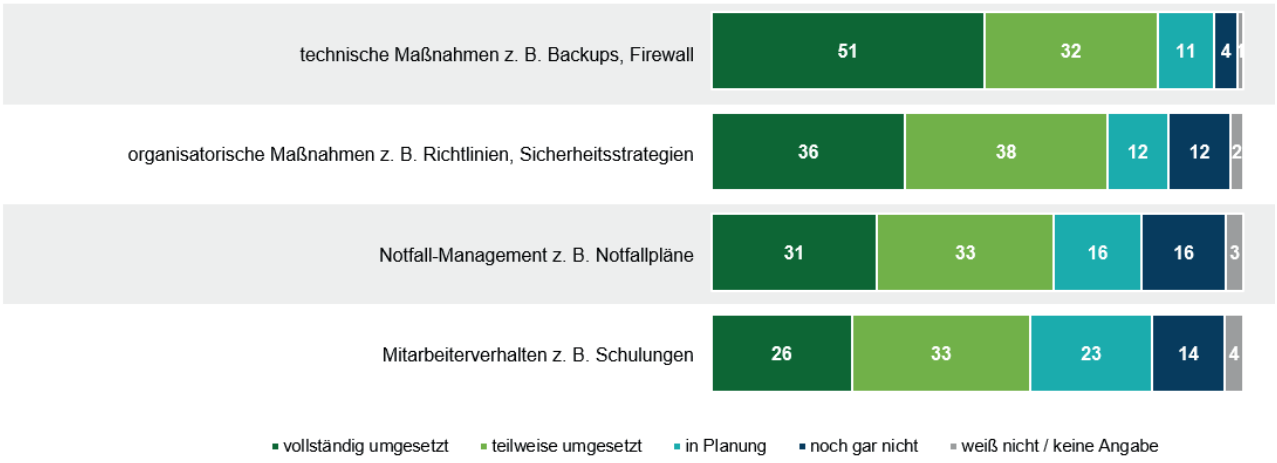
"In den vergangenen Jahren haben Cyberangriffe Schäden in dreistelliger Milliardenhöhe für die deutsche Wirtschaft verursacht. Neun von zehn aller Unternehmen sind mittlerweile von Cyberangriffen betroffen. Wir sehen hier unter anderem einen Zusammenhang zwischen Krisen und dem erhöhten Aufkommen von Cyberkriminalität. Vor allem Ransomware-Angriffe sind im Jahr 2021 gegenüber dem Vorjahr um 83% gestiegen und werden immer raffinierter. 70 % aller erfolgreichen Cyberangriffe werden durch einen unbedachten Klick auf einen böswilligen Link oder den versehentlichen Download von Schadprogrammen verursacht." Johannes Vakalis, Head of Sales & Marketing bei Perseus Technologies

Johannes Vakalis trifft es auf den Punkt. Die Anzahl an Cyberangriffen hat in den letzten Wochen, Monaten, Jahren stark zugenommen. Gerade vor diesem Hintergrund erfüllt der Beschluss der Richtlinie nach § 75B Sozialgesetzbuch (SGB) V über die Anforderungen zur Gewährleistung der IT-Sicherheit seine Zweckdienlichkeit. Die Richtlinie setzte erste Anforderungen der 16-seitigen Richtlinie bereits zum 01.04.2021 und die restlichen Anforderungen ab Januar bzw.Juli 2022.

Hervorzuheben ist, was auch die Ergebnisse der aktuellen HDI Cyber-Studie* aufzeigen, dass hier ein aktueller Handlungsbedarf im Bereich des Gesundheitswesens besteht, insbesondere bei Ärzten und Apothekern. Präventionsmaßnahmen sind wichtig und sollten in den täglichen Arbeitslauf integriert werden.

Nach den Resultaten der HDI Cyber Studie haben beispielsweise nur 33 % der Befragten eine teilweise Umsetzung von Präventionsmaßnahmen im Bereich „Mitarbeiterverhalten, z. B. Schulungen" angegeben, wohingegen bei 23 % der Befragten der Status auf „in Planung" gesetzt ist. 14 % haben sich noch gar nicht mit dem Thema befasst. Auch bei den Präventionsmaßnahmen im Bereich der technischen Maßnahmen, z. B. Backups und Firewall sprechen 32 % von einer teilweisen Umsetzung. Dies zusammengefasst, macht deutlich, dass ein generelles Gefahren- und Risikoverständnis in Bezug auf Cybergefahren existiert und nur noch nicht in den Praxen vollständig verinnerlicht ist.

* zu der Versicherungs- und IT-Entscheider von mehr als 500 KMU in Deutschland durch das Forschungs- und Beratungsinstitut Sirius Campus repräsentativ befragt wurden



Quelle: Repräsentative KMU-Stichprobe von 518 Unternehmen durch Sirius Campus im Auftrag von HDI

Die HDI Cyberversicherung mit simulierten Phishing E-Mails stellt somit einen spürbaren Indikator zur Steigerung des Gefahrenbewusstseins der Mitarbeiter dar:

Als Partner in der HDI Cyberversicherung führt Perseus Technologies GmbH in unregelmäßigen Abständen Phishing Simulationen mit verschiedenen Phishing Vorlagen durch. Mit Hilfe von Tracking Links kann das Verhalten der Mitarbeitenden unserer Versicherungsnehmer gebündelt nachverfolgt und statistisch ausgewertet werden.

Diese Umstände machen deutlich, warum die Richtlinie über die Anforderungen zur Gewährleistung der IT-Sicherheit nach § 75B SGB V ihren Fokus auf die Schutzziele von Vertraulichkeit, Integrität und Verfügbarkeit der IT-Systeme legt.

Risikofaktor Mensch

Die aktuellen Schadenzahlen[1] zeigen, dass eine Vielzahl an Schäden[2] [3] nicht durch Schwachstellen der Software hervorgerufen, sondern durch das Verhalten von Mitarbeitern verursacht werden. So ergibt auch die KPMG-Studie aus 2019[4] zu e-Crime in der deutschen Wirtschaft, dass acht von zehn Cybervorfällen auf unzureichend geschulte Mitarbeiter zurückzuführen sind. Ähnliches spiegelt auch der GDV über die Forsa-Befragung im Frühjahr 2019 wider: 70 % der erfolgreichen Cyberangriffe wurden durch E-Mails verursacht.

Begünstigt werden diese Schäden in Arztpraxen und Apotheken, durch Shared-User-Accounts, also Nutzerkonten, die von mehreren Personen gleichzeitig genutzt werden. So bekommen mehrere Menschen denselben Zugang mit identischen Rechten und Legitimationen. Auch die Passwortqualität und Geheimhaltung leiden unter einer Mehrfachverwendung eines einzelnen Nutzerkontos. Unabhängig davon werden Cybergefahren unterschätzt, was aus unserer Erfahrung zwei Ursachen hat:

Punkt 1:
Viele Unternehmen gehen davon aus, dass ihr Unternehmen zu klein sei, die Systeme umfassend geschützt und / oder die Daten nicht interessant genug seien. Außerdem wird angeführt, dass bisher auch noch keine Cyberattacke stattgefunden habe. Dies ist ein gefährlicher Denkfehler. Für die Kriminellen ist die Unternehmensgröße irrelevant und die Qualität der Daten ist zweitranging. Sie zielen in erster Linie auf das Konto! Kriminelle haben häufig ein finanzielles Interesse. Jedes Unternehmen kann Opfer werden, da es keinen hundertprozentigen Schutz geben kann. Attacken auf kleinere Unternehmen werden massenhaft gestreut. Es geht selten um zielgerichtete Angriffe.

Außerdem müssen es nicht immer nur externe Angreifer sein. Unterschätzt wird häufig der innere Personenkreis. In der Regel gehen Unternehmen zu Recht davon aus, dass die eigenen Mitarbeiter keine böswilligen Absichten hegen. Aus unserer Schadenerfahrung wissen wir, dass der Faktor Mensch beim Abwägen eines Cyberrisikos berücksichtigt werden muss. Im Detail bedeutet dies, dass der Mensch sowohl geplant als auch unwillkürlich einen Schaden in der betrieblichen Netzwerkstruktur hervorrufen kann. Es ist daher essenziell, Präventionsmaßnahmen zu initiieren. Schlussendlich spielt die Unwissenheit bzw. fehlende Sensibilisierung der Mitarbeitenden eine schwerwiegende Rolle. Daher werden viele ungezielte Angriffe durch Unachtsamkeit ermöglicht.

Punkt 2:
Das Cyberrisiko ist nicht greifbar und wird daher unterschätzt. Ein nicht greifbares Risiko ist nur schwer monetär zu bemessen. Verständlicherweise fällt es einem Unternehmer deshalb nicht leicht, eine kaufmännische Entscheidung zu treffen.

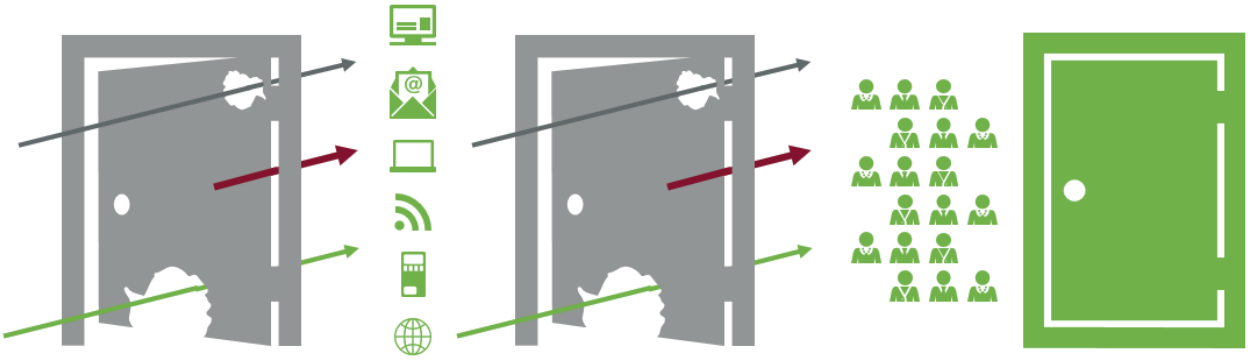
Schlussfolgernd sind bei einem Cyberangriff gerade Arztpraxen und Apotheken bei dem Thema IT-Sicherheit und Datenschutz noch nicht optimal aufgestellt und im Ernstfall hilflos. Dabei ist bei einer möglichen Datenpanne nach der Europäischen Datenschutz-Grundverordnung (DSGVO) bereits im Vorfeld einer Risikobewertung der Datensicherheit notwendig und bei Bekanntwerden einer sogenannten Datenpanne ein zügiges Handeln geboten.

Wichtig: Nach Art. 33 Abs. 1 DSGVO muss eine Datenpanne binnen 72 Stunden, nach der Kenntnis der Datenschutzverletzung, an die zuständige Datenschutzbehörde gemeldet werden.
Cyberdeckung bei HDI – das ist mehr als nur Versicherung:
Eine Cyberversicherung dient nicht nur der Absicherung von finanziellen Risiken, sondern bietet zusätzlich den Zugang zu einem umfangreichen Expertennetzwerk und zu IT-Spezialisten. Diese begleiten den Arzt oder Apotheker im konkreten Fall aus der Misere hinaus – quasi ein Rundumschutz.

[1] Tagesschau BKA Cyberkriminalität
[2] Phishing bleibt in der Pandemie wichtigstes Einfallstor für Cyberangriffe
[3] Kommunikation in der Praxis - E-Mails als Gefahr
[4] KPMG-Studie 2019: e-Crime in der deutschen Wirtschaft

... bietet Rundum-Schutz

Die HDI Cyberversicherung bietet rund-um-Schutz



Technische Maßnahmen, z. B.

- Virenschutz
- Firewall
- Intrusion-Detection-System
- Penetrations-Tests

Organisatorische & personelle Maßnahmen, z. B.

- Benennung Verantwortliche
- Risikosensibilisierung der MA
- Schulungen

HDI Cyberversicherung, z. B.

- Soforthilfe
- IT-Sicherheitsdienstleister
- Risikotransfer
- Wiederherstellung von Daten

Unter den genannten Punkten und Anforderungen der IT-Sicherheitsrichtlinie wird sich sukzessiv das Informationssicherheitsniveau steigern und auch kontinuierlich verbessern, jedoch werden die umzusetzenden technischen und organisatorischen Maßnahmen keinen hundertprozentigen Schutz darstellen können.

Die HDI Cyberversicherung schließt gerade diese Lücke des Restrisikos, sodass finanzielle und existenzbedrohende Schäden auf eine Versicherung transferiert werden. Weiter bietet die HDI Cyberversicherung Leistungen, die über den normalen Versicherungsschutz hinausgehen. Schulungs- und Präventionsmaßnahmen, eine 24/7-Hotline und ein IT-Sicherheitsdienstleister, der sich durch besondere Expertise in Sachen Cybersicherheit auszeichnet, sind dabei Dreh- und Angelpunkte.

Für weitere Informationen zum Produkt, Leistungen und Inhalten sehen Sie sich gerne unser Produktprofil an!

Autor

Sönke Glanz, HDI Produktmanagement, Underwriter Cyber

Unser Tipp

Mit dem „MedLetter" informiert HDI Sie regelmäßig über neue Entwicklungen der Rechtsprechung aus der beruflichen Tätigkeit in der ambulanten Medizin und in den Gesundheitsfachberufen.

Wir legen besonderen Wert darauf aktuelle, juristische Sachverhalte, wichtige Urteile und Entscheidungen allgemein-verständlich und damit insbesondere für Nichtjuristen aufzubereiten.

Gerade Themen wie Haftung, aktuelle Rechtssprechung, Schadenfälle, Riskmanagement und versicherungsrechtliche Fragen sind ständig in Bewegung und betreffen Sie unmittelbar. Mit dem MedLetter erhalten Sie wichtige Informationen und Hinweise für Ihre Berufspraxis und sind immer auf dem Laufenden.

Melden Sie sich am besten gleich an unter: www.hdi.de/medletter

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

Marketing-Unterlage