Kooperationspartner des

IFK – Bundesverband selbstständiger Physiotherapeuten – IFK e. V.

HELMSAUER GRUPPE

PHYSIONews

Exklusiv. Aktuell. Informativ.

Cyberkriminalität im Gesundheitswesen

– so schützen Sie Ihre Physiotherapiepraxis

In Zeiten umfassender Konnektivität ist die Gefahr von Cyberattacken leider alltäglich geworden. Die Cyberkriminalität macht gerade vor dem Gesundheitswesen nicht halt. Kaum eine Branche hantiert mit so sensiblen Daten, die es zu schützen gilt. Allerdings zeigt die Realität, dass Physiotherapiepraxen oftmals Informations- und Nachholbedarf in Bezug auf Schutzmaßnahmen haben.

Experten berichten sehr häufig zu erleben, dass sich viele Physiotherapiepraxen mit der Begründung in Sicherheit wiegen, dass sie als Adressat für Cyberattacken viel zu klein und unscheinbar im Gegensatz zu größeren Unternehmen seien. Gerade das Gegenteil ist der Fall! Gesundheitsdaten sind im Darknet begehrter denn je und viele Cyberattacken finden heute, von Servern oder Robotern gesteuert, rein zufällig statt. Diese schlagen dort zu, wo mangelnde Sicherheitsvorkehrungen sie nicht aufhalten.

Die häufigsten erfolgreichen Angriffsarten sind, laut einer Forsa-Studie, E-Mails und Hackerangriffe, die die Netzwerkstruktur gegen Forderung eines Lösegeldes lahm legen. Bei 59 % der Betroffenen führten die Cyberattacken zu wirtschaftlichen Schäden durch Kosten für Aufklärung und Wiederherstellung der Daten. 43 % der Betroffenen mussten eine vorübergehende Unterbrechung ihres Betriebes hinnehmen. Dicht gefolgt von Reputationsschäden und tatsächlichen Datendiebstählen.

Verschlechterung der Situation durch die Corona-Pandemie

Seit Beginn der Corona-Pandemie haben gezielte Cyberangriffe und Ransomware-Attacken auf bestimmte Branchen deutlich zugenommen. Dazu gehört insbesondere das Gesundheitswesen. Vergleicht man die Zahlen der Cyberattacken auf das Gesundheitswesen von Mitte 2019 mit März 2020, so ist ein Anstieg um 73 % zu verzeichnen. Dies zeigt, dass Cyberkriminelle die Pandemie genutzt haben, um dezidiert Angriffskampagnen zu starten.

Experten-Prognosen 2022

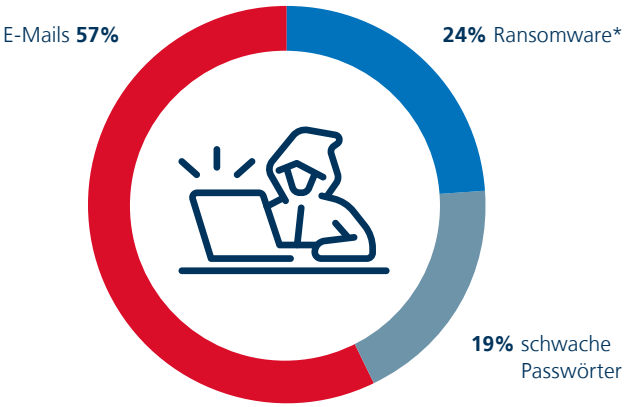
Die Veröffentlichungen von Auswertungen, Expertenmeinungen und Studien zu Beginn des Jahres 2022 sind sich einig, dass das Gesundheitswesen nach wie vor eine der am meisten gefährdetsten Branchen ist. Gerade hier ist der Druck Lösegelder zu bezahlen besonders hoch, um die sensiblen Patientendaten zu schützen.

Eine aktuelle Untersuchung von Kaspersky bestätigt, dass Patientendaten im Darknet besonders hoch gehandelt werden. Der Schutz der sensiblen Daten ist teuer, aber dennoch unerlässlich, da mit vermehrten Angriffen zu rechnen ist. Zudem werden Patientendaten zunehmend bei Cloud-Diensten gespeichert – ein weiterer Angriffspunkt für Cyberkriminelle.

Regierungsentwurf zum IT-Sicherheitsgesetz 2.0

Das Kabinett hat den Entwurf des IT-Sicherheitsgesetzes 2.0 beschlossen, das einen Durchbruch für Deutschlands IT-Sicherheit bringen soll. Dies unterstreicht die hohe Bedeutung der Cybersicherheit. Besonders im Fokus stehen kritische Infrastrukturen, zu denen das Gesundheitswesen zählt. Ein zentraler Punkt ist hier die Stärkung der Vorsorgepflichten für Einrichtungen in kritischen Infrastrukturen.

Was sind die größten Gefahrenquellen?



* Schadprogramme, die Daten verschlüsseln, um Lösegeld zu fordern.

So schützen Sie sich aktiv

Die Untersuchungen haben gezeigt, dass viele erfolgreiche Cyberangriffe nicht nur auf mangelnde Sicherheitssysteme, sondern auch auf menschliches Handeln zurückzuführen sind. „Das größte Sicherheitsrisiko sitzt vor dem Bildschirm", heißt es immer und das hat einen Vorteil. Welchen? Die Antwort lautet, dass dann Sicherheit und Schutz trainierbar sind. Über Sensibilisierung für Cybersicherheit, intelligente Sicherheitssoftware und schnelle Unterstützung von Experten im Ernstfall kann der Cyberangriff abgewehrt oder im Ernstfall der Schaden gemindert werden. Durch die aktuellen Entwicklungen angeregt, bieten professionelle Dienstleister interessante Lösungen an:

Phishing-Tests

Um sich vor Phishing-Attacken zu schützen, müssen sie als solche erkannt werden. Dafür ist es notwendig, Ihr Wissen zu der Vorgehensweise und den Möglichkeiten der Kriminellen zu erweitern. Videobasierte, praxisorientierte Online-Trainings sowie Webinare, um zu lernen, wie jeder Laie solche E-Mails zu erkennen vermag, helfen immens. Die leicht verständlichen, kompakten und anwenderfreundlichen Einheiten sensibilisieren für das Risiko und sind einfach in den Alltag zu integrieren. Somit sind diese auch machbar, wenn wenig Zeit neben dem Beruf übrig bleibt. Dienstleister bieten zudem Phishing-Simulationen an. Sie und Ihre Mitarbeiter erhalten von dem Dienstleister über einen Zeitraum realitätsnahe Phishing-Emails und können so Ihr erlerntes Wissen als praktische Übung trainieren.

Intelligente Software

Moderne Sicherheitssoftware-Lösungen bieten nicht nur effektiven Antivirenschutz, sondern zusätzlichen Schutz über die Integration künstlicher Intelligenz und maschinelles Lernen. Dadurch wird die Schadsoftware nicht nur erkannt, sondern verhindert auch deren Installation. Viren, Trojaner, Würmer und andere Schadsoftware verändern sich schnell – oft täglich. Die künstliche Intelligenz datet sich live online up, lernt dazu und kann so gefährliche Ähnlichkeiten zu bekannter Schadsoftware erkennen. Dadurch wird ein deutlich umfangreicherer Schutz vor Cyberangriffen erreicht, als dies herkömmlich der Fall war.

Mitarbeiterschulungen – online und jederzeit durchführbar

Schulungen sind dann am besten, wenn das Gelernte schnell im Alltag anwendbar ist. Kurze und kompakte Webinare informieren zu den Cyberrisiken im Praxisalltag, sensibilisieren für die Thematik und liefern Unterstützung beim Schutz vor Cyberangriffen. In Kombination mit Online-Trainings für Mitarbeiter, die jederzeit durchführbar sind, werden die Abläufe in der Praxis nicht behindert. Dennoch lernen die Mitarbeiter gezielt und tragen so erheblich zur Sicherheit der Praxis bei.

Werkzeugkasten – Hilfe für den Alltag

Mit gezielten Helfern für den Alltag sparen Sie Zeit und integrieren dennoch die notwendigen Maßnahmen zur Cybersicherheit in Ihren Praxisalltag. Dienstleister bieten über ein Online-Portal, zu dem der Anwender einen individuellen und sicheren Zugang erhält, die technischen Helfer an. So lässt sich z. B. mit einem Klick der Browser auf den neuesten Stand überprüfen. Die neueste Software bietet immer die höchste Sicherheit. Passwort-Generatoren erstellen schnell und einfach sichere Passwörter. Mit E-Mail-Scans lassen sich binnen kurzer Zeit die eingehenden E-Mails auf gefährliche Inhalte überprüfen.

Hilfe im Notfall

Im Angriffsfall ist die schnelle und kompetente Hilfestellung von Profis ausschlaggebend für das Ausmaß der Schädigung. Cyberversicherungen decken nicht nur viele materielle Schäden, sondern bieten umfassende Serviceleistungen zur Schadenbekämpfung und aktiven Unterstützung im Ernstfall. Spezielle Produkte bieten den Zugriff auf Cybercrime-Dienstleister 24-Stunden, die Ihnen im Fall der Fälle rund um die Uhr schnelle Hilfe leisten und keine zusätzlichen Kosten anfallen.

Hilfe für den Ernstfall –
was ist bei einem aktiven Cyberangriff zu tun?

Im Falle eines akuten Cyberangriffes muss klar sein, wer was zu tun hat, welche Informationen benötigt werden und wie zu kommunizieren ist. Wie immer, wenn es um die Gestaltung von Prozessen geht, an denen mehrere Personen beteiligt sind, macht es Sinn, diese aufzuschreiben und für die Beteiligten jederzeit zugänglich zu machen. Aus diesem Grund ist es empfehlenswert, diese Abläufe in das Qualitätsmanagement der Praxis zu integrieren. Auch die Thematisierung in regelmäßigen Teambesprechungen schafft Nachhaltigkeit.

Notfall-Checkliste

- ✓ Foto vom Bildschirm mit Smartphone anfertigen (+ Protokoll, Datum, Uhrzeit)
- ✓ Alle Netzwerkverbindungen trennen
- ✓ Systemdokumente/-informationen griffbereit haben (Notfallplan)
- ✓ Professionellen Cybercrime-Experten kontaktieren
- ✓ Externen Zugang zu den Systemen zur Schadenfeststellung und Begrenzung ermöglichen
- ✓ Diskretion bewahren
- ✓ Kollegen anleiten A,B,C zu tun

Um im Ernstfall weitere Schäden zu vermeiden, sind korrekte Maßnahmen und schnelle Umsetzung entscheidend für das Ausmaß der Verwüstung. Die Unterbrechung der Internetverbindung und das Ausschalten der Geräte sind als Primärmaßnahme unerlässlich, um die Verbreitung im System möglichst einzuschränken. Meist lässt sich dies nicht mehr vollständig verhindern. Aus diesem Grund sind Profis gefragt. Auf die Abwehr von Cyberangriffe spezialisierte Dienstleister bieten einen Notfallsupport 24/7 und sind in der Lage, sich extern auf die Systeme zu schalten, eine erste Einschätzung der Situation zu geben und oftmals bereits mit der Bekämpfung zu beginnen. Der absolute Vorteil ist, dass sich diese Experten, im Vergleich zu herkömmlichen IT-Häusern, hauptberuflich mit der Abwehr von Cyberattacken beschäftigen. Dies führt zu dem Wissen, welche Schadsoftware aktuell in Umlauf ist und daraus eine schnelle Bekämpfung resultieren kann.

Das Ausmaß der Schädigung ist relevant für die daraus resultierenden Folgen. Diese gehen vorerst nur Sie etwas an! Interne und externe Diskretion ist unerlässlich, um möglicherweise Reputationsschäden zu vermeiden. So haben Sie noch die Chance, sich über die weiteren Schritte in Ruhe Gedanken zu machen und notfalls Beratung einzuholen. Zur Wahrung von Diskretion müssen Sie Ihr Personal anleiten. Zu empfehlen sind Checklisten im Rahmen des Qualitätsmanagements. Hier ein Beispiel zur Unterstützung im Ernstfall.

Wenn alle Stricke reißen

Sollte es trotz aller Vorsicht und Schutzmaßnahmen zu einem Cyberangriff kommen, ist es hilfreich, die Physiotherapiepraxis über eine leistungsstarke **Cyberversicherung** abgesichert zu haben. Hier bieten wir ein spezielles Konzept für IFK-Mitglieder, das besonders auf die Bedürfnisse von Physiotherapiepraxen ausgelegt ist. Neben dem Versicherungsschutz erhalten Sie auch bereits einige der genannten Service-Leistungen und Schulungsprogramme kostenfrei. Aufgrund der aktuellen Entwicklungen ist es uns in diesem Jahr gelungen, die Inhalte des Rahmenkonzepts nochmals zu verbessern.

Rahmenkonzept für IFK-Mitglieder nochmals verbessert:

- ✓ **Kostenfreies Cyber-Security-Training für alle!** Kostenfreier Zugang zu Online-Trainings und automatisierten Phishingtests sowie zahlreiche Schulungsvideos rund um das Thema Cybersicherheit für Sie und Ihre Mitarbeiter/-Innen. Zusätzlich kostenfreie Webinare zu aktuellen Entwicklungen der Cybercrime, Präventivmaßnahmen und Handlungsempfehlungen durch die Helmsauer Akademie
- ✓ **Zweifache Maximierung der Versicherungssumme**
- ✓ **Garantierte und unverzügliche Hilfestellung** im Schadenfall – Rund um die Uhr!
- ✓ **Mitversicherung von Eigenschäden** in der Forensik und Schadenfeststellung
- ✓ **Vermögensschäden aus gefälschten E-Mails** mit Aufforderung zu Geldtransaktionen („Fake-President")
- ✓ **Wiederherstellungskosten** (inkl. Hardware-Ersatz)
- ✓ **Mitversicherung von Drittschäden**, z. B. Abwehr unberechtigter Schadenersatzansprüche
- ✓ Soweit gesetzlich zulässig: **Übernahme von Bußgeldern**
- ✓ **„Bring your own device"-Deckung** z. B. berufliche Nutzung privater Smartphones
- ✓ **Betriebsunterbrechung zur Sicherung Ihres Umsatzes** – Dies gilt auch bei technischen Störungen
- ✓ **Erweiterung** der Betriebsunterbrechungsleistung um Mehrkosten
- ✓ **Internet-Diebstahl**
- ✓ **Cyber-Spionage**
- ✓ **Cyber-Erpressung**

Ihre IFK-Hotline bei der Helmsauer Gruppe: **0911-9292 185**

> Rückantwortfax: 0911-9292 432

Ja, ich möchte weitere Informationen für Verbandsmitglieder erhalten.
Bitte nehmen Sie mit mir Kontakt auf: ☐ Cyberversicherung für IFK-Mitglieder ☐ Weiterbildungsangebot zur Cybersicherheit

☐ Herr ☐ Frau _____
Name, Vorname

_____ _____
E-Mail Telefon

Stempel:

ANTWORTSCHREIBEN an:

Helmsauer Gruppe
Dürrenhofstraße 4
90402 Nürnberg

Per E-Mail **service@helmsauer-gruppe.de**
oder per Fax **0911- 9292 432**