HELMSAUER

GRUPPE

Cyberdeckung ohne Risikofragen?

Das geht! – Nutzen Sie die Chance als Verbandsmitglied

Laut aktueller Studien bleibt die Bedrohungslage für die Cybersicherheit in Deutschland äußerst angespannt (2023/24). Insbesondere Ransomware und generative KI machen Sorgen.

Die Lage in Bezug auf Cybersicherheit in Deutschland bleibt besorgniserregend, wie aus dem Bericht des BSI für das Jahr 2023 hervorgeht. Trotz Bemühungen bleibt das allgemeine Bedrohungsniveau unverändert hoch.

Eine Viertelmillion...

...neue Schadprogramm-Varianten wurden in 2023 durchschnittlich an jedem Tag gefunden.

Quelle: BSI

Nicht nur „alte" Methoden in „neuem" Look sind auf dem Vormarsch, sondern auch Schwachstellen und mangelnde revolvierende Sicherheitsvorkehrungen führen zu erfolgreichen Cyberattacken:

Dauerbrenner Phishing

KI-basiertes Phishing: Cyberkriminelle könnten künstliche Intelligenz nutzen, um äußerst zielgerichtete und überzeugende Phishing-E-Mails zu erstellen. KI-Algorithmen können große Datensätze analysieren, um Nachrichten zu erstellen, die den Schreibstil bestimmter Personen imitieren und somit schwerer von legitimer Kommunikation zu unterscheiden sind.

66 %

aller Spam-Mails in 2023 waren Cyberangriffe:

34 % Erpressungsmails

32 % Betrugsmails

84 %

aller betrügerischen E-Mails waren Phishing-E-Mails zur Erbeutung von Authentisierungsdaten

Quelle: BSI

Schwachstellen

Schwachstellen in der Technologie stellen oft eine Eintrittspforte für Cyberangriffe dar, unabhängig davon, wie robust die Sicherheitsprotokolle erscheinen mögen. Einige der Hauptursachen für diese Schwachstellen sind:

1. **Softwarefehler und Konstruktionsmängel**
2. **Veraltete oder unzureichend umgesetzte Sicherheitsmaßnahmen**
3. **Schwache Verschlüsselung**
4. **Fehlendes Sicherheitsbewusstsein und -kultur**

Um diese Schwachstellen zu minimieren, ist eine umfassende Sicherheitsstrategie erforderlich, die regelmäßige Updates, Patch-Management, Schulungen für Mitarbeitende und eine kontinuierliche Überwachung und Bewertung der Sicherheitslage umfasst. Cyberangriffe können nie vollständig ausgeschlossen werden, aber eine proaktive Herangehensweise kann das Risiko erheblich reduzieren.

Ihre Lösung: ALL-IN-ONE für Verbandsmitglieder

- ✓ Analyse der vorhandenen Schwachstellen
- ✓ Entwicklung einer klaren Sicherheitsstrategie
- ✓ Notfallpläne für den Ernstfall
- ✓ Sensibilisierung der Mitarbeitenden
- ✓ Cyberversicherung als Existenzschutz

HIGHLIGHT!!

WEGFALL DER RISIKOFRAGEN

Ihr schneller Weg zur leistungsstarken Cyberdeckung

› EINFACH. SCHNELL. SICHER

Sicherheit durch Wissen: Der Security-Check

Kostengünstig. Professionell. Unkompliziert.

Prüfen Sie das Sicherheitskonzept Ihrer Physiotherapiepraxis.

Anhand eines Fragebogens sowie technischer und organisatorischer Begutachtung wird der aktuelle Sicherheitsstandard einer Praxis bestimmt. Gerade für die Untersuchung des Sicherheitsniveaus und die Risikobewertung durch Versicherungsunternehmen ist ein solcher Status quo enorm hilfreich.

Der Security-Check ist für Sie in nur wenigen Schritten unkompliziert durchzuführen und sollte regelmäßig erfolgen.

Ziel des Checks

- Nutzerkonten-Sicherheit
- Schutz gegen Schadsoftware
- Netzwerk-Sicherheit
- Patch-Management
- Datensicherungskonzept

Genau richtig: Nur wenige Schritte

1 Fragebogen

Eigene Angaben:

Mithilfe eines von uns vorgegebenen Leitfadens geben Sie Ihre Einschätzungen zunächst selbst ab.

2 Risikodialog

Direkter Austausch:

Ihre vorigen Angaben werden dann telefonisch besprochen, um alle Aspekte genauestens abzudecken.

3 Analyse & Dokumentation

Fremdcheck:

Ein Analyst überprüft und dokumentiert im Anschluss die technische Umsetzung von Sicherheitsaspekten in Ihrem System per Fernverbindung.

Technische Checks

User-Management
Nutzer des Betriebssystems, Berechtigungen und geteilte Konten werden ebenso geprüft wie die Sicherheit der Passwörter.

Anti-Virus-Software
Die in der Praxis genutzte Anti-Virus-Software inkl. Signaturen, Autostart und Lizenz wird getestet.

Konfiguration der Firewall
Der Firewall-Regelsatz auf Zugänge zu internen Systemen und Internetservices wird untersucht.

Patch-Management
Der Patchstand des Betriebssystems wird ebenso kontrolliert wie die Patch-Management-Konfiguration. Außerdem wird der Patchstand installierter Standardprogramme stichprobenartig geprüft.

Organisatorische Checks

Backup-Konzept
Es wird überprüft, ob Sicherheitskonzepte oder -prozesse und dazugehörige empfohlene Vorgehensweisen in der Praxis eingehalten werden.

Umfang der Analyse

Um die Sicherheitsanforderungen zu prüfen, werden stichprobenartig einzelne Systeme (maximal drei) analysiert und zufällig ausgewählte Dokumente gesichtet. Außerdem werden Mitarbeiter zu bestimmten Sicherheitsaspekten befragt. Bei einer solchen Analyse werden nur die wichtigsten Einstellungen, also die Basiskonfigurationen, betrachtet. Das spart Zeit und Aufwand, deckt aber dennoch die Anforderungen an eine sichere Physiotherapiepraxis ab.

Ihre Vorteile auf einen Blick

- Status quo des aktuellen Sicherheitsstandards Ihrer IT-Systeme
- Aufdecken von Sicherheitslücken und Verbesserungspotenzialen
- Prüfung technischer und organisatorischer Maßnahmen zur Cybersicherheit
- Reportbericht zur Dokumentation und ggf. Unterstützung zur Enthaftung
- Optionaler Zusatzbaustein p.a. in Ihrem Cyberversicherungskonzept
- Versicherungsschutz unabhängig vom Check-Ergebnis möglich
- Verzicht auf den Einwand der Obliegenheiten möglich
- Kein Selbstbehalt beim ersten Schadenfall

Machen Sie den Check!

Wie sicher ist Ihre Praxis?
Fragen Sie jetzt Ihr persönliches Sicherheitsrisiko ab.

Wenn alle Stricke reißen

Sollte es trotz aller Vorsicht und Schutzmaßnahmen dennoch zu einem Cyberangriff kommen, ist es hilfreich, die Physiotherapiepraxis über eine leistungsstarke Cyberversicherung abgesichert zu haben. Hier bieten wir ein spezielles Konzept für Verbandsmitglieder, das besonders auf die Bedürfnisse von Physiotherapiepraxen ausgelegt ist. Neben dem Versicherungsschutz erhalten Sie auch bereits einige der genannten Service-Leistungen und Schulungsprogramme kostenfrei. Durch Gründung unserer Assekuradeur GmbH ist es uns gelungen, die Inhalte des Rahmenkonzeptes nochmals zu verbessern.

Rahmenkonzept für Verbandsmitglieder nochmals verbessert:

- ✓ **Kostenfreies Cyber-Security-Training für alle** Ihre Mitarbeiterinnen und Mitarbeiter mit Online-Training und Erklär-Videos und einem Wissenstest sowie Bereitstellung einer datenschutzkonformen Softwareplattform zur Prüfung von potenziell infizierten E-Mails und eines Werkzeugkastens für eine sichere Passwort-Programmierung
- ✓ **Zweifache Maximierung der Versicherungssumme**
- ✓ **Garantierte und unverzügliche Hilfestellung durch Cybercrime-Experten** im Schadenfall – rund um die Uhr!
- ✓ **Mitversicherung von Eigenschäden** in der Forensik und Schadenfeststellung
- ✓ **Vermögensschäden aus gefälschten E-Mails** mit Aufforderung zu Geldtransaktionen
- ✓ **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 Betriebsunterbrechungs-Leistung um Mehrkosten
- ✓ **Internet-Diebstahl**
- ✓ **Cyber-Spionage**
- ✓ **Cyber-Erpressung**
- ✓ **Sicherheitsanalyse: Cyber-Security-Check**

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

> Rückantwortfax: 0911-9292 432 **> oder über unser digitales Kontaktformular:**

Ja, ich möchte weitere Informationen zu folgenden Themen erhalten: ☐ Cyberversicherung ☐ Security-Check

Bitte nehmen Sie mit mir Kontakt auf:

☐ 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**

Hinweis zum Datenschutz: Die o. a. Angaben werden ausschließlich zur Berechnung/Beratung von Angeboten verwendet. Sie können der Speicherung Ihrer personenbezogenen Daten jederzeit widersprechen.
Weitere Infos zum Datenschutz finden Sie unter: www.helmsauer-gruppe.de/datenschutz

Stand 23/04/2024