HORNETSECURITY BY proofpoint.

FACTSHEET

CYBERSECURITY IM GESUNDHEITSSEKTOR

Digitale Unterbrechungen im Gesundheitswesen können sich auf Forschung, Gesundheitsversorgung, Vertrauen und Sicherheit auswirken.

In der heutigen digitalen Welt des Gesundheitswesens hängt alles, von der Diagnose und Behandlung bis hin zu Patientenakten und Abrechnungen, von sicheren und zuverlässigen IT-Systemen ab. Ein einziger Sicherheitsverstoß kann weitreichende Folgen haben und nicht nur sensible Patientendaten gefährden, sondern auch den Klinikbetrieb stören, Behandlungen verzögern und im schlimmsten Fall sogar Leben gefährden. Anders als in vielen anderen Branchen bedeutet eine Betriebsunterbrechung im Gesundheitswesen nicht nur Produktivitätsverluste und finanzielle Einbußen, sie kann sich auch direkt auf die Gesundheit der Patienten auswirken, weshalb Cybersicherheit ein kritischer Faktor für eine hochwertige Versorgung ist.

Wieso ist das Gesundheitswesen ein bevorzugtes Ziel?

» **Wertvolle Daten:** **Gesundheitsorganisationen verfügen über umfangreiche personenbezogene Daten, die sich ideal für Identitätsdiebstahl, Betrug und Erpressung eignen**

» **Dringlichkeit der Versorgung:** **Zeitdruck erhöht die Wahrscheinlichkeit, dass Lösegeld gezahlt wird, um den Betrieb schnell wiederherzustellen**

» **Der Faktor Mensch:** **vielbeschäftigte Mitarbeiter und komplexe Zusammenarbeit bedeuten ein erhöhtes Risiko für Phishing, Social Engineering und versehentliche Datenlecks**

» **Veraltete Infrastruktur:** **veraltete Systeme und schwer zu patchende Umgebungen schaffen ausnutzbare Sicherheitslücken**

PATIENTEN- UND BETRIEBSDATEN	FORSCHUNGSDATEN
• Patientenakten und Krankengeschichten • Diagnosen, Laborergebnisse, Bildgebungsdaten • Versicherungs-, Abrechnungs- und Zahlungsdetails • Zugangsdaten, E-Mails und interne Dokumente von Mitarbeitern	• Daten und Protokolle zu klinischen Studien • Datensätze von Forschungsteilnehmern • Genom- und Biomarker-Daten • Studienergebnisse und Dokumente zur Zusammenarbeit
Vertrauen, Glaubwürdigkeit, Ruf, Vertrauen der Stakeholder	**Forschungsintegrität, Arbeitgebermarke**

03/26

hornetsecurity.com | info@hornetsecurity.com | +49 511 515 464-0

HORNETSECURITY
BY proofpoint.

$7.42 MIO.
Durchschnittliche Kosten einer Datenschutzverletzung im Gesundheitswesen (seit 14 Jahren in Folge die teuerste Branche)

279 TAGE
Durchschnittliche Zeit bis zur Identifizierung und Eindämmung einer Datenschutzverletzung im Gesundheitswesen (längste Zeit aller Branchen, >5 Wochen länger als der Durchschnitt)

18 %
der Ransomware-Angriffe im Gesundheitswesen wurden durch kompromittierte Anmeldedaten verursacht

22 %
der Angriffe im Gesundheitswesen wurden durch bösartige E-Mails verursacht

WAS PASSIERT, WENN DATEN GESTOHLEN WERDEN

1. TÄUSCHUNG
Phishing-E-Mail | gefälschte Anmeldung | „dringende Anfrage“

2. ZUGRIFF ERLANGT
z. B. über gestohlene Anmeldedaten

3. VERBREITUNG
geteilte Links
laterale Bewegungt

4. DATEN GEFUNDEN
Patientenakten
Forschungsdateien

5. EXFILTRATION
Daten werden unbemerkt kopiert

6. DRUCK
Lecks der Daten im Dark Web führen zu Erpressung | Lösegeldforderungenen wiederholte Erpressung

VEREINBAREN SIE JETZT IHRE DEMO

HORNETSECURITY
BY proofpoint.

10 BEST PRACTICES UM DATENVERSTÖSSE ZU VERHINDERN

Evaluieren & verbessern

1. Führen Sie regelmäßige Risikobewertungen von Systemen, Geräten und Arbeitsabläufen durch.
2. Testen Sie Kontrollen (simulieren Sie Angriffe, prüfen Sie Erkennungs- und Reaktionspläne).

Menschliche Risiken reduzieren

3. Schulen Sie Ihre Belegschaft kontinuierlich (z. B. zu Phishing und Social Engineering).
4. Schaffen Sie eine Kultur, in der Sicherheit an erster Stelle steht (klare Berichterstattung).

Zugriff & Systeme schützen

5. Implementieren Sie strenge Zugriffskontrollen nach dem Prinzip der geringsten Privilegien ('Principle of least privilege').
6. Nutzen Sie Multi-Faktor-Authentifizierung (MFA) überall, wo dies möglich ist.
7. Patchen und aktualisieren Sie IT- und medizinische Geräte.

Schützen und wiederherstellen

8. Verschlüsseln Sie sensible Daten.
9. Sichern Sie kritische Systeme und Daten mithilfe einer robusten Backup-Strategie wie 3-2-1-1.
10. Entwickeln Sie einen Plan für die Reaktion auf Vorfälle, welcher Rollen, Kontaktpersonen und Prioritäten für die Wiederherstellung klar definiert.

WIE HORNETSECURITY DAS GESUNDHEITSWESEN UNTERSTÜTZT

Eine umfassende Cloud-Sicherheitssuite für Microsoft 365, die Sicherheit, Compliance, Sensibilisierung und Backup abdeckt. Sie hilft Organisationen im Gesundheitswesen, Vorfälle zu verhindern und sich schneller zu erholen. Hier ein Einblick in einige der hilfreichen Dienste, die enthalten sind:

SECURITY AWARENESS	Stärken Sie Ihre menschliche Firewall mit gezielten Schulungen und realistischen Phishing-Simulationen, um die Anfälligkeit für Angriffe im Laufe der Zeit messbar zu reduzieren.
ADVANCED THREAT PROTECTION	Schützt vor raffinierten Angriffen (z. B. Spear-Phishing, Ransomware, Zero-Day-Exploits) mithilfe fortschrittlicher Erkennungsmethoden.
SPAM & MALWARE PROTECTION	Blockiert bösartige E-Mail-Inhalte, bevor sie die Posteingänge Ihrer Mitarbeiter erreichen, und schützt so die klinische Kommunikation und reduziert Risiken im Posteingang.
365 TOTAL BACKUP	365 Total Backup: Ermöglicht die schnelle Wiederherstellung von Microsoft 365-Daten, um die Kontinuität der Versorgung und die Einhaltung von Vorschriften zu unterstützen und gleichzeitig die Auswirkungen von Ransomware und versehentlichem Löschen zu reduzieren.
PERMISSION MANAGEMENT	365 Permission Manager: Erzwingt den Zugriff mit geringsten Berechtigungen in Microsoft 365 und macht auf riskante Freigaben und Fehlkonfigurationen aufmerksam.

hornetsecurity.com | info@hornetsecurity.com | +49 511 515 464-0