HORNETSECURITY

INFOSHEET
AI POWERED

SECURITY AWARENESS SERVICE

FÜR ORGANISATIONEN IM GESUNDHEITSWESEN

Die Cyberbedrohungen im Gesundheitswesen nehmen weiter zu, da menschliches Versagen, digitale Schwachstellen und komplexe Lieferketten wichtige Daten gefährden. Integrierte Cybersicherheitsinitiativen in Kombination mit maßgeschneiderten Sicherheitsschulungen versetzen Ihr Team in die Lage, die Abwehrkräfte zu stärken und wichtige Dienste zu schützen.

WACHSENDE BEDROHUNGEN FÜR DEN GESUNDHEITSSEKTOR

Organisationen des Gesundheitswesens werden zunehmend zur Zielscheibe ausgeklügelter Cyberangriffe, wobei mehrere größere Angriffe und jüngste Trends zu verzeichnen sind:

- Vermehrte Cyber-Vorfälle: Im Jahr 2023 haben sich die Cyber-Ereignisse im Gesundheitssektor fast vervierfacht und enthüllten mehr als 133 Millionen Datensätze bei 725 Sicherheitsverletzungen.
- Ransomware-Störungen: Angriffe wie der Vorfall bei Change Healthcare und andere haben gezeigt, wie Ransomware wichtige medizinische Verfahren verzögern, die Notaufnahme blockieren und die Patientensicherheit gefährden kann.
- Schwachstellen der digitalen Expansion: Mit der Einführung von digitalen Hilfsmitteln in Krankenhäusern – wie zum Beispiel elektronische Gesundheitsakten, Telemedizin, KI-Diagnosen und mehr - wächst auch die Zahl der potenziellen Einstiegspunkte für Cyberkriminelle.
- Lieferkette und Compliance-Risiken: Die Interdependenz digitaler Systeme und der Druck, strenge Cybersicherheitsvorschriften einzuhalten, haben die Cybersicherheit im Gesundheitswesen noch komplexer gemacht.

Diese Herausforderungen gefährden nicht nur die Patientenversorgung, sondern setzen die Organisationen auch erheblichen finanziellen und Reputationsrisiken aus.

HEUTE AKTIV WERDEN

Lassen Sie nicht zu, dass Cyberbedrohungen Ihre Gesundheitsdienste gefährden. Statten Sie Ihr Team mit dem notwendigen proaktiven Schutz aus.

JETZT DEMO BUCHEN

SECURITY
AWARENESS SERVICE

EU-AKTION: EINE RICHTLINIE FÜR PROAKTIVE CYBERSICHERHEITSMASSNAHMEN

Als Reaktion auf diese eskalierenden Bedrohungen hat die Europäische Kommission einen umfassenden Aktionsplan zur Stärkung der Cybersicherheit im Gesundheitswesen vorgestellt. Zu den wichtigsten Aspekten gehören:

- Prävention Beratung & Finanzielle Hilfe: Angebot von Gutscheinen für Cybersicherheit und maßgeschneiderte Anleitungen, um Krankenhäusern zu helfen, stärkere Schutzmaßnahmen zu ergreifen.
- Erkennung von Bedrohungen und schnelle Reaktion: Vorschlag für ein EU-weites Frühwarnsystem und ein spezielles Zentrum zur Unterstützung der Cybersicherheit im Gesundheitswesen.
- Internationale Zusammenarbeit: Einsatz von Instrumenten wie der Cyber Diplomacy Toolbox zum Schutz vor bösartigen Cyberaktivitäten.

DIE BEDEUTUNG DES SICHERHEITSBEWUSSTSEINS

95 % aller Vorfälle im Bereich der Cybersicherheit werden durch menschliches Versagen verursacht. Mitarbeiter stehen an vorderster Front im Kampf gegen Cyber-Bedrohungen. Umfassende Schulungen zum Sicherheitsbewusstsein können:

- Personal befähigen: Geben Sie jedem Teammitglied das Wissen an die Hand, um Bedrohungen wie Phishing und Ransomware zu erkennen und zu entschärfen.
- Verbesserte Compliance: Stellen Sie sicher, dass Ihr Unternehmen die strengen EU-Cybersicherheitsvorschriften erfüllt.
- Reduzieren Sie Unterbrechungen: Vermeiden Sie Verzögerungen bei wichtigen Gesundheitsdiensten durch die Minimierung des Risikos erfolgreicher Cyberangriffe.
- Patientendaten schützen: Schützen Sie die sensiblen Informationen, die essenziell für das Vertrauen und die Versorgung des Patienten sind.

SECURITY AWARENESS SERVICE: PARTNER FÜR DIE CYBERABWEHR IM GESUNDHEITSWESEN

Hornetsecurity bietet hochmodernes Security Awareness Training an, das zum Schutz von Organisationen in einer Vielzahl von Branchen, einschließlich des Gesundheitswesens, entwickelt wurde. Hier sehen Sie, wie unsere Lösung den Unterschied macht:

- Maßgeschneiderte Trainingsprogramme: Maßgeschneiderte Module gehen auf die besonderen Herausforderungen der Cybersicherheit im Gesundheitswesen ein und stellen sicher, dass Ihre Mitarbeiter auf reale Bedrohungen vorbereitet sind.
- Umfassender Inhalt: Vom sicheren Surfen im Internet bis zum sicheren Umgang mit persönlichen Gesundheitsdaten deckt unsere Schulung alle wichtigen Themen ab.
- Leichte Implementierung: Unser Service ist so konzipiert, dass er sich nahtlos in Ihre bestehenden Systeme integrieren lässt, wodurch Ausfallzeiten reduziert und die allgemeine Ausfallsicherheit erhöht wird.
- Laufende Unterstützung: Kontinuierliche Aktualisierungen und Folgemaßnahmen stellen sicher, dass Ihr Unternehmen den sich entwickelnden Cyber-Bedrohungen immer einen Schritt voraus ist.