Medizinisch
Personal
Technologie

Management des Cyberrisikos

relyens

EUROPÄISCHE GRUPPE AUF GEGENSEITIGKEIT
VERSICHERUNG UND RISIKOMANAGEMENT

relyens.eu

DAS RISIKOMANAGEMENT

Das Risikomangement von Relyens unterstützt Sie bei der Aufrechterhaltung Ihrer Geschäftskontinuität, der Sicherstellung der Patientenbehandlung und der Optimierung des Cyberbudgets. Das sind unsere Ziele im Risikomanagement.

Unser Geschäft ist es, Risiken zu identifizieren, denen Sie ausgesetzt sind, und diese zu minimieren. Wir bieten Ihnen Lösungen in folgenden Risikobereichen an:

- Medizinische Risiken
- Technologische Risiken

Unsere jahrzehntelange Erfahrung ermöglicht es uns, einen umfassenden Ansatz zu entwickeln, um Sie bei Ihren (Cyber-) Herausforderungen zu unterstützen.

STEUERUNG | **PRÄVENTION** | **VERSICHERUNG**

DIE CYBERKRIMINALITÄT IST EIN STÄNDIGER FAKTOR, DER DIE SICHERHEIT DER GESUNDHEITSVERSORGUNG GEFÄHRDET

Die Patientensicherheit und die Kontinuität der medizinischen Versorgung werden heute von der zunehmenden Bedrohung durch Cyberkriminalität gefährdet.

Der zunehmende Einsatz von Technologie und deren gegenseitigen Abhängigkeiten durch Vernetzung gefährdet die kontinuierliche Patientenversorgung der Gesundheitseinrichtung:

- Fehlfunktionen (Programmfehler, Fehlkonfigurationen, 0-Days)
- Erpressungsversuche (Ransomware, Dataleakage)

Rund **21.000** infizierte Systeme und **250.000** Schadprogramm-Varianten werden letztes Jahr täglich erkannt und vom BSI (Bundesministerium für Sicherheit in der Informationstechnik) an die deutschen Provider gemeldet.

Um dieser Cyberbedrohung zu begegnen, schlagen wir Ihnen einen umfassenden Ansatz vor, bei dem die Reife der (Cyber-) Sicherheitspolitik Ihrer Gesundheitseinrichtung berücksichtigt wird.

STEUERUNG - IHR RISIKONIVEAU DANK UNSERER RISIKOSTEUERUNGSLÖSUNG FÜR CYBER VERSTEHEN

WIE?

Relyens bietet Ihnen eine neuartige und innovative Lösung für:

- Die **Quantifizierung des Risikos** auf Basis Ihrer Daten, um eine genaue Beschreibung Ihres Risikos zu erhalten
- Die **Cyber-Security-Budgetplanung**, welche Ihnen die Möglichkeit gibt, virtuelle Auswirkungen von Cyber-Lösungen auf Ihr Risiko zu testen, um die maximale Effizienz Ihres Cyberbudgets sicherzustellen
- Umsetzbare **Empfehlungen und operative Lösungen**, die auf Ihr Unternehmen zugeschnitten sind, um die Auswirkungen von Risiken zu begrenzen

Relyens hat sich mit Citalid, einem französischen Start-up-Unternehmen, welches sich auf Cyber Threat Intelligence (CTI)* spezialisiert hat, zusammengeschlossen, um eine einzigartige und souveräne Lösung zur Steuerung von Cyberrisiken zu entwickeln. Die Lösung berechnet das Cyberrisiko und die möglichen Verluste, die mit den verschiedenen Angriffsszenarien verbunden sind, denen jede Gesundheitseinrichtung ausgesetzt ist, präzise und schätzt sie in Euro.

**CTI: Cyber Threat Intelligence definiert die Erforschung, Analyse und Modellierung von Cyberbedrohungen.*

MIT WELCHEN ERGEBNISSEN?

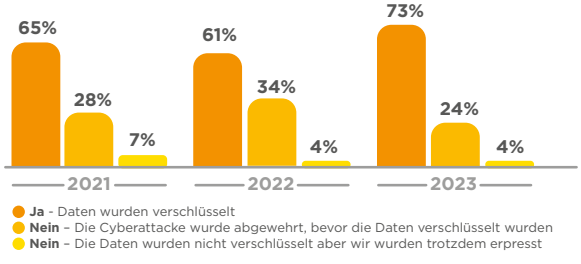
- **Umfassende Steuerung:** von der strategischen Vision bis zum operativen Ansatz
- **Vorausschauende Angriffsvektoren**, die in zwei Szenarien (Ransomware und Datenleck) standardmäßig vordefiniert werden:
  - Anzahl der Cyberangriffe, denen Ihre Einrichtung durchschnittlich ausgesetzt ist
  - Die Wahrscheinlichkeit eines erfolgreichen Angriffs
  - Die durchschnittlichen und maximalen personalisierten finanziellen Kosten (darunter Betriebsverluste, zusätzliche Betriebskosten…)
  - Die angepasste jährliche empfohlene Rückstellung zur Deckung des Risikos
  - Empfehlungen, die auf Ihren Kontext zugeschnitten sind
- eine Auswahl an **technologischen Lösungen** zur Prävention, die auf Ihre Bedürfnisse ausgerichtet sind
- eine **Rationalisierung und Planung** der in Ihrer Einrichtung umzusetzenden Cyber-Sicherheitsmaßnahmen
- eine **dynamische Überwachung Ihrer Risiken** entsprechend der sich verändernden Bedrohungslage

Die größte Bedrohung geht aktuell von Ransomware aus. Sie machen aktuell 60% aller erfolgreichen Cyberangriffe auf Gesundheitseinrichtungen aus:

2021	2022	2023
34%	66%	60%

Quelle: The State of Ransomware in Healthcare in 2023 by Sophos

Übersicht der Ransomwareangriffe



Quelle: The State of Ransomware in Healthcare in 2023 by Sophos

PRÄVENTION - DURCH EINE VORAUSSCHAUENDE STRATEGIE VORBEUGEN

WIE?

Wir bieten in Partnerschaften mit Forescout und Cynerio, zwei der weltweit führenden Anbieter von Cybersicherheit, technologische Lösungen an, die sich den Herausforderungen des Gesundheitswesens widmen.

Sie profitieren dabei von einer

- **Vollständigen Abbildung und Kategorisierung** aller Geräte, die sich in Ihren Netzwerken befinden, inklusive IoT, IoMT und Medical OT-Geräte
- **Identifizierung** der **Expositionsfläche**: Risikobewertung für jedes Gerät entsprechend seiner Nähe zum Patienten (Verletzlichkeit, Bedrohung, Konformität)
- **Analyse der Kommunikationsflüsse** innerhalb des Netzwerks und Erkennung von Verhaltensanomalien mittels eines nicht invasiven Netzwerkanalysesystems
- **Risk Governance**: Erstellung von IT- und biomedizinischen Berichten, die automatisch von der Lösung generiert werden, und die Möglichkeit, Ihre eigenen Berichte anzupassen

MEHR INFOS

VERSICHERUNG - UM DIE FINANZIELLEN UND RUFSCHÄDIGENDEN AUSWIRKUNGEN ZU BEGRENZEN

EINE ÜBERNAHME DER KOSTEN FÜR DEN VORFALL: CYBERVERSICHERUNG

Das Risiko kann mit unseren Ansätzen stark reduziert werden, dennoch wird es niemals gänzlich verschwinden. In jedem Fall sollte das Restrisiko über eine Versicherung abgedeckt werden.

Unsere Cyberversicherung ist ein speziell für Akteure des Gesundheitswesens entwickeltes Produkt.

- Die Risikoübernahme beinhaltet Garantien für die Bewältigung von Vorfällen, die Wiederherstellung im Falle einer Verletzung personenbezogener Daten und schützt die Einrichtung vor der Haftung im Falle einer Verletzung personenbezogener Daten
- die Übernahme der Schritte zur Validierung der Integrität der Patientendaten durch die jeweiligen Herausgeber vor der Wiederinbetriebnahme des Informationssystems

UNTERSTÜTZUNG BEI DER KRISENBEWÄLTIGUNG

Wir begleiten Sie vom ersten Augenblick des Vorfalls an bei Ihrem Krisenmanagement:

- 24/7 Persönliche Betreuung und Nachverfolgung von Vorfällen durch Cyber-Sicherheitsexperten
- Rechtsberatung zur Beantwortung Ihrer Fragen durch unsere Juristen
- Unterstützung bei der Krisenkommunikation im Falle von Medienereignissen, die dem Ruf der Einrichtung schaden könnten

Ein ganzheitlicher Ansatz für das Management von Cyber- und IT-Risiken VOR, WÄHREND und NACH einem Vorfall:

Relyens Mutual Insurance
Niederlassung Deutschland:
Erkrather Straße 228b
40233 Düsseldorf
kontakt@relyens.eu

Dieses Dokument wurde von der Kommunikationsabteilung der Gruppe Relyens erstellt - 50141-DEU-24A-02/2024 - Bildnachweis: © G - Stockadobe.com

Relyens Mutual Insurance
VVaG nach französischem Recht
Niederlassung Deutschland:
Erkrather Straße 228b, 40233 Düsseldorf, DEUTSCHLAND
Tel.: +49 (0)221 882427 00 - www.relyens.eu
Handelsregister HRB Nr. 29551

relyens
EUROPÄISCHE GRUPPE AUF GEGENSEITIGKEIT
VERSICHERUNG UND RISIKOMANAGEMENT