RISIKOBEREIT ODER RISIKOGEFÄHRDET:

COHESITY

Die Kluft in der Cyber-Resilienz in Gesundheitswesen

Cyberangriffe sind keine isolierten Einzelgeschehen mehr, sondern ein anhaltendes Merkmal unserer digitalen Welt. Jeder Tag bringt eine neue Mahnung, da Gesundheitseinrichtungen weltweit zunehmend ins Visier geraten. Kein Unternehmen ist immun, und die zunehmende Häufigkeit und Raffinesse der Bedrohungen haben zu einer Flut von schwerwiegenden Cyberangriffen geführt, die messbare finanzielle, operative und Reputationsschäden verursachen.

EINE WELTWEITE UMFRAGE UNTER FAST 400 ENTSCHEIDUNGSTRÄGERN AUS DEN BEREICHEN IT- UND SICHERHEITSBETRIEB IN GESUNDHEITSORGANISATIONEN ZEIGT DIE REALITÄT AUF.

85 %
der Gesundheitsorganisation en haben einen schwerwiegenden Cyberangriff erlebt

66 %
wurden in den letzten 12 Monaten angegriffen

1 VON 3
Jede dritte wurde mehrfach angegriffen

DER SCHADEN IST BETRÄCHTLICH UND **DIE KOSTEN SUMMIEREN SICH SCHNELL.**

92 %
verzeichneten Umsatzeinbußen

59 %
verloren Patienten oder Kunden

80 %
der börsennotierten Unternehmen mussten ihre Finanzprognosen revidieren

97 %
sahen sich mit rechtlichen oder regulatorischen Konsequenzen konfrontiert

94 %
zahlten in den letzten 12 Monaten Lösegeld

TROTZ KLARER BELEGE ÜBERSCHÄTZEN VIELE ORGANISATIONEN IM GESUNDHEITSWESEN IHRE RESILIENZ.

49 %
haben volles Vertrauen in ihre Cyber-Resilienz-Strategie

DIE MEISTEN PRIORISIEREN IMMER NOCH PRÄVENTION UND ERKENNUNG GEGENÜBER DEN EBENSO WICHTIGEN FUNKTIONEN DER REAKTION UND WIEDERHERSTELLUNG.

Reihenfolge basierend auf dem NIST-Cybersicherheits-Framework. Die Größe der Kästchen zeigt den Anteil der Investitionen in Cyber-Resilienz vom höchsten zum niedrigsten an.

#2	#1	#3	#4	#5
Identifizieren	Sichern	Erkennen	Reagieren	Wiederherstellen

VERTRAUEN UND AUSGABENMUSTER GEBEN JEDOCH **NUR BEGRENZT AUFSCHLUSS ÜBER DIE GESAMTLAGE**

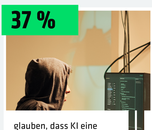
Wahre Resilienz stützt sich auf Praktiken und Fähigkeiten, die sie untermauern. Bei der Bewertung anhand der realen Leistungskriterien zeigen nur 2 % der Unternehmen Reife in fünf wesentlichen Bereichen: **Datensicherung, Datenwiederherstellung, Bedrohungserkennung und -untersuchung, Anwendungsresilienz und Optimierung des Datenrisikos.**

Ein Bewusstsein für die Notwendigkeit, die Resilienz zu verbessern, treibt die nächste Entwicklung voran – unterstützt durch Automatisierung und KI. Da Bedrohungen immer schneller und komplexer werden, ist die Automatisierung der Schlüssel zur schnelleren Erkennung, effizienteren Reaktion und verbesserten Wiederherstellung.

61 %

geben an, dass eine bessere Automatisierung bei der Erkennung, Reaktion und Wiederherstellung zu den wichtigsten Erkenntnissen nach dem Cyberangriff gehören.

37 %



glauben, dass KI eine zentrale Rolle bei der Erkennung und Reaktion auf Bedrohungen spielen wird, einschließlich autonomer Entscheidungsfindung.

99 %

planen, bis 2026 KI zur Unterstützung von Datensicherheitsvorgän gen zu nutzen.

SIND SIE AUF RISIKEN VORBEREITET?

- **Jetzt den Cyber-Resilience-Branchenbericht für das Gesundheitswesen herunterladen** – mit detaillierten Ergebnissen.
- **Buchen Sie einen Ransomware-Resilienz-Workshop.**
- Holen Sie sich unser E-Book **„5 wichtige Schritte zur Verbesserung der Cyber-Resilienz Ihres Unternehmens“,** um Ihre Reife noch heute voranzutreiben.

Vanson Bourne befragte 3.200 Führungskräfte aus den Bereichen IT und Sicherheit aus nordamerikanischen, asiatisch-pazifischen, europäischen und lateinamerikanischen Regionen, die Organisationen mit 1.000 oder mehr Mitarbeitern im Jahr 2025 repräsentieren. Zu den Befragten gehörten 371 Teilnehmer aus Gesundheitsorganisationen.

COHESITY VansonBourne

COHESITY
cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054
6200507-001-EN 4-2026