RISIKOBEREIT ODER RISIKOGEFÄHRDET

COHESITY

Die digitale Kluft der Cyber-Resilienz im öffentlichen Sektor

Cyberangriffe sind keine isolierten Einzelgeschehen mehr, sondern ein anhaltendes Merkmal unserer digitalen Welt. Jeden Tag werden wir erneut daran erinnert, dass Organisationen des öffentlichen Sektors weltweit zunehmend ins Visier genommen werden. 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 399 ENTSCHEIDUNGSTRÄGERN AUS DEN BEREICHEN IT- UND SICHERHEITSBETRIEB IN ORGANISATIONEN DES ÖFFENTLICHEN SEKTORS ZEIGT DIE REALITÄT AUF.

67 %
der Organisationen haben bereits einen schwerwiegenden Cyberangriff erlebt

49 %
wurden in den letzten 12 Monaten angegriffen

1 VON 4
Jeder vierte wurde mehrfach angegriffen

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

85 % verzeichneten Umsatzeinbußen

42 % verloren Kunden

61 % der börsennotierten Unternehmen mussten ihre Finanzprognosen revidieren

97 % erlitten rechtliche oder regulatorische Konsequenzen

92 % zahlten in den letzten 12 Monaten Lösegeld

TROTZ DIESER OFFENSICHTLICHEN BEWEISLAGE ÜBERSCHÄTZEN VIELE UNTERNEHMEN IHRE RESILIENZ.

54 %
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. Identifizieren

1. Sichern

3. Erkennen

4. Reagieren

5. 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 4 % der Unternehmen Reife in fünf wesentlichen Bereichen: **Datensicherung, Datenwiederherstellung, Bedrohungserkennung und -untersuchung, Anwendungsresilienz und Optimierung des Datenrisikos.**

11 % Am wenigsten ausgereift

22 % Aufstreben

57 % Entwicklungsphase

8 % Verbesserung

4 % Am weitesten entwickelt

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.

56 %

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

42 %

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

98 %

planen, bis 2026 KI zur Unterstützung von Datensicherheitsvorgänge n zu nutzen.

SIND SIE AUF RISIKEN VORBEREITET?

Laden Sie den Bericht zur Cyber-Resilienz im öffentlichen Sektor herunter, um detaillierte Ergebnisse zu erhalten.

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 399 Teilnehmer aus Organisationen des öffentlichen Sektors.

COHESITY VansonBourne

COHESITY
cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

6200042-001-GE 4-2026