

RISIKOBEREIT ODER RISIKOGEFÄHRDET:

The digitale Kluft der Cyber-Resilienz im Finanzdienstleistungssektor



Cyberangriffe sind keine isolierten Einzelgeschehen mehr, sondern ein anhaltendes Merkmal unserer digitalen Welt. Jeden Tag werden wir erneut daran erinnert, dass Finanzdienstleistungsunternehmen 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 FAST 400 ENTSCHEIDUNGSTRÄGERN AUS DEN BEREICHEN IT- UND SICHERHEITSBETRIEB IN FINANZDIENSTLEISTUNGSUNTERNEHMEN ZEIGT DIE REALITÄT AUF.

77 %

der Finanzdienstleistungsunternehmen haben bereits einen schwerwiegenden Cyberangriff erlebt

57 %

wurden in den letzten 12 Monaten angegriffen

Jeder vierte

wurde mehrfach angegriffen

DER SCHADEN IST BETRÄCHTLICH UND DIE KOSTEN SUMMIEREN SICH SCHNELL

87 %

verzeichneten Umsatzeinbußen

35 %

verloren Kunden

62 %

der börsennotierten Finanzdienstleistungsunternehmen mussten ihre Finanzprognosen revidieren

93 %

erlitten rechtliche oder regulatorische Konsequenzen

79 %

zahlten in den letzten 12 Monaten Lösegeld

TROTZ DIESER OFFENSICHTLICHEN BEWEISLAGE ÜBERSCHÄTZEN VIELE FINANZDIENSTLEISTUNGSUNTERNEHMEN IHRE RESILIENZ.

46 %

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.

#3

Identifizieren

#1

Sichern

#2

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

4 %

Am wenigsten ausgereift

13 %

Aufstrebend

65 %

Entwicklungsphase

13 %

Verbesserung

5 %

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.

39 %



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 Datensicherheitsvorgängen zu nutzen.

SIND SIE AUF RISIKEN VORBEREITET?

Laden Sie den Bericht zur Cyber-Resilienz in der Finanzdienstleistungsbranche 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 Organisationen mit 1.000 oder mehr Mitarbeitern im Jahr 2025 repräsentieren. Zu den Befragten gehörten 390 Teilnehmer aus Finanzdienstleistungsunternehmen.