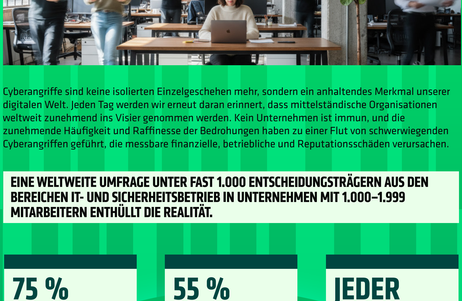
# RISIKOBEREIT ODER RISIKOGEFÄHRDET

COHESITY

## Die Kluft bei der Cyber-Resilienz in mittelständischen Organisationen



Cyberangriffe sind keine isolierten Einzelgeschehen mehr, sondern ein anhaltendes Merkmal unserer digitalen Welt. Jeden Tag werden wir erneut daran erinnert, dass mittelständische Organisationen 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, betriebliche und Reputationsschäden verursachen.

**EINE WELTWEITE UMFRAGE UNTER FAST 1.000 ENTSCHEIDUNGSTRÄGERN AUS DEN BEREICHEN IT- UND SICHERHEITSBETRIEB IN UNTERNEHMEN MIT 1.000–1.999 MITARBEITERN ENTHÜLLT DIE REALITÄT.**

**75 %**
der Organisationen haben bereits einen schwerwiegenden Cyberangriff erlebt.

**55 %**
wurde in den letzten 12 Monaten angegriffen.

**JEDER VIERTE**
wurde mehrfach angegriffen.

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

**85 %**
Entgangener Umsatz

**36 %**
haben Kunden verloren

**76 %**
der börsennotierten Unternehmen mussten ihre Finanzprognosen revidieren

**92 %**
sahen sich mit rechtlichen oder regulatorischen Konsequenzen konfrontiert

**82 %**
zahlten in den letzten 12 Monaten Lösegeld

**TROTZ DIESER OFFENSICHTLICHEN BEWEISLAGE ÜBERSCHÄTZEN VIELE UNTERNEHMEN IHRE RESILIENZ.**

**47 %**
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.

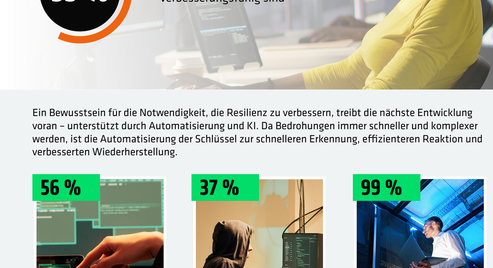
| Nr. 3 | Nr. 1 | Nr. 2 | Nr. 4 | Nr. 5 |
|---|---|---|---|---|
| Identifizieren | Sichern | Erkennen | Reagieren | Wiederherstellen |

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


Für die Organisationen mit der höchsten Cyber-Resilienz ist Resilienz ein systematischer und umfassender Ansatz. Neben anderen bewährten Methoden stellen sie sicher, dass sensible Daten weltweit gesichert werden, dass eine Multi-Faktor-Authentifizierung und Admin-Kontrollen durchgesetzt werden, dass Threat Intelligence maximiert wird, dass die Wiederherstellung durch Abhilfemaßnahmen sichergestellt ist und dass Compliance-Schutzmaßnahmen konsequent eingehalten werden.

## DENNOCH IST REIFE NICHT STATISCH.



**53 %**
geben an, dass ihre Resilienzstrategien noch verbesserungsfähig sind

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

**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 Datensicherheitsvorgäng en zu nutzen

## SIND SIE AUF RISIKEN VORBEREITET?

- Erfahren Sie mehr über **die Lösungen von Cohesity zur Cyber-Resilienz** für **mittelständische Unternehmen**.
- Bewerten Sie den **Reifegrad Ihrer Cyber-Resilienz** mit dieser **Resilienz-Scorecard**
- Optimieren Sie Ihre Cyber-Resilienz mit einem **Fünf-Schritte-Aktionsplan**

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 977 Teilnehmer aus mittelständischen Unternehmen mit 1.000-1.999 Mitarbeitern.

COHESITY VansonBourne



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

620003-001-DE 7-2026