zscaler™

THE RESILIENCE FACTOR

Das Vertrauen der Finanzwelt in die Cyber-Resilienz ist fehl am Platz

Ein neuer Report von Zscaler: **The Resilience Factor: Warum « Resilient by Design » für eine zukunftsfähige Cyberstrategie unverzichtbar ist.** Dies unterstreicht die Notwendigkeit einer stärkeren Priorisierung und höherer Investitionen, um sicherzustellen, dass Cyberresilienz-Strategien auf unvermeidliche zukünftige Ausfallszenarien vorbereitet sind.

FINANZWESEN: DIE WICHTIGSTEN ERGEBNISSE IM ÜBERBLICK

Angesichts zunehmender Bedrohungen und eines zunehmend volatilen Betriebsumfelds ist die Geschäftskontinuität gefährdet

45 % der Unternehmen erlebten **in den letzten 6 Monaten** ein schwerwiegendes Ausfallszenario

58 % der Unternehmen rechnen mit einem schwerwiegenden Ausfallszenario **in den nächsten 12 Monaten**

IT-Verantwortliche glauben, auf derartige Ausfallszenarien gut vorbereitet zu sein

59 % der IT-Verantwortlichen halten ihre IT-Infrastruktur für **hochgradig resilient**

81 % bezeichnen den Ansatz ihres Unternehmens zur Cyberresilienz als **ausgereift**

96 % halten ihre aktuellen Maßnahmen zur Cyberresilienz für **wirksam**

Bei genauerer Betrachtung werden jedoch Unstimmigkeiten, Lücken und Ineffizienzen sichtbar

NUR **49 %** der IT-Verantwortlichen geben an, ihre Cyberresilienz-Strategie sei dem **aktuellen Stand der KI-Entwicklung** gewachsen

40 % geben zu, **ihre Cyberresilienz-Strategie** in den letzten 6 Monaten nicht überprüft zu haben

Die nachstehend aufgezählten proaktiven Sicherheitstools werden jeweils von weniger als der Hälfte der Unternehmen eingesetzt

Mangelndes Interesse seitens der obersten Führungsebene als Reibungspunkt identifiziert

NUR 44 % der IT-Verantwortlichen glauben, dass Cyberresilienz für die Unternehmensführung oberste Priorität hat

46 % stimmen der Aussage zu, dass das für Cyberresilienz vorgesehene Budget den steigenden Bedarf nicht deckt

NUR 44 % sagen, dass die Cyberresilienz-Strategie in die allgemeine Resilienz-Strategie ihres Unternehmens integriert ist

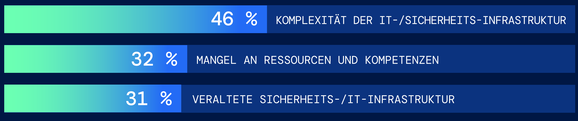
NUR 46 % sagen, dass der CISO an der Resilienzplanung beteiligt ist

Zur Überwindung der entscheidenden Hindernisse, die der Implementierung einer robusten Cyberresilienz-Strategie im Weg stehen, ist ein Mentalitätswandel erforderlich

61 % der IT-Verantwortlichen glauben, dass ihr Unternehmen der Prävention in ihrer Cybersicherheitsstrategie eine zu hohe Priorität einräumt

59 % sagen, dass ihre Geschäftsführung einen Cybersicherheitsausfall weiterhin als Erstzugriff (durch einen Bedrohungsakteur) definiert.

Die drei größten Hindernisse auf dem Weg zu mehr Resilienz:



Cyberresilienz von Anfang an in die Geschäftsstrategie integrieren

IT-Verantwortliche erkennen durchaus den Zusammenhang zwischen einer robusten Cyberresilienz-Strategie und einer besseren Geschäftsleistung, haben jedoch Schwierigkeiten, mit ihren derzeitigen Maßnahmen Ergebnisse zu erzielen.

56 % verzeichnen einen **Rückgang** der Datenverluste

53 % erleben **eine schnellere** Wiederherstellung nach Vorfällen

51 % berichten über eine **schnellere** Vorfallerkennung und -eindämmung

Der heutige Geschäftskontext erfordert, dass Unternehmen der Cyberresilienz mehr Aufmerksamkeit schenken — dass sie diese besser finanzieren, häufiger überprüfen und ihre Erwartungen an sie erhöhen. Es ist ein grundlegender Wandel in Ansatz und Denkweise erforderlich, um die Cyberresilienz von Anfang an zu einem wesentlichen Bestandteil der Sicherheitsstrategie zu machen. Wir nennen dies **« Resilient by Design ».**

Erfahren Sie hier mehr über den Ansatz « Resilient by Design », der durch die Zero Trust Exchange ermöglicht wird. Zum Report

METHODIK

Im Dezember 2024 beauftragte Zscaler Sapio Research mit der Durchführung einer Umfrage unter 1.700 IT-Entscheidungsträgern (IT-Verantwortlichen) in 12 Märkten (Australien, Frankreich, Deutschland, Indien, Italien, Japan, Niederlande, Singapur, Spanien, Schweden, Großbritannien und Irland, USA). 259 dieser IT-Verantwortlichen arbeiten bei Unternehmen aus der Finanzbranche.

ÜBER ZSCALER

Zscaler beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Die Zscaler Zero Trust Exchange schützt Tausende Kunden weltweit mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust. Die in 160 Rechenzentren auf der ganzen Welt verfügbare SSE-basierte Zero Trust Exchange ist die weltweit größte Inline-Cloud-Sicherheitsplattform.

zscaler™