zscaler

CISOs im Brennpunkt

Aus Sicht der CISOs

Anstatt der üblichen Schlagzeilen und der euphorischen Berichterstattung zur enormen Dynamik der Cybersicherheitsbranche enthält der von CISOs Connect in Zusammenarbeit mit der AimPoint Group und W2 Communications erstellte Report „CISOs im Brennpunkt“ eine Diskussion der größten Sorgen führender Experten im Bereich sowie der schwerwiegendsten Probleme, mit denen sich Teams konfrontiert sehen. Darüber hinaus werden die Prioritäten und Pläne aufgezeigt, die Cybersicherheitsbeauftragte zum erfolgreichen Schutz ihrer Unternehmen einsetzen.

Eine wichtige Erkenntnis: Die Implementierung eines Zero-Trust-Sicherheitsmodells hat aus Sicht der CISOs mittlerweile oberste Priorität.

Die derzeitige Risikoeinstufung in Bezug auf Cyberangriffe: EXTREM HOCH

75 %
waren mindestens einmal von einem Cyberangriff betroffen, der in den letzten 12 Monaten zu wesentlichen Schäden geführt hat.

57 %
waren von mehr als einem Cyberangriff betroffen, der in den letzten 12 Monaten zu wesentlichen Schäden geführt hat.

67 %
schätzen die Bedrohungslage heute schlechter ein als noch vor einem Jahr.

Die besorgniserregendsten Cyberbedrohungen

- Ransomware
- Phishing/Spear-Phishing
- Supply-Chain-Angriffe

Schwachstellen und Konsequenzen, die CISOs besonders beunruhigen

Die größten Sicherheitsrisiken

Nr. 1
Durch Drittparteien (wie verbundene Partner) verursachte Sicherheitslücken

#2
Ungepatchte Software/ Systeme

#3
Lücken in der Cloud-Sicherheit

Folgen eines erfolgreichen Angriffs

Nr. 1
Offenlegung von personenbezogenen Daten/Kundendaten

#2
Ausfallzeiten für kritische Infrastrukturen/Services

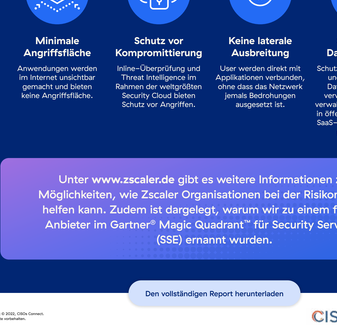
#3
Marken- oder Reputationsschäden

Externe Auswirkungen bereiten CISOs derzeit die größten Sorgen, da die Fehler in diesen Bereichen weitreichende Konsequenzen mit sich bringen, die sich über die betroffene Organisation hinaus auswirken.

Der bevorzugte Weg nach vorne

Angesichts der expandierenden Angriffsfläche und der anhaltenden Bedrohungslage setzt die überwältigende Mehrheit der Organisationen heutzutage auf ein Zero-Trust-Sicherheitsmodell.

Auf welchem Stand ist Ihr Unternehmen hinsichtlich der Implementierung eines Zero-Trust-Sicherheitsmodells?



96.5 %
Prozentsatz der CISOs, die zur Verbesserung des Sicherheitsstatus ihrer Organisation auf ein Zero-Trust-Sicherheitsmodell setzen

Identität als neuer Perimeter

Aufgrund der Cloud-Nutzung und Remote-Arbeit werden Ressourcen (Anwendungen, Systeme und User) aus dem Unternehmen heraus verlagert. Aufgrund dieses Wandels verlieren herkömmliche perimeterbasierte Ansätze für Netzwerksicherheit zunehmend an Bedeutung, da sie keine zuverlässige Vertrauensgrenze mehr darstellen. Das Grundprinzip von Zero Trust bringt eine zentrale Veränderung mit sich: Identität wird zum neuen Perimeter. CISOs müssen sich an diese sich neue Realität anpassen und setzen unter anderem auf die folgenden Maßnahmen:

- **Investitionen in Lösungen zur Minderung des Risikos durch offengelegte Anmeldedaten/ Identitätsangaben**
- **Zunehmende Überprüfung von User-Geräten vor der Zugriffsgewährung**
- **Investitionen in MFA-Lösungen der nächsten Generation zur Gewährleistung einer reibungslosen Anwendererfahrung**
- **Schnellere Einführung eines Zero-Trust-Sicherheitsmodells**

Die wichtigsten Technologie-Investitionen

Prozentsatz der Befragten, die in den nächsten 12 Monaten in die einzelnen Technologien investieren wollen:

63 %
Netzwerk-/ Mikrosegmentierung

56%
SSE-Plattform (Security Service Edge)

53 %
Cloud Native Application Protection Platform (CNAPP)

41 %
Deception Technology/ Aktive Abwehr

Schutz durch Zscaler

Die Zscaler Zero Trust Exchange ermöglicht eine sichere Cloud-Transformation und bietet standortunabhängigen Schutz für User, Anwendungen und Workloads. Zscaler basiert auf der weltweit größten Security Cloud und stoppt Bedrohungen anhand eines Vier-Stufen-Ansatzes:

Minimale Angriffsfläche

Anwendungen werden im Internet unsichtbar gemacht und bieten keine Angriffsfläche.

Schutz vor Kompromittierung

Inline-Überprüfung und Threat Intelligence im Rahmen der weltgrößten Security Cloud bieten Schutz vor Angriffen.

Keine laterale Ausbreitung

User werden direkt mit Applikationen verbunden, ohne dass das Netzwerk jemals Bedrohungen ausgesetzt ist.

Schutz vor Datenverlusten

Schutz vor Datendiebstahl und versehentlicher Datenexposition auf verwalteten und nicht verwalteten Geräten sowie in öffentlichen Clouds und SaaS-Anwendungen wird gewährleistet.

Unter **www.zscaler.de** gibt es weitere Informationen zu den Möglichkeiten, wie Zscaler Organisationen bei der Risikominderung helfen kann. Zudem ist dargelegt, warum wir zu einem führenden Anbieter im Gartner® Magic Quadrant™ für Security Service Edge (SSE) ernannt wurden.

Den vollständigen Report herunterladen

CISOs CONNECT