

Mit Firewalls und VPNs lässt sich Zero Trust nicht realisieren

Um die Produktivität und Sicherheit dezentraler Belegschaften zu gewährleisten, benötigen Unternehmen einen neuen Sicherheitsansatz.

Wir arbeiten heute anders als früher.

Heute sind User, Daten und Anwendungen überall.

300 %

höherer Anteil der Remote-User an der Belegschaft insgesamt.¹

50 %

aller Unternehmensdaten werden in der Cloud gespeichert.²

70 %

der Geschäftsanwendungen, mit denen Unternehmen heute arbeiten, sind SaaS-basiert.³

Neue Arbeitsmodelle erfordern neue Sicherheitskonzepte.

Der bisherige Ansatz, den Perimeter abzusichern und alle Entitäten und Ressourcen innerhalb des Netzwerks automatisch als vertrauenswürdig einzustufen, funktionierte gut, solange die User im Büro saßen und die Anwendungen im Rechenzentrum bereitgestellt wurden. Inzwischen gibt es den Perimeter im eigentlichen Sinn nicht mehr, und die herkömmlichen Methoden zur Absicherung des Netzwerks bieten keinen ausreichenden Schutz.



der Unternehmen sind der Meinung, dass sie ihre Sicherheitsvorkehrungen verbessern müssen, um Mitarbeiter im Büro und an Remote-Standorten zuverlässiger zu schützen.⁴



der Unternehmen priorisieren aktuell den Umstieg auf ein Zero-Trust-Modell.⁵

Die Lösung heißt Zero Trust.

Unternehmen, die mit zukunftsfähigen Arbeitskonzepten agil und wettbewerbsfähig bleiben wollen, dürfen sich nicht auf veraltete Sicherheitsarchitekturen verlassen. Stattdessen empfiehlt sich der Umstieg auf eine global verfügbare Lösung, die jede einzelne Verbindung zwischen einem User und einer Anwendung basierend auf Kontextdaten und Richtlinien genehmigt – und zwar unabhängig vom jeweiligen Standort.

Mit Firewalls und VPNs lässt sich Zero Trust jedoch nicht realisieren. Woran liegt das?

Bedrohungen können sich Zugang zum Netzwerk verschaffen und dort problemlos lateral ausbreiten. Denn mit Firewalls müssen User und Geräte wie gehabt mit dem Netzwerk verbunden werden, um Zugriff auf Anwendungen zu erhalten.



der Unternehmen bezweifeln, dass eine Umsetzung des Zero-Trust-Konzepts mit ihren vorhandenen Technologien möglich ist.⁵

Die Angriffsfläche des Unternehmens vergrößert sich, da Anwendungen im Internet öffentlich sichtbar sind.



der Unternehmen setzen ungerechtfertigtes Vertrauen in vorhandene Technologien und gewähren Usern Zugang zum Unternehmensnetzwerk.⁵

Daten können nicht zuverlässig geschützt werden, da die Passthrough-Architektur von Firewalls nur begrenzte Optionen zum Überprüfen des Traffics bietet.

Zero Trust basiert auf einem grundlegend anderen Ansatz.

Bei herkömmlichen Ansätzen werden Entitäten und Ressourcen innerhalb des Netzwerkperimeters automatisch als vertrauenswürdig eingestuft. Zero Trust beruht hingegen auf dem Prinzip der minimalen Rechtevergabe. Entsprechend wird keinem User und keiner Anwendung automatisch vertraut. Eine echte Zero-Trust-Lösung stellt basierend auf Geschäftsrichtlinien sichere Verbindungen zwischen Anwendungen und Usern über das Internet her. Das hat drei große Vorteile:



Keine laterale Bewegungsfreiheit

User und Geräte werden direkt mit Anwendungen – und niemals mit dem Netzwerk – verbunden.



Minimale Angriffsfläche

User und Anwendungen sind niemals im Internet sichtbar. Hacker können sie also weder entdecken noch angreifen.



Schutz vor Bedrohungen und Datenverlusten

Durch Überprüfen des gesamten verschlüsselten und unverschlüsselten Traffics wird zuverlässiger Schutz vor Cyberbedrohungen und Datenverlusten gewährleistet.

Zscaler: der Marktführer für Zero Trust.

Die Zscaler Zero Trust Exchange basiert auf der weltweit größten Security Cloud. Sie unterstützt bereits IT-Teams in zahlreichen Unternehmen bei der Umsetzung eines echten Zero-Trust-Konzepts, das Risiken reduziert, mehr Agilität ermöglicht und hervorragende Anwendererfahrungen gewährleistet.

Die Zscaler Zero Trust Exchange

SICHERT ÜBER 200 MILLIARDEN Transaktionen

VERHINDERT ÜBER 7 MILLIARDEN Sicherheitsvorfälle und Richtlinienverstöße

VERARBEITET ÜBER 200 000+ individuelle Sicherheits-Updates pro Tag

Die Zero-Trust-Transformation beginnt mit Zscaler.

Zscaler hat bereits über 5.000 Unternehmen bei der sicheren Transformation mit Zero Trust unterstützt.

Auf unsere Lösungen ist Verlass.

[Weitere Informationen](#)

