E-BOOK

Wie herkömmliche SD-WANs Ransomware-Angriffe begünstigen — und wie man sie verhindern kann

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Einführung

Obwohl die Sicherheitsherausforderungen stetig komplexer werden, haben sich die Netzwerkarchitekturen nicht entsprechend weiterentwickelt. Laut dem Ransomware-Report 2024 von Zscaler ThreatLabz wurden höhere Lösegeldzahlungen als je zuvor verzeichnet und die Zahl der erpressten Unternehmen stieg im Vergleich zum Vorjahr um 58 %. Ransomware verbreitet sich in Unternehmen aus einem einfachen Grund schnell: In veralteten Netzwerken werden alle verbundenen Entitäten automatisch als vertrauenswürdig eingestuft, sodass Ransomware ungehindert von infizierten Geräten in entfernten Zweigstellen zu den wichtigsten Anwendungen gelangen kann.

In der Vergangenheit verließen sich Unternehmen auf ein Sicherheitsmodell nach dem Festung-mit-Burggraben-Prinzip, bei dem der gesamte Traffic innerhalb des Netzwerks standardmäßig als sicher galt und Sicherheitskontrollen nur am Perimeter durchgesetzt wurden. Als ihre Netzwerke immer verteilter und cloudzentrierter wurden, dehnten Unternehmen diese einfach mithilfe von Software-Defined Wide Area Networks (SD-WAN) und Site-to-Site-VPNs auf Zweigstellen und Clouds aus. So entstanden große, flache, als vertrauenswürdig erachtete Netzwerke, in denen sich Angreifer trotz der Vielzahl flächendeckend eingesetzter Firewalls lateral bewegen können.

Mittlerweile umfassen Netzwerke eine ständig wachsende Zahl von IoT-Geräten. Schätzungen zufolge werden bis 2025 55,7 Milliarden dieser Geräte mit Unternehmensnetzwerken verbunden sein und jedes Jahr 80 Milliarden Zettabyte an Daten erzeugen.[1] Diese Erweiterung der Edge schafft eine immer größere Angriffsfläche, wodurch Unternehmen angreifbarer werden. All diese Trends machen perimeterbasierte Sicherheitsansätze zunehmend unhaltbar. Infolgedessen steigen Anzahl — und Kosten — von Datenpannen von Jahr zu Jahr weiter an und die Ransomware-Aktivitäten nehmen weiter zu.

Um ihre Infrastruktur vor diesen wachsenden Bedrohungen zu schützen, setzen Unternehmen branchenübergreifend zunehmend auf einen Zero-Trust-Ansatz für die Cybersicherheit.

17,8 % Anstieg der Ransomware-Angriffe von 2023 bis 2024.[2]

75 Millionen US-Dollar: Rekordverdächtige Lösegeldzahlung bei Ransomware-Angriff im Jahr 2024 gemeldet.[2]

104 % mehr Opfer von Datenschutzverletzungen zwischen 2023 und 2024.[3]

Die weltweiten Durchschnittskosten einer Datenpanne erreichten einen historischen Höchststand von **4,88 Millionen US-Dollar** im Jahr 2024.[4]

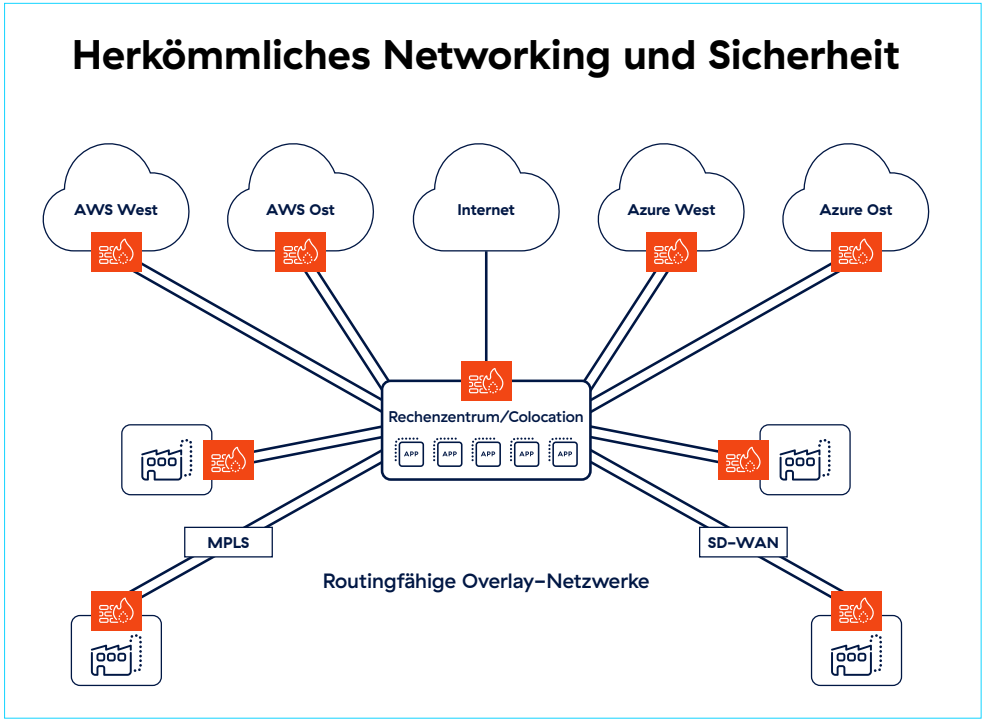
1: IDC Research, Future of Industry Ecosystems: Shared Data and Insights, 2021.
2: Ransomware-Report 2024 von Zscaler ThreatLabz.
3: Identity Theft Resource Center, Data Breach Analysis H1 2024.
4: IBM, Cost of a Data Breach Report 2024.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Was genau ist ein herkömmliches SD-WAN?

Ein SD-WAN nutzt Automatisierung, um den Traffic im Netzwerk auf dem effizientesten Weg über verschiedene Transportservices und Infrastrukturen zu leiten. Anwendungsorientierte Routing-Protokolle verbessern die Anwendungsperformance, indem sie den Traffic zwischen kritischen Anwendungen priorisieren.

Herkömmliche SD-WAN-Lösungen erweitern das Unternehmensnetzwerk einfach auf Zweigstellen und Rechenzentren. SD-WAN wurde entwickelt, um die Konnektivität zu vereinfachen, und ermöglicht es Geräten überall — auch in Zweigstellen, Fabriken und an externen Standorten — mit Anwendungen im Rechenzentrum oder in der öffentlichen Cloud zu kommunizieren. Diese Architekturen bestehen aus einem Geflecht von Geräten und Site-to-Site-VPNs und bieten wenig bis gar keinen Schutz vor lateralen Bedrohungsbewegungen und Ransomware.



Lässt laterale Ausbreitung von Bedrohungen zu, was Ransomware-Angriffe erleichtert

Erweitert die Angriffsfläche auf Zweigstellen, Fabriken und die Cloud

Erhöht Kosten, Komplexität und Bereitstellungszeiten

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

SD-WAN wurde entwickelt, um die Konnektivität zu verbessern und Usern einen schnelleren und einfacheren Zugriff auf Ressourcen bereitzustellen. Konnektivität bedeutet jedoch nicht gleich Sicherheit. Im Rahmen eines Zero-Trust-Ansatzes hingegen müssen Identität und Sicherheitsstatus überprüft werden, bevor eine Verbindung hergestellt wird. Das in Legacy-Netzwerke integrierte implizite Vertrauen erschwert nur deren Absicherung und begünstigt die schnelle Verbreitung von Ransomware.

Um Zero Trust in einem herkömmlichen SD-WAN zu realisieren, muss ein Unternehmen zusätzliche Sicherheitsanwendungen, Tools und Durchsetzungspunkte für Richtlinien einrichten. Das Ergebnis ist ein Sammelsurium aus Firewalls, Mesh-VPNs und anderen Tools wie Network Access Control (NAC), DNS-Sicherheitslösungen usw. Diese Architektur ist komplex und die Verwaltung bindet übermäßig viele finanzielle und personelle Ressourcen.

> „Tatsächlich steht die Konnektivität, die durch standardmäßiges Vertrauen erreicht wird, im Widerspruch zum Zero-Trust-Modell.“

Was ist Zero Trust?

Zero Trust ist eine Sicherheitsstrategie, die auf dem Prinzip beruht, dass keine Entität — User, App, Dienst oder Gerät — standardmäßig als vertrauenswürdig eingestuft werden darf. Nach dem Prinzip der minimalen Rechtevergabe wird vor dem Zulassen einer Verbindung die Vertrauenswürdigkeit basierend auf dem Kontext und der Sicherheitslage der Entität geprüft und dann für jede neue Verbindung kontinuierlich neu bewertet, auch wenn die Entität zuvor authentifiziert wurde.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Erste Schritte mit Zero Trust

Wenn man von einem offenen, flachen Netzwerk ausgeht und Durchsetzungspunkte und Sicherheitskontrollen hinzufügt, um Zero Trust zu erzielen, ist dies betrieblich komplex und teuer. Projekte zur Netzwerksegmentierung dauern oft Monate oder sogar Jahre, und die Anforderungen ändern sich oft, bevor diese Projekte abgeschlossen sind. Und wenn Sie es andersherum angehen könnten? Angenommen, Ihre Zweigstellen wären wie Cafés, ohne ein routingfähiges Netzwerk, das sie mit Unternehmensanwendungen in der Cloud verbindet?

Es verbindet User und Geräte mit Anwendungen auf der Grundlage von Richtlinien, nicht von Netzwerkpräsenz, und bietet sowohl robuste Sicherheit als auch eine einfache Bedienung.

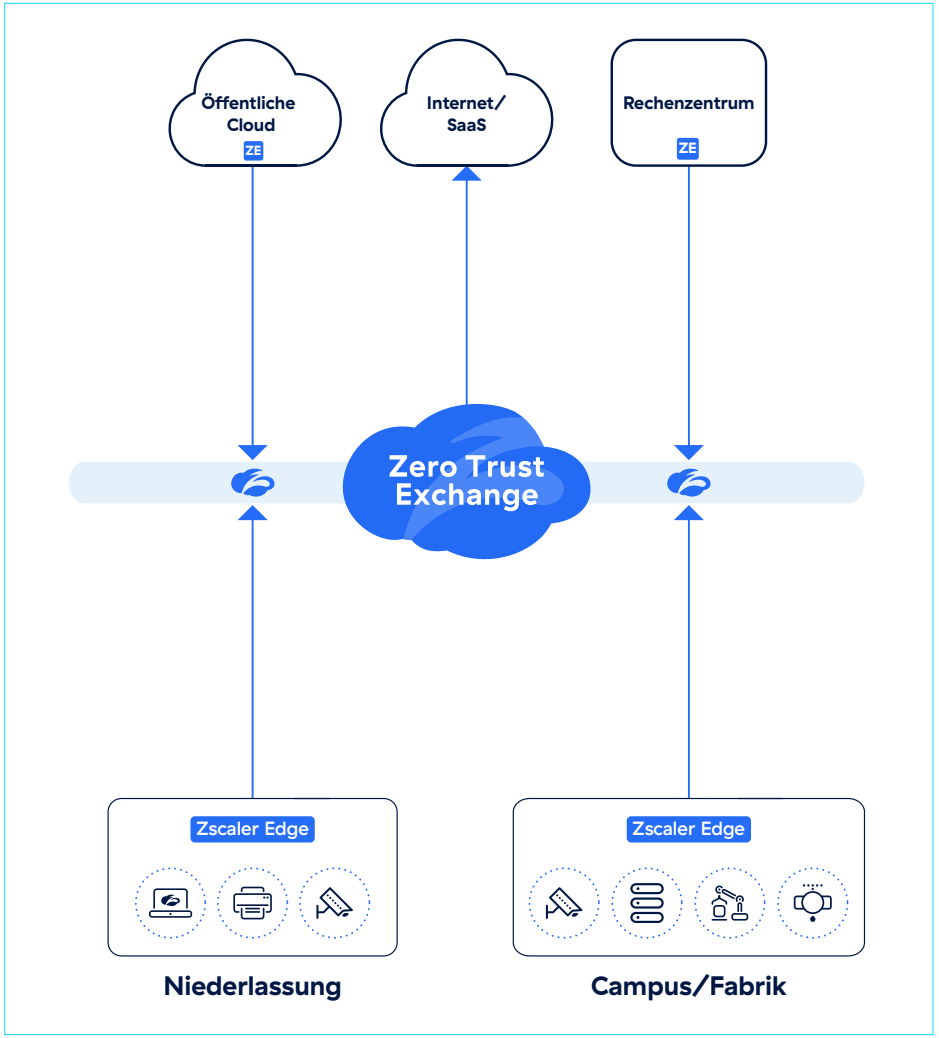
Hierbei handelt es sich um einen nativen Zero-Trust-Ansatz, der laterale Bewegungen unmöglich macht, da User und Geräte — einschließlich IoT- (Internet of Things) und OT-Geräte (Operational Technology) — nie direkt mit Anwendungen verbunden sind. Stattdessen kommunizieren sie über die Plattform Zscaler Zero Trust Exchange™, die einen umfassenden Cyberbedrohungsschutz und Data Protection mit robusten identitäts- und kontextbasierten Zugriffskontrollen gewährleistet.

> „Zero Trust SD-WAN ist eine neue Möglichkeit, Zweigstellen und Rechenzentren schnellen und zuverlässigen Zugriff auf das Internet, private Anwendungen und Cloud-Services zu bieten, ohne das Unternehmensnetzwerk erweitern zu müssen.“

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Die Vorteile dieses Zero-Trust-Ansatzes:

- **Optimierte Anwendungsperformance:**
  Ersetzen Sie komplexe Site-to-Site-VPNs durch eine einfache Direct-to-Cloud-Architektur, die die Anwendungsperformance verbessert und die Produktivität steigert.
- **Minimierte Angriffsfläche im Internet:**
  Bei Legacy-WAN-Lösungen sind VPN-Ports über das öffentliche Internet zugänglich, wodurch Netzwerke angreifbarer sind. Durch Zero Trust SD-WAN wird die Zero Trust Exchange privaten Anwendungen vorgeschaltet, sodass sie nicht im Internet auffindbar und somit auch nicht angreifbar sind.
- **Unterbindung lateraler Bedrohungsbewegungen:**
  Site-to-Site-VPNs erzeugen ein großes routingfähiges Netzwerk, in dem eine Malware-Infektion von einem einzigen Gerät auf alle Entitäten im Netzwerk übertragen werden kann. Mit Zero Trust SD-WAN werden Verbindungen direkt zu Anwendungen hergestellt, nicht zum Netzwerk. Dadurch werden laterale Bewegungen unmöglich.
- **Weniger Kosten und Komplexität:**
  Dieser Ansatz macht mehrere Firewalls, VPNs, NAC und andere mehrschichtige Lösungen überflüssig. Das Ergebnis ist eine Architektur, die einfacher, kostengünstiger und viel leichter zu konfigurieren und zu warten ist.



© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Zscaler löst die Herausforderungen herkömmlicher SD-WANs

Durch die sichere Verbindung von Zweigstellen, Fabriken und Rechenzentren über die Zero Trust Exchange gewährleistet Zscaler einen einheitlichen, konsistenten Zero-Trust-Zugriff für alle User, IoT/OT-Geräte und Anwendungen.

	Zero Trust SD-WAN	Herkömmliches SD-WAN
Minimiert die Angriffsfläche und das Risiko der lateralen Ausbreitung von Bedrohungen	Ja	Nein
Reduziert die Komplexität von Firewall- und ACL-Regeln	Ja	Nein
Bietet sowohl optimale Sicherheit als auch Performance	Ja	Nein
Macht Firewalls in Zweigstellen überflüssig	Ja	Nein

Zscaler Zero Trust SD-WAN ist flexibel genug, um mehrere Bereitstellungsoptionen zu unterstützen, die keinen vollständigen Austausch erfordern. Die Lösung kann mit Ihrer bestehenden SD-WAN-Infrastruktur für Zweigstellen kombiniert werden und Zero-Trust-Overlays für die Zero Trust Exchange erstellen. Dadurch wird ein sicherer und leistungsstarker Zugriff von Ihren Zweigstellengeräten auf private Anwendungen an anderen Standorten und in der Cloud gewährleistet, ohne dass sich Bedrohungen lateral ausbreiten können.

Wenn Sie einen neuen Ansatz für die Konnektivitätsanforderungen Ihres Unternehmens verfolgen, beginnen Sie mit einer nativen Zero-Trust-Architektur, die die Komplexität reduziert und dafür sorgt, dass keine zusätzlichen Firewalls mehr erforderlich sind. Zscaler Zero Trust SD-WAN kann Ihre ISP-Verbindungen verwalten und den Traffic der Anwendungen intelligent steuern, um Ihren Usern eine sichere, caféähnliche Erfahrung in Zweigstellen zu bieten und gleichzeitig Ihr Unternehmen vor Ransomware-Angriffen zu schützen.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Bekämpfung von Ransomware mit Zero Trust

Zero Trust ist entscheidend, um den heutigen Sicherheitsherausforderungen zu begegnen — und das Risiko von Ransomware-Angriffen zu reduzieren. Mit Zscaler Zero Trust SD-WAN kann Ihr Unternehmen die gesamte Kommunikation absichern und laterale Bedrohungsbewegungen unterbinden, ohne die Kosten und die betriebliche Komplexität herkömmlicher Ansätze in Kauf nehmen zu müssen. Darüber hinaus sorgen erstklassige digitale Erfahrungen dafür, dass Kunden, Mitarbeiter und andere Enduser produktiv und problemlos arbeiten können.

zscaler™ | Experience your world, secured.™

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, resilienter und sicherer arbeiten können. Die Zscaler Zero Trust Exchange™ schützt tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen überall vor Cyberangriffen und Datenverlust. Die SASE-basierte Zero Trust Exchange ist weltweit in 150 Rechenzentren verfügbar und ist somit die größte Inline-Cloud-Sicherheitsplattform der Welt. Weitere Informationen finden Sie unter **www.zscaler.com/de**.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ und weitere unter **zscaler.com/de/legal/trademarks** aufgeführte Marken sind entweder (i) eingetragene Marken bzw. Dienstleistungsmarken oder (ii) Marken bzw. Dienstleistungsmarken von Zscaler, Inc. in den USA und/oder anderen Ländern. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.

+1 408 533 0288 Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA

zscaler.com/de