

E-Book

4 Voraussetzungen für eine Zero-Trust-Zweigstelle

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Durch die Einführung eines Zero-Trust-Ansatzes in Zweigstellen können Unternehmen nicht nur ihre Netzwerke vor Bedrohungen schützen, sondern auch die Konnektivität für User, Geräte und Anwendungen an verschiedenen Standorten optimieren.

In der dynamischen Geschäftswelt von heute stehen viele Unternehmen vor der Herausforderung, die Sicherheit ihrer User, Geräte und Anwendungen gewährleisten zu müssen. In der Vergangenheit, als sich Anwendungen noch in Rechenzentren befanden und User in erster Linie vom Büro aus Verbindungen mit dem Netzwerk herstellten, waren die Anforderungen an die Konnektivität relativ unkompliziert. Herkömmliche Hub-and-Spoke- und Firewall-basierte Architekturen konnten diesen Anforderungen gerecht werden. Da sich moderne Arbeitsumgebungen jedoch weiterentwickelt haben, können diese herkömmlichen Ansätze keinen angemessenen Schutz vor Bedrohungen und keine optimale User Experience mehr bieten.

Heutzutage verbinden sich User nicht mehr ausschließlich im Büro, sondern an einer Vielzahl von Orten, wie z. B. zuhause, in Cafés, an Flughäfen und anderen Orten. Die zunehmende Nutzung des Internets der Dinge (IoT) verkompliziert die Sicherheitslandschaft in Unternehmen zusätzlich, da IoT-/OT-Geräte ein weiteres Sicherheitsrisiko darstellen.

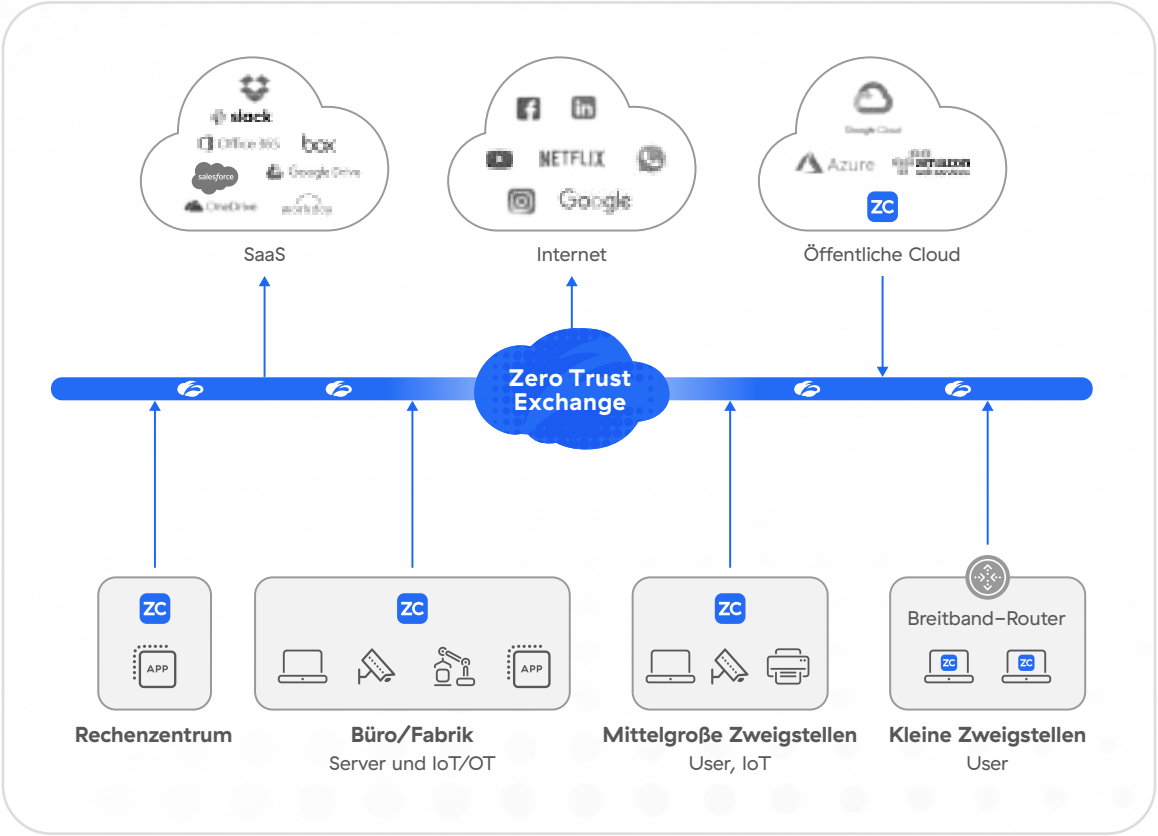


Abbildung 1: Zero Trust Branch bietet einen Zero-Trust-Ansatz für Netzwerkkonnektivität

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Die sich verändernde Landschaft zwingt Unternehmen dazu, einen Zero-Trust-Ansatz für die Sicherheit einzuführen. Mithilfe von Zero-Trust-Prinzipien — keiner Entität vertrauen, alle Verbindungen überprüfen und Zugriff mit minimaler Rechtevergabe durchsetzen — konnten viele Unternehmen ausgeklügelte Cyberangriffe verhindern. Im Gegensatz zu VPNs, die User in das Netzwerk einbinden und ihnen uneingeschränkten Zugriff gewähren, erhalten User bei Zero Trust nur Zugriff auf Anwendungen, die sie tatsächlich benötigen. Durch die Anwendung von Zero-Trust-Prinzipien auf die Netzwerkkonnektivität können sich Unternehmen besser vor Bedrohungen schützen, insbesondere vor solchen, die von den Standorten ausgehen. Die Implementierung eines Zero-Trust-Ansatzes in Zweigstellen sorgt für sichere Konnektivität und vereinfachte Betriebsabläufe. Dabei werden kompliziertes Routing und schlechte User Experiences vermieden, während gleichzeitig die Angriffsfläche minimiert und die laterale Ausbreitung von Bedrohungen unterbunden wird.

Eine Zero-Trust-Architektur in Zweigstellen gewährleistet verbesserte Sicherheit für alle Standorte, einschließlich Zweigstellen, Fabriken, Kioske und Rechenzentren. Im Folgenden finden Sie vier wichtige Voraussetzungen für eine Zero-Trust-Zweigstelle:

Sicherstellung der Zero-Trust-Prinzipien in Ihrem Netzwerk 1

Absicherung von IoT-/OT-Geräten in Ihren Zweigstellen 2

Sicherstellung von Direct-to-Cloud-Pfaden für SaaS-/Internet-Traffic 3

Gewährleistung einer konsistenten User Experience für Mitarbeiter im Büro und Remote-Mitarbeiter 4

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Herkömmliches SD-WAN ist kein Zero Trust

Herkömmliche SD-WAN-Appliances dehnen das Unternehmensnetzwerk einfach auf Remote-Zweigstellen aus und erweitern so die Angriffsfläche des Unternehmens. Sie bieten nur unzureichenden Schutz vor der lateralen Ausbreitung von Bedrohungen und lassen kompromittierte Geräte an Remote-Standorten mit geschäftskritischen Anwendungen im Rechenzentrum oder in der öffentlichen Cloud kommunizieren. Unternehmen sind bei der Verwendung von herkömmlichem SD-WAN einem größeren Risiko durch laterale Bedrohungsbewegungen und internetbasierte Angriffe ausgesetzt. Ein Sammelsurium aus Sicherheitsappliances, -tools und nicht standardisierten Richtlinien führt zu einem erhöhten Sicherheitsrisiko aufgrund bekannter und unbekannter Sicherheitslücken. Daher ist es bei der Planung sicherer Zweigstellenkonnektivität unerlässlich, sich auf die Implementierung von Zero Trust zu konzentrieren, um die Angriffsfläche zu verringern und die laterale Ausbreitung von Bedrohungen zu unterbinden.

Ein 2023 von Cybersecurity Insiders erstellter Report über VPN-Risiken, für den 382 IT-Fachleute und Cybersicherheitsexperten befragt wurden, ergab, dass VPNs Sicherheitsrisiken bergen. 88 % der Unternehmen äußerten leichte bis erhebliche Bedenken, dass VPNs die Sicherheit ihres Unternehmens gefährden könnten.

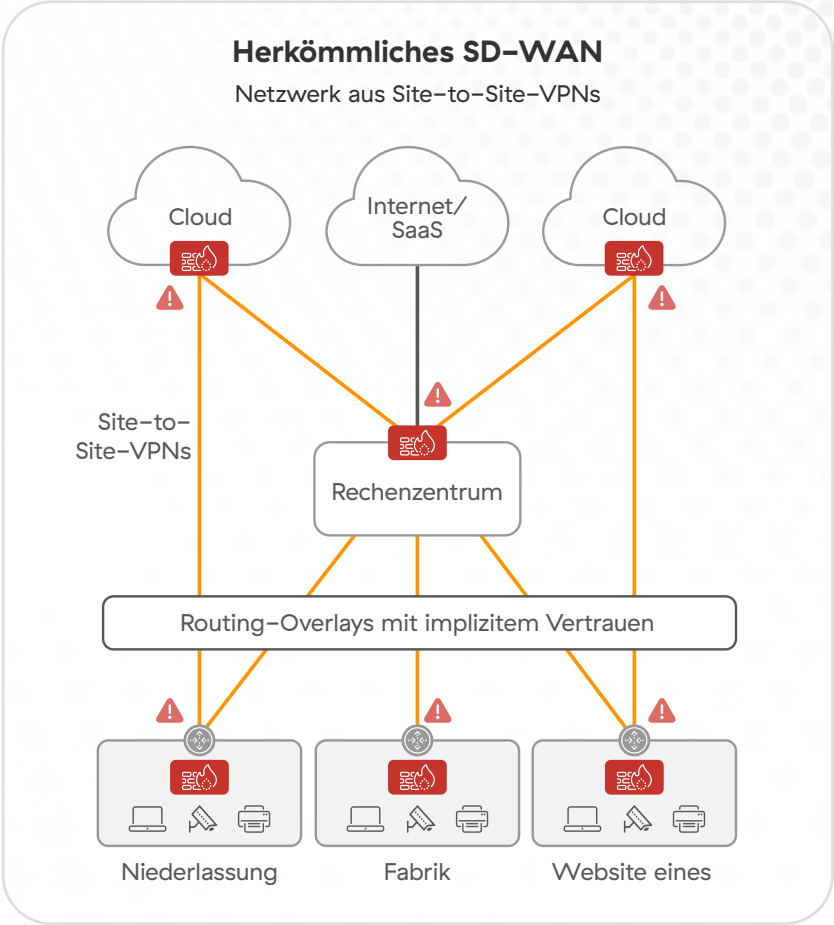


Abbildung 2: Herkömmliche SD-WANs vergrößern die Angriffsfläche und begünstigen die laterale Ausbreitung von Bedrohungen.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.



Darüber hinaus gaben 45 % der Unternehmen an, in den letzten 12 Monaten mindestens einen Angriff erlebt zu haben, bei dem Schwachstellen in VPNs ausgenutzt wurden — jedes dritte Unternehmen wurde Opfer von Ransomware-Angriffen im Zusammenhang mit VPNs. Die zunehmende Bedrohung durch Cyberangriffe, bei denen Schwachstellen in VPNs ausgenutzt werden, unterstreicht die dringende Notwendigkeit, die Sicherheit der aktuellen Architekturen zu verbessern.

War Ihre Organisation in den vergangenen zwölf Monaten von einem Angriff betroffen, bei dem Sicherheitslücken in Ihren VPN-Servern ausgenutzt wurden?

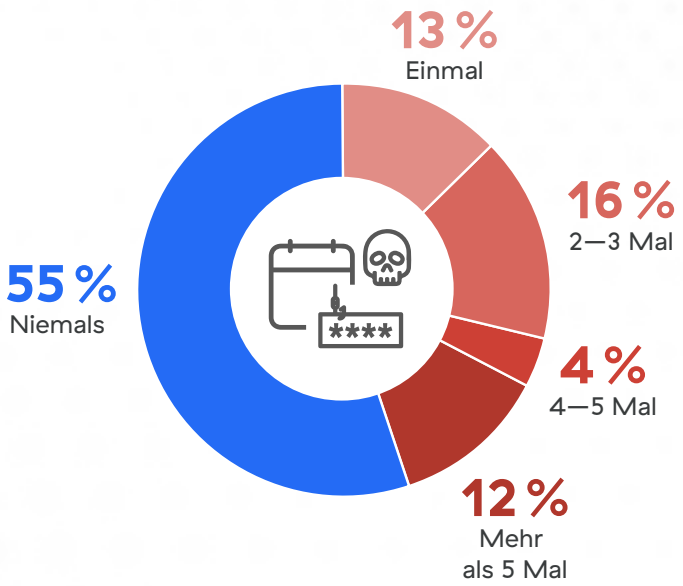


Abbildung 3: Unternehmen sind vermehrt von Cyberangriffen aufgrund von Schwachstellen in VPN-Servern betroffen.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Mit Firewalls und VPNs ist Zero Trust nicht möglich

Bislang setzten Unternehmen Site-to-Site-VPNs ein, um die Konnektivität zu wichtigen, im Rechenzentrum gehosteten Anwendungen sicherzustellen. Wenn diese Anwendungen jedoch in die Cloud migriert werden, wird die herkömmliche Site-to-Site-VPN-Architektur immer weniger praktikabel, da der Traffic immer noch zum Rechenzentrum zurückgeleitet wird, was zu einer verschlechterten User Experience und Performanceproblemen führt.

Außerdem erhöht sich die betriebliche Komplexität, da für VPN-Tunnel eine individuelle Standortverwaltung und -einrichtung erforderlich ist. Daher möchten IT-Teams in Unternehmen von einem Hub-and-Spoke-Netzwerk zu einer Direct-to-Cloud-Architektur wechseln, die den Anwendungstraffic an einen Cloud-Sicherheitsanbieter sendet und so die Anwendungsperformance verbessert.

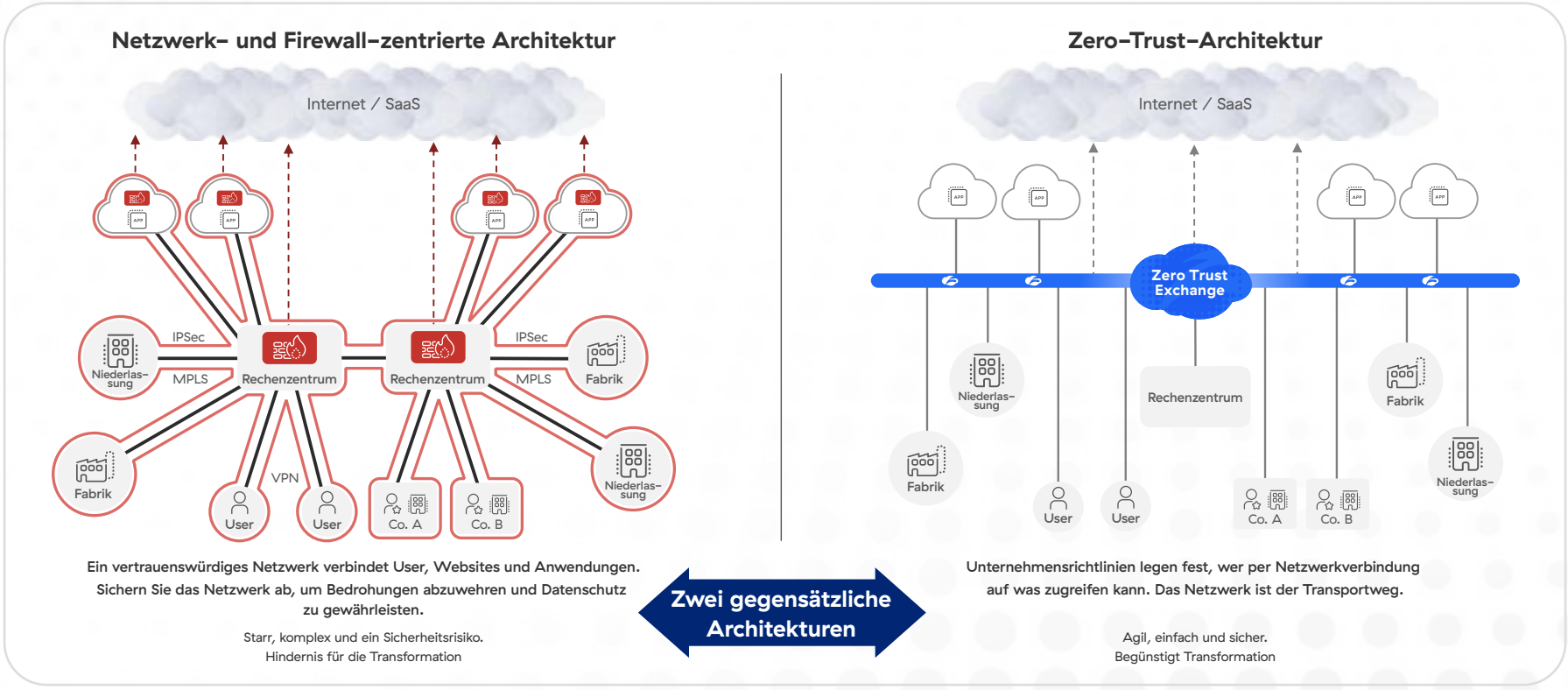


Abbildung 4: Hub-and-Spoke-Netzwerke verfügen über eine komplexe und starre Architektur. Im Gegensatz dazu ist eine Zero-Trust-Architektur agil, einfach und sicher und begünstigt eine Transformation.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Vier Voraussetzungen für eine Zero-Trust-Zweigstelle

1 Sicherstellung der Zero-Trust-Prinzipien in Ihrem Netzwerk

Site-to-Site-VPNs erweitern Ihr Unternehmensnetzwerk auf Zweigstellen, Rechenzentren, Cloud-Regionen und externe User. Herkömmliche Netzwerke dehnen Ihre Angriffsfläche auf Entitäten aus, die sich Ihrer direkten Kontrolle entziehen, und lassen den Traffic ungehindert fließen, was die laterale Ausbreitung von Bedrohungen begünstigt. Im Gegensatz zur herkömmlichen Netzwerksegmentierung, bei der das Netzwerk in Zonen aufgeteilt wird und deren Verwaltung komplex ist, bietet die User-to-App- und Device-to-App-Segmentierung granularen, kontextbezogenen Zugriff — und zwar nur dann, wenn er autorisiert ist. Eine Netzwerkgrundlage, die auf Zero-Trust-Prinzipien basiert, beseitigt die inhärenten Risiken in herkömmlichen flachen Netzwerken und hilft Ihnen, die Komplexität von Firewalls zu reduzieren, die für Probleme mit Sicherheitskontrollen, Anwendererfahrung und Performance verantwortlich sind. Außerdem erhöht sich die betriebliche Komplexität, da für VPN-Tunnel eine individuelle Standortverwaltung und -einrichtung erforderlich ist.

2 Absicherung von IoT-/OT-Geräten in Ihren Zweigstellen

IoT-/OT-Geräte werden mit der zunehmenden Nutzung von „intelligenten“ Geräten wie Druckern, Fernsehern, Kameras, Kartenlesern und Sensoren in nahezu jedem Unternehmen eingesetzt. Auf diesen Geräten läuft eine Vielzahl von Betriebssystemen mit unterschiedlichen Sicherheitsrisiken, und die Patch-Verwaltung bleibt eine Herausforderung. Viele IT-Verantwortliche haben keinen Einblick in diese Geräte, geschweige denn ein detailliertes Inventar. Dennoch haben diese Geräte oft uneingeschränkten Zugriff auf die wichtigsten Anwendungen in Ihren Rechenzentren und Cloud Services. Da die Zahl der Angriffe durch IoT-Malware um 400 %[1] gestiegen ist, stellt dies eine erhebliche Bedrohung für Ihr Unternehmen dar. Unternehmen müssen IoT/OT-Geräte in Zweigstellen oder Fabriken absichern, um ihre Geschäftsabläufe zu schützen.

IoT- und OT-basierte Malware-Angriffe haben seit 2022 um 400 % zugenommen und stellen somit einen bedeutenden Bedrohungsvektor dar.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

3 Sicherstellung von Direct-to-Cloud-Pfaden für SaaS-/Internet-Traffic

Die Direct-to-Cloud-Architektur verbindet jeden User oder jedes IoT-/OT-Gerät schnell mit jeder Anwendung, egal wo auf der Welt sich der User oder das IoT-/OT-Gerät befindet. Die Implementierung von Direct-to-Cloud-Pfaden für SaaS- und Internet-Traffic ist entscheidend für die Optimierung der Netzwerkperformance und die Gewährleistung nahtloser Konnektivität. Hub-and-Spoke-Architekturen, die den Traffic über teure MPLS-Verbindungen an ein Rechenzentrum weiterleiten, verschlechtern die Anwendungsperformance und behindern die Unternehmensproduktivität. Als sich Anwendungen noch im Rechenzentrum befanden, war es sinnvoll, den Anwendungstraffic zu einem regionalen Hub zu leiten. Wenn Anwendungen jedoch in die Cloud verschoben werden, ist es am sinnvollsten, den Traffic von Usern oder IoT-/OT-Geräten direkt an das Ziel zu senden. Mit einer Direct-to-Cloud-Architektur können SaaS-Anwendungen und Internet-Traffic den effizientesten und direktesten Weg zu ihren Zielen nehmen. Dies hat viele Vorteile, darunter Kosteneinsparungen, eine verbesserte User Experience und eine Vereinfachung des Netzwerks.

Heutzutage wünschen sich Führungskräfte eine Café-ähnliche Erfahrung für ihre User und IT-Teams, die den Zugriff auf Geschäftsanwendungen so einfach wie möglich macht und gleichzeitig eine hervorragende Anwendungsperformance bietet.

4 Gewährleistung einer konsistenten User Experience für Mitarbeiter im Büro und Remote-Mitarbeiter

Viele Mitarbeiter arbeiten remote oder sind teilweise im Homeoffice und im Büro tätig. Diese neuen Arbeitsmodelle haben eine große Herausforderung mit sich gebracht. User sind nämlich häufig unzufrieden mit der Qualität der Konnektivität im Büro im Vergleich zu ihrer Arbeitsumgebung zu Hause. Diese Situation stellt IT-Teams vor eine Reihe neuer Probleme. VPN-Technologien, die den Traffic an ein Rechenzentrum zurückleiten, führen zu einer schlechten und inkonsistenten User Experience, was sich negativ auf den Geschäftsbetrieb auswirkt und die Produktivität verringert.

Heutzutage wünschen sich Führungskräfte eine Café-ähnliche Erfahrung für ihre User und IT-Teams, die den Zugriff auf Geschäftsanwendungen so einfach wie möglich macht und gleichzeitig eine hervorragende Anwendungsperformance bietet. Sie möchten, dass ihre User zu Hause und im Büro gleichermaßen unkompliziert auf die benötigten Anwendungen zugreifen können, was bei der Verbindung mit Netzwerken über VPNs unmöglich ist. Um in der heutigen wettbewerbsorientierten Welt konkurrenzfähig zu bleiben, müssen Unternehmen eine konsistente User Experience für Mitarbeiter im Büro und an Remote-Standorten gewährleisten, um die Produktivität der Belegschaft zu steigern und ihre Kreativität zu fördern.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Anwendung von Zero-Trust-Prinzipien auf SASE

Secure Access Service Edge (SASE) integriert Netzwerk- und Sicherheitsservices in eine einheitliche, in der Cloud bereitgestellte Lösung, die den Betrieb optimiert, die Komplexität reduziert und es Unternehmen ermöglicht, einheitliche Richtlinien in ihren Netzwerken durchzusetzen. SASE kombiniert Zero-Trust-Networking mit grundlegenden, in der Cloud bereitgestellten Sicherheitsservices wie SWG, CASB, FWaaS und ZTNA. SASE-Lösungen, die auf herkömmlichem SD-WAN aufbauen, bieten nur unzureichenden Schutz, vergrößern die Angriffsfläche des Unternehmens und setzen kritische Anwendungen verschiedenen Internetbedrohungen aus.

Darüber hinaus sind die Segmentierungsfunktionen in herkömmlichen SD-WANs fragmentiert und ungenau, sodass sich Bedrohungen leicht auf andere Systeme ausbreiten können und das Risiko besteht, dass ganze Standorte oder Netzwerke ausfallen.

Die Enterprise Strategy Group (ESG) von TechTarget befragte 390 IT- und Cybersicherheitsexperten in verschiedenen Unternehmen in Nordamerika (USA und Kanada), um den aktuellen Stand von SASE zu ermitteln. Laut dieser Studie sind die drei wichtigsten Anwendungsfälle, die Unternehmen zur Nutzung von SASE bewegen, folgende:

1. Angleichen von Netzwerk- und Sicherheitsrichtlinien
2. Reduzierung oder Beseitigung der Angriffsfläche im Internet
3. Verbesserung der Sicherheit von Remote-Usern

Alle drei SASE-Anwendungsfälle unterstreichen die Bedeutung der Bereitstellung sicherer Konnektivität für User, Geräte und Anwendungen bei der Einrichtung eines resilienten SASE-Frameworks. Unternehmen, die mit der Implementierung von SASE beginnen, müssen Lösungen priorisieren, die den Grundsätzen von Zero Trust entsprechen. Herkömmliche SD-Wans verbinden verschiedene Standorte über Site-to-Site-VPNs oder Routing-Overlays und etablieren so implizites Vertrauen, das selbst kompromittierten Entitäten uneingeschränkten Zugriff auf wichtige Geschäftsressourcen gewährt. SD-WANs, die auf Zero-Trust-Prinzipien basieren, reduzieren hingegen die Angriffsfläche und schützen vor der lateralen Ausbreitung von Bedrohungen, während sie sichere User-to-App-, Device-to-App- und App-to-App-Kommunikation ermöglichen.



Abbildung 5: Erkenntnisse der ESG-Umfrage hinsichtlich aktueller oder voraussichtlicher SASE-Anwendungsfälle.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Fazit

Herkömmliche Netzwerkarchitekturen in Zweigstellen beruhen auf implizitem Vertrauen, wodurch sich die Angriffsfläche auf die am weitesten entfernte Zweigstelle ausdehnt und Cyberbedrohungen sich lateral durch das Unternehmen bewegen können. Durch die Einführung eines Zero-Trust-Ansatzes in Zweigstellen können Unternehmen nicht nur ihre Netzwerke vor Bedrohungen schützen, sondern auch die Konnektivität für User, IoT-/OT-Geräte und Anwendungen an verschiedenen Standorten optimieren. Die Planung eines Zweigstellennetzes nach den Grundsätzen von Zero Trust verbessert den Sicherheitsstatus des Unternehmens, indem die Angriffsfläche beseitigt und die laterale Ausbreitung von Bedrohungen unterbunden wird, während zudem komplexes Routing entfällt. Es ist wichtig, dass Unternehmen bei der Implementierung von Zero-Trust-Prinzipien in Zweigstellen die vier hier beschriebenen Voraussetzungen genau berücksichtigen, um die komplexen und sich ständig ändernden Anforderungen an Sicherheit und Netzwerkkonnektivität effektiv zu bewältigen.

Quellenangaben:

1. zscaler.de/press/zscaler-threatlabz-finds-400-increase-iot-and-ot-malware-attacks-year-over-year-underscoring
2. info.zscaler.com/2023-vpn-risk-report-de
3. zscaler.de/resources/industry-reports/esg-sse-leads-the-way-to-sase.pdf

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.



Experience your world, secured.™

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Die Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust. Die SASE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Weitere Informationen finden Sie auf **zscaler.de** oder auf Twitter unter **@zscaler**.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™, Zscaler Digital Experience, ZDX™ und weitere unter **zscaler.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.de