zscaler™

E-Book

Zero Trust: 7 Anzeichen, warum Firewalls der Vergangenheit angehören

und 7 Lösungen, die eine echte Alternative darstellen

Zero Trust ist für heutige Unternehmen unverzichtbar

Die Einsicht, dass Zero Trust das richtige Sicherheitskonzept für zukunftsfähige digitale Unternehmen ist, hat sich unter Cybersicherheitsexperten längst durchgesetzt. Umfragen zufolge ist die Umstellung auf Zero Trust Network Access bei 78 % der Unternehmen entweder bereits vollzogen oder in Planung.[1] IT-Verantwortliche wissen, dass ein effektiver Schutz einen Paradigmenwechsel erfordert. Datenorientierte Organisationen mit dezentralen Arbeitskonzepten müssen weg vom herkömmlichen Modell der Netzwerksicherheit und hin zur Absicherung von Usern, Daten und Anwendungen.

Vor Jahrzehnten, als Hub-and-Spoke-Netzwerke den neuesten Stand der Technik darstellten, waren Firewalls und die entsprechenden Netzwerkarchitekturen darauf ausgelegt, die damaligen Anforderungen vollkommen zu erfüllen. Im heutigen Zeitalter des Cloud-Computing hingegen reichen diese Anforderunge nicht mehr aus. Firewalls sind schlichtweg überfordert. Das herkömmliche "Castle-and-Moat"-Architekturmodell, bei dem jeder innerhalb des Netzwerks standardmäßig vertrauenswürdig ist, ist grundlegend nicht mit einem zeitgemäßen Zero Trust Sicherheitsmodell kompatibel.

Dieser Leitfaden nennt sieben Anzeichen, an denen man auf den ersten Blick erkennen kann, warum eine Firewall den Anforderungen einer Zero Trust Sicherheit nicht gewachsen ist. Jeder der hier aufgeführten Anzeichen macht deutlich, warum der Wechsel zu einem Zero Trust Sicherheitskonzept unvermeidbar ist und welche alternativen Lösungen es für Unternehmen gibt.

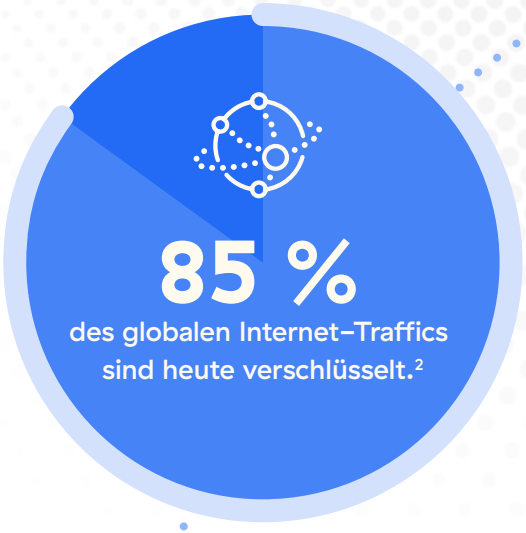
1. Quelle: Cybersecurity Insiders, Zero Trust Adoption Report, 2019.

ANZEICHEN NR. 1

Dramatischer Abfall der Netzwerkleistung

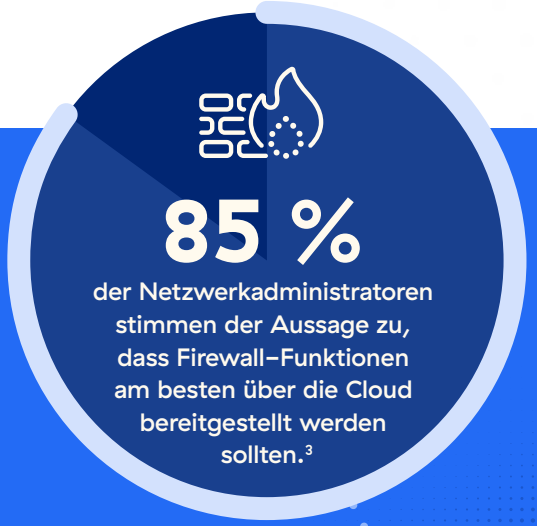
Unabhängig von ihrer Größe und technischen Auslegung sind Hardware-basierte Firewalls nicht in der Lage, hohe Volumen von SSL-verschlüsseltem Traffic zu überprüfen. Dieses Manko erweist sich durch den wachsenden Anteil SSL-verschlüsselter Daten am globalen Internet-Traffic als echtes Problem. Denn Angreifer machen es sich zunutze und schleusen komplexe Bedrohungen im verschlüsselten Traffic in die IT-Umgebungen von Organisationen ein.

Ein Leistungsabfall um >50 % beim Versuch, die SSL-Überprüfung zu aktivieren, ist als sicheres Anzeichen dafür zu werten, dass die Firewall mit dieser Fülle an Überprüfungen offensichtlich überfordert ist. Um eine Performance zu gewährleisten, die den Ansprüchen der User entspricht, ist entweder ein Upgrade auf eine Firewall mit höherer Kapazität oder die Implementierung zusätzlicher Appliances (bzw. virtueller Firewall-Instanzen) erforderlich.



LÖSUNG

Die Umstellung auf einen Cloud-basierten Service, der Cloud-native Firewall-Funktionen bereitstellt, ist eine weitaus wirksamere Alternative zur o.g. Skalierung von virtuellen Versionen veralteter physischer Appliances. Denn nur Cloud-basierte Services und Lösungen bieten die flexible Skalierbarkeit, die unter heutigen Vorzeichen zur Überprüfung des gesamten Traffics erforderlich ist — auch bei SSL-Verschlüsselung.



2. Quelle: Agentur der Europäischen Union für Cybersicherheit, Analyse des verschlüsselten Traffics
3. Quelle: Zscaler, Umfrage zu Netzwerk-Firewalls

ANZEICHEN NR. 2

Wer einmal drin ist, kann alles sehen. Und alles infizieren

Firewalls wurden als Aussenschutz für herkömmliche Netzwerke entwickelt, die auf dem "Castle-and Moat-Konzept" beruhten. Sie bewachten quasi die Zugbrücke und entschieden darüber, welchem Traffic Zutritt ins Netzwerk gewährt wurde. Der gesamte Traffic innerhalb des Netzwerks wurde somit automatisch als vertrauenswürdig eingestuft. Voraussetzung für das Funktionieren dieses Konzepts war, dass sich die Mehrzahl der User im Büro, die Mehrzahl der Infrastruktur an Unternehmensstandorten und die Mehrzahl der Anwendungen im Rechenzentrum befand. Heute trifft keine dieser Bedingungen mehr zu, denn mittlerweile fließen 70 % des Traffics netzwerkintern zwischen Servern und Anwendungen innerhalb der privaten Cloud-Umgebung oder des Rechenzentrums. Firewalls bieten so gut wie keine Möglichkeiten, diesen Traffic zu überprüfen oder zu blockieren. Angreifer, denen es gelingt, sich Zugang zum Netzwerk zu verschaffen, haben freien Zugriff auf sämtliche Ressourcen.

Ist der Angreifer erstmal drin, wird die Entdeckung der einzelnen vernetzten Assets einfach. Mithilfe eines Open-Source-Scanners kann ein unbefugter User problemlos sämtliche IP-Adressen innerhalb des Netzwerks ausfindig machen. Die Auslieferung von Ransomware bzw. Exfiltration wertvoller Daten stellt ebenfalls keine große Herausforderung dar — und lässt sich mit einer Firewall nicht verhindern.

64 %

der Netzwerkadministratoren meinen, dass Firewalls laterale Bewegungen nicht effektiv verhindern können.[4]

57 %

der Entscheidungsträger im IT-Bereich sind überzeugt, dass Firewalls nicht zur Abwehr von Ransomware-Angriffen geeignet sind.[4]

LÖSUNG

- Zero Trust Network Access verfolgt ein anderes Konzept, weil Verbindungen erst nach Verifizierung der Identitäten sowie des Sicherheitsstatus der betreffenden User und Geräte zugelassen werden. Sicherheitsrichtlinien werden für jede einzelne Verbindung konsequent durchgesetzt. Statt ungeschützter Verbindungen zu einem Netzwerk lassen sich auf diese Weise sichere Direktverbindungen zwischen Usern und Anwendungen herstellen.

4. Quelle: Zscaler, Umfrage zu Netzwerk-Firewalls

ANZEICHEN NR. 3

Zu viele Richtlinien, die sich nicht mehr verwalten lassen

Sicherheitsteams versuchen, Legacy-Architekturen auf ein Zero Trust Konzept umzustellen, indem Richtlinien zur Segmentierung des Netzwerk in immer kleinere Einzelteile konfiguriert werden. Theoretisch handelt es sich dabei um Mikrosegmentierung. In der Praxis wird der damit verbundene Verwaltungsaufwand allerdings untragbar.

Zum Schutz von Anwendungen in heutigen IT-Umgebungen wird eine ständig zunehmende Anzahl virtueller Firewalls im gesamten Netzwerk eingesetzt. Das Ergebnis ist ein Wust von Richtlinien, die laufend neu konfiguriert werden müssen, damit sie annähernd einem Zero Trust Modell ähneln.

Virtuelle Firewalls leiden an dem gleichen Problem wie ihre physischen Vorgänger: Sie lassen sich nur begrenzt skalieren. Letztendlich werden zum Schutz einer Unternehmensumgebung Tausende oder gar Zehntausende von Richtlinien benötigt, deren Verwaltung eine massive Belastung für die IT darstellt.

LÖSUNG

Als optimale Lösung hat sich die Trennung zwischen Netzwerkzugang und Anwendungszugriff bewährt. Mit Zero Trust Network Access kann einzelnen Usern sicherer Direktzugriff auf Anwendungen gewährt werden, ohne dass sie Zugang zu Netzwerksegmenten — geschweige denn zum Netzwerk selbst — erhalten. Konkret heißt das, dass User unmittelbar mit den jeweils benötigten Anwendungen verbunden werden und der gesamte Traffic auf dem kürzestmöglichen Verbindungspfad weitergeleitet wird. Administratoren und Sicherheitsbeauftragte werden ebenfalls entlastet, da sie sich nicht mehr um die Verwaltung der zugrundeliegenden Infrastruktur kümmern müssen.

Zugegeben, die Bereitstellung ist mit einem gewissen Zeitaufwand verbunden. Der wird jedoch durch die radikal reduzierte Komplexität bei optimierter Anwendererfahrung für die Enduser mehr als aufgewogen.

ANZEICHEN NR. 4

Virtuelle Firewalls, die öffentliche Cloud-Umgebungen gefährden

Im Online-Softwarehandel werden virtuelle Firewalls gängiger Cloud-Anbieter mit entsprechender Zertifizierung zum Nachweis ihrer vermeintlichen Praxistauglichkeit angeboten. Hier ist jedoch Vorsicht geboten: In vielen Fällen handelt es sich lediglich um virtuelle Versionen Appliance-basierter Firewalls, die als VM-Instanzen in öffentlichen Cloud-Umgebungen ausgeführt werden.

Im Grunde sind diese virtuellen Firewalls nichts anderes als eine externe Erweiterung der Legacy-Netzwerkarchitektur auf Cloud-basierte IT-Ressourcen. Dadurch erhalten sämtliche User innerhalb des Netzwerks Zugriff auf die Cloud-basierten Assets einer Organisation. Das Problem bleibt also unverändert, denn auch Angreifer, denen es gelingt, die Firewall-basierten Schutzmechanismen zu überwinden, können sich innerhalb dieses erweiterten Netzwerks frei bewegen.

Die Konfiguration von Richtlinien für den Traffic zwischen Workloads in öffentlichen Cloud-Umgebungen und virtuellen Private Clouds ist zudem äußerst umständlich und unübersichtlich. Jeder einzelne Eintritts- und Austrittspunkt in der Cloud-Architektur muss durch eine virtuelle Firewall geschützt werden. Angesichts der inhärenten Interkonnektivität von Cloud-Umgebungen leuchtet sofort ein, warum dieses Modell alles andere als eine elegante oder auch nur praktikable Lösung darstellt.

Erschwerend kommt hinzu, dass eine komplizierte Routing- und Netzwerkarchitektur verwaltet werden muss, nur um die reibungslose Anbindung dieser Cloud-Architektur an das Legacy-Netzwerk zu gewährleisten.

Firewalls eignen sich nicht zum Blockieren lateraler Bewegungen.

LÖSUNG

- Zukunftsfähige Plattformen können Direktverbindungen zwischen Workloads in beliebigen Umgebungen vermitteln. Dadurch lässt sich verhindern, dass Angreifer von aussen auf Netzwerkressourcen zugreifen. Zugleich wird der Aufwand für die Verwaltung und Fehlerbehebung reduziert. Administratoren haben damit eine granulare, bedingte Zugriffskontrolle, die jederzeit widerrufen werden kann, wenn sich der Kontext ändert.

ANZEICHEN NR. 5

Mehr Agilität, mehr Freiheit — aber auch mehr Risiko

Die Cloud-Transformation bringt einschneidende Veränderungen im Wirtschaftsleben mit sich. Branchenübergreifend nehmen Organisationen die Umstellung auf Cloud-basierte Modelle als Chance für mehr Agilität und Innovationsfreiheit wahr. Eine Freiheit, die für IT- und Sicherheitsexperten jedoch auch mit erheblichen Belastungen und Herausforderungen verbunden ist.

Denn sie sind es, die Firewall-basierte Altsystem-Architekturen entsprechend neu konfigurieren müssen, um einen zuverlässigen Schutz für Ressourcen in der Cloud zu gewährleisten. Im Dickicht der ausufernden Richtlinien fällt es oft schwer, den Überblick zu behalten — und die Anwender erwarten weiterhin reibungslosen Zugriff auf die Anwendungen, die sie zur Erledigung ihrer Arbeit benötigen.

Vor diesem Hintergrund überrascht es kaum, wenn 90 % der IT- und Sicherheitsexperten zugeben, sie hätten zumindest vorübergehend sehr großzügige Richtlinien[5] angewendet, um Projekte schneller abzuwickeln und Usern alle erforderlichen Zugriffsberechtigungen zu gewähren. Das ist gefährlich, denn je mehr sich die zeitweise Nachlässigkeit zu einem permanenten Risikoverhalten wird, desto mehr steigt die Gefahr, dass die Organisation Opfer einer Datenpanne oder eines verheerenden Cyber-Angriffs wird. Solche Nachlässigkeiten stehen in direktem Widerspruch zu einem Zero Trust Ansatz mit minimaler Rechtevergabe.

85 %
aller Organisationen planen bis 2025 die Umstellung auf eine „Cloud first"-Strategie.[5]

95 %
aller neuen digitalen Workloads werden heute auf Cloud-nativen Plattformen bereitgestellt.[5]

LÖSUNG

Eine Cloud-basierte Zero Trust Lösung sorgt dafür, dass Anwender die Chancen und Innovationen einer Cloud-Transformation nutzen können — ohne, dass die IT-Abteilung hohen Aufwand betreiben muss. Denn eine zentrale Zero Trust Plattform mit einer einzigen Verwaltungskonsole lässt sich nicht nur viel schneller konfigurieren und einfacher verwalten als herkömmliche Perimeter-Firewalls, sondern überzeugt auch durch ein höheres Sicherheitsniveau.

5. Quelle: Gartner, „Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences"

ANZEICHEN NR. 6

Was man sieht, kann man auch angreifen

Perimeter-Firewalls wurden als Netzwerk-Frontends konzipiert. Sie sind von außen im Internet erkennbar und ermöglichen direkten Zugriff auf interne Netzwerke und Ressourcen, wenn es einem Angreifer oder sonstigem unbefugten User gelingt, sie zu überwinden. Organisationen, die eine herkömmliche Firewall als Gateway für die Bereitstellung von VPN-Services nutzen, gefährden dadurch die Sicherheit ihres Netzwerks.

Wie gravierend diese Risiken sind, zeigte sich zuletzt an einer Reihe erfolgreicher Angriffe auf prominente Ziele, bei denen Sicherheitslücken in Legacy-VPNs ausgenutzt wurden. So auch beim bisher schwersten öffentlich gemeldeten Cyberangriff auf systemrelevante Infrastruktur in den USA: Das VPN, über das der Ransomware-Angriff auf die Colonial Pipeline verübt wurde, hätte laut dem CEO des Unternehmens „eigentlich nicht mehr in Betrieb sein dürfen“.[6]

Firewall-basierte VPNs ermöglichen weder die Implementierung granularer Zugriffskontrollen, noch haben Administratoren die Option festzulegen, welche Anwender auf welchen Ressourcen Zugriff haben dürfen. Organisationen, die sich auf VPNs verlassen, um Usern Remotezugriff auf unternehmenseigene Anwendungen zu gewähren, erweitern damit die externe Angriffsfläche ihres Netzwerks. Von der Cloud bis zu den privaten WLAN-Routern und -Netzwerken der Mitarbeiter — alles ist gefährdet. Je größer das Netzwerk, desto größer der Schaden, den Angreifer innerhalb kürzester Zeit anrichten können.

Firewall-basierte VPNs ermöglichen weder granulare Zugriffskontrollen noch Optionen zur Festlegung, welche User mit bestimmten Ressourcen verbunden werden dürfen.

LÖSUNG

Als wirksamere Alternative zu VPNs sollten Lösungen eingesetzt werden, die sicheren Zugriff auf Anwendungen durch Direktverbindungen zwischen einzelnen Usern und einzelnen Anwendungen unter Berücksichtigung dynamischer Identitäts- und Kontextdaten ermöglichen. Da diese Lösungen nur ausgehende Verbindungen zulassen, sind Anwendungen nicht im öffentlichen Internet sichtbar. Durch ihren Einsatz lässt sich sowohl der Sicherheitsstatus der Organisation als auch die Performance ihrer Anwendungen drastisch verbessern.

6. Quelle: „Colonial Pipeline hack explained: Everything you need to know“, TechTarget, April 2022.

ANZEICHEN NR. 7

Das Netzwerk wird zum Flaschenhals

Dezentrale Unternehmensstrukturen sind in manchen Branchen eher die Regel als die Ausnahme. Home Office hat sich mittlerweile überall durchgesetzt. Der Versuch, die wachsende Anzahl der Remote-User über eine Legacy-Netzwerkarchitektur mit geschäftskritischen Anwendungen zu verbinden, geht zu Lasten der Performance. Warum? Weil dass hohe Trafficvolumen zwecks Überprüfung durch die Firewall zuerst ins unternehmenseigene Rechenzentrum umgeleitet werden muss.

Dieses als Backhauling bezeichnete Verfahren ist so umständlich wie unsinnig. Legacy-Firewalls und Appliance-basierte Security-Stacks sind mit einem hohen Verwaltungsaufwand verbunden. Organisationen, die mit gemieteten Standleitungen arbeiten, zahlen erhebliche Summen für eine Infrastruktur mit komplexen Routing-, Switching- und Traffic-Segmentierungsoptionen. Aus dieser Erfahrung rührt das steigende Interesse an SD-WAN (Software-Defined Wide Area Networking). Das Grundproblem der hohen Kosten und Komplexität, die mit der Verwaltung von Firewalls verbunden sind, wird durch den Einsatz von überlagernden Netzwerken jedoch keineswegs gelöst, sondern eher verschärft.

Die Umleitung des Netzwerkverkehrs senkt die Performance und beeinträchtigt die User Experience. Außerdem entstehen Latenzen — ein ständiges Problem, das sich mit der zunehmenden Nutzung von Kommunikationsanwendungen mit hohem Bandbreitenverbrauch wie Zoom, Microsoft Teams u.a. nur noch verschlimmern wird.

LÖSUNG

- Eine Cloud-basierte Zero Trust Lösung stellt Sicherheitskontrollen dort bereit, wo sich User und Anwendungen heute befinden: in der Cloud. Richtlinien werden inline und an der Edge durchgesetzt, sodass der Traffic nicht unnötig um- bzw. weitergeleitet werden muss. Als Inline-Lösung, die im Datenpfad arbeitet, kann eine Zero Trust Plattform zudem sämtliche Verbindungen überwachen und Performance-Probleme automatisch erkennen und beheben.

ZERO TRUST IST DAS ULTIMATIVE SICHERHEITSKONZEPT

Zscaler bietet eine zuverlässige und sichere Option für anfällige Netzwerke

Die Zscaler Zero Trust Exchange™ ist eine Cloud-native Plattform, die eigens für Zero Trust Architekturen entwickelt wurde. Die Zero Trust Exchange ermöglicht direkte und sichere Verbindungen gemäß dem Prinzip der minimalen Rechtevergabe. Bevor eine Verbindung zustande kommt, werden Inhalte gründlich überprüft und Zugriffsrechte anhand von Identität und Kontextdaten verifiziert.

Die KI/ML-gestützte Policy-Engine von Zscaler basiert auf der weltweit größten Security Cloud. Sie berücksichtigt Kontextdaten zu User, Gerät und Anwendung und entscheidet anhand dieser Informationen, ob und in welchem Umfang dem jeweiligen Anwender Zugriff auf die jeweilige Anwendung gewährt wird. So werden User und Daten zuverlässig geschützt. Durch Vermittlung von Direktverbindungen zwischen einzelnen Usern und einzelnen Anwendungen gewährleistet die Zero Trust Exchange zudem, dass Anwendungen im Internet unsichtbar bleiben, und verkleinert dadurch die Angriffsfläche.

Mit diesem Ansatz stellt Zscaler unkomplizierte Zero Trust Sicherheit für Organisationen aller Größen und Branchen bereit. Branchenführer und Fachanalysten sind sich einig: Die Zero Trust Exchange von Zscaler ist die ausgereifteste und benutzerfreundlichste Zero Trust Plattform.

Die Zscaler Zero Trust Exchange lässt sich zügig und unkompliziert bereitstellen. Organisationen profitieren damit von einem breiten Spektrum integrierter Inline-Sicherheitstools zur Verstärkung der marktführenden SSE-Funktionen (Security Service Edge). Insbesondere werden folgende Tools bereitgestellt:

- **Cloud-Generation Firewall**
- **Erweiterte Cloud Sandbox**
- **Secure Web Gateway (SWG)**
- **Data Loss Prevention (DLP)**
- **CASB**
- **und weitere Funktionen**

Weitere Informationen unter:
www.zscaler.de/products/zscaler-internet-access

zscaler™ | **Experience your world, secured.™**

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

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