zscaler™

White Paper

Die 5 wichtigsten Herausforderungen für Netzwerksicherheit

und wie sich diese mit **Zero Trust** erfolgreich bewältigen lassen

In den letzten Jahrzehnten wurden vor allem Remote User, Zweigstellen und andere externe Standorte mit Hub-and-Spoke Netzwerken ans Unternehmensnetzwerk angebunden. Diese Konstrukte waren ausschließlich auf ein zentralisiertes Rechenzentrum mit den dort befindlichen Sicherheitsfunktionen ausgerichtet. Da sich sämtliche Teilnehmer im Netzwerk befanden, war die Hauptaufgabe der IT-Sicherheit, mit Firewalls eine solide Barriere zwischen dem vertrauenswürdigen Netzwerk und der Außenwelt (d. h. dem Internet) zu schaffen. Dieser Ansatz mit Perimetern und Firewalls prägte den Begriff des Castle-and-Moat-Prinzips. Durch die enorm gestiegene Verbreitung von Remote Arbeit und immer mehr Cloud basierten Anwendungen ist dieses rein lokal ausgelegte Modell jedoch überholt.

Für Organisationen wird es immer schwieriger, ihre hybriden Belegschaften und Cloud basierten Anwendungen mit den alten Netzwerksicherheitsarchitekturen zu schützen. Welche Herausforderungen damit verbunden sind, wird im Folgenden ausführlich beleuchtet:

#1

Unbekannte und unkontrollierte Risiken

Die Cybersicherheit gestaltet sich Tag für Tag schwieriger. Raffinierte Angreifer spüren Firewalls, VPNs und Cloud basierte virtuelle Firewalls auf und überwinden sie. Jede dem Internet zugewandte Firewall — ob im Rechenzentrum, in der Cloud oder in Zweigstellen — kann von Cyberkriminellen erkannt, angegriffen und ausgenutzt werden. Die Angreifer suchen nach möglichen Sicherheitslücken, um Zugriff zu erlangen. Nach erfolgreichem Angriff können sie sich an den Daten bedienen, Zugriff verweigern oder sich lateral im Netzwerk bewegen, andere Geräte ins Visier nehmen oder Sicherheitslücken aufspüren.

Herkömmliche Sicherheitsarchitekturen sind zur Abwehr solcher komplexen Angriffe ungeeignet, denn jeder User mit Zugriff auf das „gesicherte" Netzwerk gilt automatisch als vertrauenswürdig und kann auf sämtliche Anwendungen zugreifen — auch wenn er böse Absichten hat. Virtuelle Firewalls können ebenfalls entdeckt werden und bergen im schlimmsten Fall sogar ein deutlich größeres Risiko als physische Firewalls.

Die meisten Angreifer schlagen nicht direkt beim erstbesten Rechner zu. Stattdessen wird die Umgebung auf mögliche Wege zur lateralen Ausbreitung untersucht, um möglichst noch mehr Angriffsziele zu infizieren. Bedrohungen bewegen sich so unbemerkt durch das gesamte Netzwerk und legen Ransomware in weiteren Systemen ab. Sobald eine kritische Masse erreicht ist, verschlüsselt die Ransomware alle Angriffsziele auf einmal und kann dem Unternehmen damit einen vernichtenden Schlag versetzen. Durch die flachen Netzwerksicherheitsarchitekturen wird das überhaupt erst möglich.

Ein Vergleich: Einbrecher, die über das Badezimmerfenster in ein Haus gelangen, finden dort zwar noch keine Wertsachen, können von dort aus aber ohne Probleme das Schlafzimmer oder andere Orte im Haus aufsuchen, die weder verschlossen noch anderweitig geschützt sind.

Geringeres Risiko mit Zero Trust

Damit nur berechtigte User auf Anwendungen zugreifen können, müssen die Angriffsfläche beseitigt und Sicherheitsmaßnahmen inline und an der Edge durchgesetzt werden. Wenn Anwendungen für Angreifer unsichtbar und nur für befugte User zugänglich sind, verschwindet damit auch die Angriffsfläche. Der Zugriff auf Anwendungen — ob im Internet, in SaaS oder in öffentlichen/privaten Clouds — ist auf diese Weise immer sicher.

Was wird der lateralen Ausbreitung von Bedrohungen entgegengesetzt? Bei Zero Trust verbindet sich eine berechtigte Entität (z. B. ein authentifizierter User) direkt mit einer bestimmten Anwendung.

67 % der Unternehmen sind überzeugt, dass Firewalls nicht in der Lage sind, schnellen und sicheren Zugriff für Remote User zu schaffen[1]

Der authentifizierte Benutzer hat als einziger Zugriff auf die angeforderte Anwendung. Unberechtigte User können die Anwendung nicht sehen, wodurch nicht nur der Angriffsweg eliminiert, sondern auch eine laterale Ausbreitung auf andere Geräte oder Anwendungen verhindert wird.

Wenn etwas keine Angriffsfläche hat, kann es auch nicht angegriffen werden — so wie die Einbrecher im vorherigen Beispiel nie in das Haus einbrechen könnten, wenn es gar nicht erst zu finden wäre. Und selbst wenn sie es entdecken würden, wären sämtliche anderen Räume eigene, völlig unabhängige Einheiten, zu denen der Zugang jeweils nur individuell möglich wäre. Dadurch kämen die Einbrecher nie weiter als bis zum Badezimmer.

Zero Trust arbeitet mit Identität und Kontext, wobei der Kontext ständig geprüft wird. Eine Zero Trust Lösung sollte sämtliche Daten verschlüsseln, mögliche Datenverluste erkennen und einen Austausch von Bedrohungen verhindern. Für eine sichere Verbindung wird ständig überprüft, ob ein User bestimmte kontextuelle und räumliche Anhaltspunkte erfüllt, etwa Standort, IP Adresse, Gerätestatus und Tageszeit. Dies geschieht unbemerkt, wodurch es für authentifizierte Benutzer zu keinen Unterbrechungen kommt.

#2 Steigende Komplexität

Eine der gefürchtetsten Aufgaben für die IT Sicherheit ist die Verteilung von Richtlinien über einen Flickenteppich aus Cloud- und hardwarebasierter Infrastruktur. Unternehmen bestimmen anhand von Richtlinien auf höchster Ebene, worauf Mitarbeiter zugreifen dürfen und worauf nicht. Diese Geschäftsrichtlinien werden dann in Netzwerkrichtlinien übersetzt, da das Perimeter Sicherheitsmodell mit Netzwerkzugriff arbeitet. Bei verteilten Infrastrukturen, bei denen anders als beim klassischen Rechenzentrum mehr SaaS- oder Cloud basierte Anwendungen zum Einsatz kommen und zahlreiche User remote arbeiten, wird die Anwendung von Netzwerkrichtlinien immer komplizierter. Hier dehnt sich der Perimeter plötzlich über das Rechenzentrum hinaus auf alle Standorte von Anwendungen und Usern aus. Für ein solches Netzwerk müssen unzählige Richtlinien mühsam definiert werden: für Zugriff vom Büro aus, für SaaS Applikationen, Firewalls, IPS/IDS und vieles mehr.

Heutzutage liegen Anwendungen nicht in einer einzigen Cloud, sondern sind in mehreren Abhängigkeiten über Multicloud Umgebungen die häufig miteinander kommunizieren müssen, verteilt. Die Verwaltung von Anwendungen in Multicloud Umgebungen ist wesentlich komplexer als das Zusammenfügen sicherer Verbindungen über mehrere Clouds und Rechenzentren hinweg. So entsteht ein immer komplexeres Geflecht aus Site-to-Site-VPNs, Firewalls, Transit Gateways und Peering Richtlinien.

Die Verantwortlichen müssen den künftigen Bedarf prognostizieren und anhand aufwändiger Kapazitätsplanung die entsprechende Bandbreite und Skalierfähigkeit des Netzwerks sicherstellen. Ist der Bedarf am Ende größer als veranschlagt, leidet die Performance. Eine Überkapazität hingegen bedeutet unnötige Kosten und überschüssige Hardware. Darüber hinaus muss die IT-Sicherheit für zahllose Einzelprodukte

75 % aller Unternehmen sehen Hardware, Upgrades und Bereitstellung als Herausforderung[1] für Firewalls

regelmäßig Updates, Patches und Fehlerbehebungen vornehmen. Diese für die Unternehmenssicherheit unerlässlichen Aufgaben können Wochen oder gar Monate in Anspruch nehmen.

Weniger Komplexität mit Zero Trust

Bei Zero Trust erfolgt die Durchsetzung von Richtlinien an einem Punkt zwischen dem Gerät (z. B. Mobilgerät oder IoT) und den angeforderten Ressourcen wie unter anderem Cloud Applikationen, SaaS Applikation und Internet Anwendungen. Für die Entscheidung, ob ein bestimmtes Gerät Zugriff auf die angeforderte Ressource bekommt, wird neben Geschäftsrichtlinien hinsichtlich der Zugriffsberechtigungen auch der Kontext auf verschiedene Weise berücksichtigt. Dadurch, dass Geschäftsrichtlinien inline durchgesetzt werden, entfällt die aufwändige Übersetzung in Netzwerkrichtlinien, die bei perimeterbasierten Modellen erforderlich ist.

Eine integrierte Zero Trust Lösung benötigt zum Absichern sämtlicher SaaS-, Internet- und privater Applikationen nur eine einzige Plattform und keine arbeitsaufwändigen hardwarebasierten oder virtuellen Lösungen mehr. Einheitliche Zero Trust Plattformen mit einer einzigen Verwaltungskonsole lassen sich viel schneller konfigurieren und einfacher verwalten als herkömmliche perimeterbasierte Sicherheitslösungen und überzeugen durch vereinfachte Richtlinien bei höherem Sicherheitsniveau.

Bei einer Cloud basierten Zero Trust Lösung sind Sicherheitskontrollen, User und Anwendungen alle in der Cloud, was das Skalieren erleichtert. Auch bei einer steigenden Anzahl von Usern und Anwendungen bleibt die schnelle und nahtlose schlechte Anwendererfahrung erhalten. Durch noch transparentere Sichtbarkeit zwischen Usern, Clouds und Workloads erleichtert Zero Trust den Betrieb und vereinfacht die Fehlerbehebung.

#3

Schlechte Nutzererfahrung

User erwarten, dass Anwendungen überall gleich gut funktionieren — ob im Büro, zu Hause oder unterwegs. Wie der Zugriff auf eine Anwendung genau erfolgt oder welches Sicherheitsmodell im Backend zum Einsatz kommt, ist für sie uninteressant. Wenn Anwendungen nicht abrufbar sind oder nur langsam reagieren, geht dies auf Kosten der Produktivität und der Anwendererfahrung.

In herkömmlichen Hub-and-Spoke Netzwerkarchitekturen müssen Remote Büros und Zweigstellen durch Firewalls über MPLS mit der Unternehmenszentrale (dem Rechenzentrum) verbunden werden, während Remote User VPNs benötigen.

Es entsteht ein flaches Netzwerk unter Einbeziehung sämtlicher Standorte, bei dem der gesamte Netzwerk Traffic durch einen zentralen Security Stack geleitet wird. Der Traffic wandert also zunächst vom Remote User durchs Rechenzentrum und von dort aus in die Cloud und dann in umgekehrter Richtung wieder zurück zum User. Das führt zu unvorhersagbarer

300 %
Wachstum beim Anteil von Remote Usern an der Gesamtbelegschaft[4]

Latenz und einer erheblichen Beeinträchtigung der User Experience. Das Problem besteht auch bei Cloud basierten virtuellen Firewalls in ihrer Eigenschaft als Bestandteil einer flachen Netzwerkarchitektur, denn auch hier muss sämtlicher Traffic zunächst zur virtuellen Firewall fließen, wodurch ein neuer Flaschenhals in der Cloud entsteht.

Organisationen sind darauf angewiesen, dass Mitarbeiter, Partner, Lieferanten oder Kunden gleichermaßen mit jedem Gerät von überall problemlos und schnell auf Anwendungen zugreifen können. Die zunehmende Dezentralisierung von Usern, Daten, Anwendungen und Geräten kann die Arbeit für die IT jedoch erschweren.

Optimierte Anwendererfahrung mit Zero Trust

Zero Trust behebt Probleme mit der User Experience, da Richtlinien inline (an der Edge) durchgesetzt werden und keine zusätzlichen Hops nötig sind. Es schafft eine direkte Verbindung mit Anwendungen unabhängig von Standort und Gerät. Die direkte Verbindung beseitigt zudem Latenzen, da das Traffic Backhauling über zentralisierte Sicherheitskontrollen überflüssig wird. Dadurch, dass eine Zero Trust Plattform im Datenpfad arbeitet, kann sie zudem sämtliche Verbindungen überwachen und Performance Probleme automatisch erkennen und beheben.

Eine an der Edge bereitgestellte Zero Trust Lösung prüft sämtliche Inhalte in einem einzigen Schritt, ohne Pakete kopieren zu müssen. Anders als beim Ansatz mit hintereinandergeschalteten physischen und virtuellen Appliances, bei dem jeder einzelne Sicherheitsservice Pakete verarbeitet, entsteht so keine Latenz durch zusätzliche Hops. Ein einziger Scan reicht aus, um Richtlinien auf verschiedene Sicherheitssysteme anzuwenden — bei minimaler Latenz.

Anwendungen nach dem Prinzip „Critical Unified Communications as a Service (UCaaS)“ wie etwa Microsoft Teams und Zoom sind auf geringe Latenzen angewiesen. Mit Zero Trust ist eine solche geringe Latenz bei zugleich hoher Verfügbarkeit möglich, da hierbei je nach Verfügbarkeit und Kapazitäten der Anwendung ein direktes Peering mit dem Anwendungsanbieter erfolgen kann. Greift beispielsweise ein User in Texas auf Microsoft365 zu, wird eine Verbindung mit dem nächsten Rechenzentrum hergestellt und die Sicherheit inline überprüft. Durch die Richtliniendurchsetzung an der Edge sind keine zusätzlichen Hops nötig — ein erheblicher Vorteil zu Hub-and-Spoke Architekturen.

Um Zusammenarbeit und Produktivität im Unternehmen zu optimieren, muss Zero Trust diese Anwendungen mittels Digital Experience Monitoring (DEM) überwachen und Fehler schnell beheben. Als Inline Lösung, die im Datenpfad arbeitet, kann eine Zero Trust Plattform zudem sämtliche Verbindungen erheblich leichter überwachen und Performance Probleme sowohl automatisch erkennen als auch beheben.

#4

Zögerliche IT-Transformation

Die Transformation eines Unternehmens setzt auch eine Transformation der IT voraus. Auf eine Cloud basierte Zero Trust Lösung umzusteigen und die Hardware Infrastruktur zu ersetzen, kann durchaus einschüchternd wirken. Es ist eine Aufgabe, bei der neben den verschiedenen Bereichen der IT wie unter anderem Sicherheit, Netzwerke und Betrieb das gesamte Unternehmen gefordert ist.

Kaum etwas erschwert die digitale Transformation in Organisationen so sehr wie unzureichende Kommunikation zwischen verschiedenen Bereichen der IT. Das liegt in der Natur der Sache, da die Teams für klar getrennte Bereiche von Netzwerk- und Sicherheitsinfrastruktur zuständig sind, an verschiedenen Komponenten arbeiten und nicht unbedingt ein übergreifendes Problem im Blick haben. So kümmert sich

das Sicherheits Team um Firewalls, VPNs und den Security Stack, wohingegen das für das Netzwerk zuständige Team ein funktionierendes Routing und Switching gewährleistet und Protokolle wie beispielsweise MPLS und OSPF bereitstellt. Diese beiden Teams arbeiten weitgehend unabhängig voneinander, es sei denn, sie befassen sich mit der Interoperabilität von Systemen. Für den Umstieg auf eine Cloud basierte Infrastruktur ist anders als bisher nun ihre Zusammenarbeit gefordert. Ohne die geeigneten Tools, Weiterbildungen und Prozesse kann sich dieser Wandel in der Arbeitsweise schwierig gestalten.

67 % aller Sicherheitsexperten sehen ihre Zukunft in der Cloud Sicherheit und nicht in der Firewall Verwaltung[1]

Darüber hinaus stellt der Umstieg auf eine neue Architektur die Investitionen in die bisherigen Netzwerksicherheitsarchitekturen infrage, was zunächst schwer zu vermitteln sein kann. Bei den letztlich für einen Umstieg in die Cloud verantwortlichen Teams kann eine solche Trans-formation angesichts seit Jahrzehnten etablierter Herangehensweisen zunächst auf Widerstand stoßen. Außerdem kann es besonders unter den seit Jahrzehnten an Firewalls und VPNs gewöhnten Mitarbeitern im Netzwerk-Team Bedenken hinsichtlich der eigenen Kompetenz im Umgang mit Cloud basierten Lösungen geben.

Schnelle und sichere Transformation mit Zero Trust

Eine Cloud basierte Zero Trust Plattform vereinfacht das Sicherheitsmanagement und die betrieblichen Abläufe. Die verschiedenen Unternehmensbereiche können gemeinsam die Umstellung weg vom Perimeter hin zu einer Cloud basierten und auf Geschäftsrichtlinien aufsetzenden Zero Trust Lösung gestalten. Dadurch werden zeitliche Kapazitäten frei, die in strategische Projekte investiert werden können — wie etwa Datenanalysen, Optimierung der Sicherheit und andere mit größerem Mehrwert für die Unternehmensziele verbundene Aktivitäten. Wenn Teams Silos einreißen und an einem Strang ziehen, profitiert davon die Sicherheit von Organisationen erheblich.

Der Umstieg hin zu einer Cloud basierten Zero Trust Lösung bedeutet eine erhebliche Entlastung des IT Teams, da die Anschaffung, Verwaltung, Wartung und Überwachung von Legacy Hardware entfallen und Kapazitäten frei werden. CISOs und CIOs müssen keine genauen Prognosen des künftigen Hardwarebedarfs und der Kosten für Bandbreite mehr erstellen. Durch klare Kommunikation und einen konkreten Plan kann die Unternehmensleitung die IT für sich gewinnen und eine erfolgreiche Cloud Transformation einläuten.

#5 Hohe Infrastrukturkosten und Ineffizienzen

Hub-and-Spoke Architekturen mit Protokollen wie MPLS erfordern kostspielige Hardware und müssen von erfahrenen IT Kräften gewartet werden. Hinzu kommen Kosten für Bandbreite durch unnötiges Traffic Routing zurück zum Rechenzentrum. Diese Ausgaben fallen auch dann an, wenn die Bandbreite gar nicht genutzt wird, etwa beim Zugriff auf eine Cloud basierte SaaS Applikation. Neben der Netzwerkinfrastruktur schlagen auch die kostspieligen Komponenten der Sicherheitsinfrastruktur mit Firewalls, Switches, Load Balancern, Zugriffskontrollen, VPNs, Sandboxes und Eindringschutzsystemen zu Buche. Darüber hinaus entstehen Kosten für Installation, Konfiguration, Bereitstellung, Tests und Fehlerbehebung und auch für die Wartung. Sind dann noch verschiedene Einzelprodukte im Einsatz, vervielfachen sich die Kosten und der Bedarf an hochqualifizierten Fachkräften.

CIOs und CISOs müssen den zukünftigen Bedarf genau prognostizieren, um die entsprechende Hardware und Bandbreite bereitzustellen. Nur so ist es möglich, den gesamten Traffic über MPLS zur Überprüfung ins Rechenzentrum zu schicken. Es ist ein schwieriger Balanceakt: Wird zu wenig eingeplant, ist nicht genug Spielraum zum Skalieren da, bei zu großzügiger Planung entstehen unnötige Kosten. Wird der Netzwerkbedarf unterschätzt, kann das außerdem die Produktivität beeinträchtigen, wohingegen eine Überkapazität unnötige Kosten und ungenutzte Hardware bedeuten würde. Letztlich benötigt jeder Standort eine eigene Appliance Bereitstellung, wodurch eine uneinheitliche Infrastruktur mit verschiedensten Produkten droht.

Bei Internetbound Traffic sind Breitbandverbindungen sinnvoller, da sie nur einen Bruchteil der Kosten einer Infrastruktur für Netzwerksicherheit ausmachen. Allerdings müssen diese Verbindungen gesichert werden. Dazu müsste jedoch für jede Zweigstelle Gateway Sicherheit für direkte Verbindungen bereitgestellt werden, was ebenfalls mit horrenden Ausgaben verbunden wäre.

50 % aller Unternehmensdaten werden in der Cloud gespeichert[2] und

70 % der Unternehmensanwendungen beruhen auf SaaS[3]

Optimierte Kosten und Effizienz mit Zero Trust

Durch den Umstieg zu einer Cloud Native Zero Trust Lösung sparen sich Unternehmen VPNs, Kosten für die Übertragung in die öffentliche Cloud sowie die Entwicklung eigener Netzwerkarchitekturen. Dadurch sinken Ausgaben bei zugleich erhöhter Sicherheit. Zero Trust mindert die zusätzlichen Kosten aufgrund des steigenden Bedarfs an Remotezugriffen, für den bisher bei perimeterbasierten Lösungen bestehende Firewalls und VPNs unter dem Einsatz teurer Hardware und Infrastruktur skaliert werden mussten.

Zero Trust macht kostspielige MPLS Netzwerke, die komplexes Routing, Switching, Netzwerksegmentierung usw. erfordern, überflüssig. Stattdessen werden schnelle und sichere Direktverbindungen zur Cloud bzw. Konnektivität zwischen unterschiedlichen Cloud Instanzen ermöglicht. Mit einer Zero Trust Architektur verfügen Unternehmen über eine vereinheitlichte Sicherheit, was die Bereitstellung erheblich beschleunigt und die frühzeitige Erkennung und Vermeidung kostspieliger Datenpannen ermöglicht, die sonst Schäden in Millionenhöhe verursachen könnten. Cloud basierte Zero Trust Lösungen können dem Bedarf entsprechend erworben und so wesentlich einfacher, günstiger und schneller skaliert werden. Minutiöse Planung und die Gefahr eines Übereinkaufs entfallen damit.

Zscaler hilft Ihnen bei der Umsetzung von Zero Trust

Zscaler Zero Trust Exchange nutzt die weltweit größte Security Cloud für die Bereitstellung schneller und sicherer Verbindungen auf Zero Trust Basis. Damit können Mitarbeiter überall und auf jedem Gerät mit dem Internet als Unternehmensnetzwerk arbeiten. Im Unterschied zu Firewalls und VPNs beruht die Zero Trust Exchange auf dem Prinzip der minimalen Rechtevergabe — es wird also keinem User und keiner Anwendung automatisch vertraut. Stattdessen werden Verbindungen anhand von Unternehmensrichtlinien in Verbindung mit Identität und Kontext autorisiert. Nach Überprüfung und Durchsetzung der kontextbasierten Unternehmensrichtlinien vermittelt die Zero Trust Exchange die Verbindung zwischen den jeweiligen Ressourcen. User und Geräte werden direkt mit Anwendungen verbunden und erhalten niemals Zugang zum Unternehmensnetzwerk.

Mehr zur Zero Trust Exchange: www.zscaler.de/platform/zero-trust-exchange

Warum Firewalls kein Zero Trust können — ein Webinar:
info.zscaler.com/webinar-why-firewalls-cannot-do-zero- trust?utm_source=digital

Quellen:
[1]Virtual Intelligence Briefing (ViB) Networks Security Survey 2021
[2]Statista. Weltweiter Anteil von Daten und sensiblen Daten, die in der Cloud gespeichert werden.
www.statista.com/statistics/1202541/sensitive-data-cloud-location
[3]Better Cloud. (2021). The State of SaaSOps 2021.
stateofsaasops.bettercloud.com/?_ga=2.164919740.241347015.1636678142-1969514686.1636678142
[4]Grady, John. (2021). The State of Zero Trust Security Strategies. Enterprise Strategy Group.
https://info.zscaler.com/resources-industry-report-the-state-of-zero-trust-security-strategies

zscaler™ | **Erleben Sie Ihre Welt, sicher.**

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 Benutzern, 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. Informieren Sie sich auf **zscaler.de** oder folgen Sie uns auf Twitter **@zscaler**.

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