Perimeter-Firewalls: Fünf Hauptrisiken und eine überzeugende Alternative

Firewalls sind schon seit Langem ein fester Bestandteil der Netzwerkarchitektur im Unternehmen. Im Zuge des Umstiegs auf digitale Geschäftsmodelle erweist sich das einstmals solide Bollwerk jedoch zunehmend als Sicherheitsrisiko. Im Folgenden sollen die größten Gefahrenquellen aufgezeigt und eine effektive Möglichkeit für ihre Bewältigung vorgestellt werden.

In einer herkömmlichen perimeterbasierten Sicherheitsarchitektur mit Firewalls und VPNs beschränken sich die Schutzmaßnahmen auf die Sicherung des Perimeters bzw. der Vertrauenszone. Sämtliche User und Anwendungen gelten automatisch als vertrauenswürdig, wenn sie sich innerhalb des Perimeters befinden, und als potenziell gefährlich, wenn sie außerhalb positioniert sind. Dieses Sicherheitskonzept ging auf, solange die Mehrzahl der User in der Unternehmenszentrale saß und die Mehrzahl der Anwendungen im Rechenzentrum untergebracht war. In Ausnahmefällen wurden externe User und Anwendungen durch Erweiterung des Perimeters ins Netzwerk und damit in die Vertrauenszone einbezogen.

Seit der Erfindung der Firewall hat sich die Geschäftswelt aber grundlegend verändert. Inzwischen arbeiten Mitarbeiter an beliebigen und wechselnden Standorten: im Homeoffice, in Bürogemeinschaften, Zweigstellen des Unternehmens usw., also überall dort, wo eine Internetverbindung und ein Stromanschluss vorhanden sind. Standortferne User und Anwendungen, die früher als Ausnahmefall behandelt wurden, machen heute den Großteil des unternehmensinternen Traffics aus. Entsprechend ist die Erweiterung des Perimeters zur Einbeziehung von Remote-Usern keine gangbare Lösung mehr. Das Prinzip einer Vertrauenszone ist damit ebenfalls obsolet und muss buchstäblich ins Gegenteil verkehrt werden – nämlich durch den Umstieg auf ein Zero-Trust-Modell. Indes ist der Versuch, dieses neue Konzept mit Firewalls und VPNs umzusetzen, nicht nur zum Scheitern verurteilt, sondern birgt auch eine Reihe von Risiken.

In diesem Whitepaper wird Zero Trust als zukunftsfähiger Ansatz zur Bewältigung der fünf Hauptrisiken aufgezeigt, die der Einsatz von Firewalls in einer Cloud-orientierten und mobilen Geschäftswelt mit sich bringt.

RISIKO Nr. 1

Große Angriffsfläche

Als Angriffsfläche wird die Gesamtheit aller offengelegten Punkte bezeichnet, die Angreifern unter Umständen ermöglichen, Sicherheitsrisiken zu erkennen und auszunutzen, um auf ein System zuzugreifen und wertvolle Daten zu exfiltrieren. Dazu zählen u. a. IP-Adressen. Grundsätzlich gilt: Je kleiner die Angriffsfläche, desto schwieriger ist es für Angreifer, sich unbefugten Zugriff zu verschaffen. Durch die zunehmende Verlagerung von Anwendungen in die Cloud und den Umstieg auf mobile Arbeit hat sich die Angriffsfläche vieler Organisationen indes exponentiell vergrößert. Entsprechend höher ist ihre Anfälligkeit für Cyberbedrohungen. Der Einsatz perimeterbasierter physischer oder virtueller Firewalls schafft hier keine Abhilfe, sondern verschärft das Problem eher. Hierdurch entstehen nämlich zusätzliche Angriffsflächen, über die sich Cyberkriminelle Zugang zum Netzwerk bzw. den Cloud-Instanzen verschaffen können.

Konkret liegt das daran, dass Firewalls die IP-Adressen der Server und Anwendungen im Internet veröffentlichen, um sie für die Mitarbeiter und Geschäftspartner eines Unternehmens zugänglich zu machen. Damit werden sie jedoch auch für Angreifer sichtbar. Jede im Internet sichtbare Firewall – ob im Rechenzentrum, in der Cloud oder in Zweigstellen – kann von Cyberkriminellen erkannt und für Angriffe ausgenutzt werden. Der Versuch, das Risiko zu verringern, indem virtuelle statt physischer Firewalls eingesetzt werden, bewirkt eher das Gegenteil. Denn die Veröffentlichung von IP-Adressen im Internet wird dadurch nicht verhindert, sondern im schlimmsten Fall sogar um ein Vielfaches multipliziert.

Zero Trust zur Minimierung der Angriffsfläche

Die erfolgreiche Minimierung der Angriffsfläche ist die Grundvoraussetzung für die Sicherung des Netzwerks, der Anwendungen und vor allem der Daten einer Organisation. Eine echte Zero-Trust-Lösung gewährleistet, dass Anwendungen weder routingfähig noch für potenzielle Angreifer sichtbar sind, sodass Ressourcen nicht von Unbefugten im Internet erkannt werden. Eine echte Zero-Trust-Plattform fungiert als Vermittler zwischen Usern und Anwendungen. Das heißt, die gesamte Kommunikation läuft über die Plattform und jede Verbindung zu Anwendungen muss erst durch die Plattform zugelassen werden.

Der grundsätzliche Unterschied zu Perimeter-Firewalls liegt darin, dass nur ausgehende Verbindungen zugelassen werden. Dadurch entfällt im Gegensatz zu den traditionell eingehenden Verbindungen die Notwendigkeit, IP-Adressen im Internet zu veröffentlichen. Indem Anwendungen für Angreifer unsichtbar und nur für befugte User zugänglich gemacht werden, verschwindet die Angriffsfläche im Prinzip. Der Zugriff auf Anwendungen – ob im Internet, in SaaS oder in öffentlichen oder privaten Clouds – ist auf diese Weise immer sicher.

Erkennen von Angriffsflächen

Manuell sind Angriffsflächen oft schwer zu erkennen. Daher gibt es Tools zur Analyse der Internet-Angriffsfläche, die Auskunft über sämtliche Server, Namespaces, Sicherheitsrisiken und Cloud-Instanzen liefern, die aktuell im Internet erkennbar sind. Durch Abfragen öffentlicher Quellen werden sämtliche offengelegten Ressourcen erkannt, die ein Sicherheitsrisiko darstellen. Dadurch erhalten Unternehmen aussagekräftige Informationen über ihre Angriffsflächen und können ein Zero-Trust-Konzept zu ihrer Reduzierung implementieren.

RISIKO Nr. 2

Verringerung der Anwendungsperformance

Die Mitarbeiter stellen heute hohe Ansprüche an die Ladegeschwindigkeit und Verfügbarkeit von Cloud-Anwendungen – und machen immer wieder die Erfahrung, dass die vom Unternehmen eingesetzten Lösungen für den Netzwerkzugang bei Weitem nicht an die zügige und reibungslose User Experience heranreichen, die sie beim Direktzugriff auf Cloud-Anwendungen im Privatleben gewohnt sind. Die unzureichende Anwendungsleistung beeinträchtigt sowohl ihre Produktivität als auch die Fähigkeit zur effektiven virtuellen Zusammenarbeit mit Kollegen. Zur Vermeidung dieser Probleme werden Sicherheitskontrollen gerne umgangen – eine riskante Strategie, zumal der Zugriff auf unternehmenskritische Ressourcen häufig über nicht verwaltete Geräte bzw. ungesicherte WLAN- oder Heimnetzwerke erfolgt. Zudem werden die Identifizierung, Diagnose und Behebung von Beeinträchtigungen der User Experience erschwert, die durch die Verfügbarkeit von SaaS- oder Cloud-Anwendungen, Gerätekapazität, Netzwerkpfadausfälle oder Netzwerküberlastung verursacht werden.

In herkömmlichen, sogenannten Hub-and-Spoke-Netzwerkarchitekturen müssen Remote-Büros und Zweigstellen durch Firewalls über MPLS mit der Unternehmenszentrale (dem Rechenzentrum) und durch VPN mit Remote-Usern verbunden werden. Es entsteht durch diese Architektur ein flaches Netzwerk unter Einbeziehung sämtlicher Standorte. Der gesamte Netzwerk-Traffic wird durch einen zentralen Security-Stack geleitet. Der Traffic wird also zunächst vom Remote-User durch das Rechenzentrum und von dort aus in die Cloud und dann in umgekehrter Richtung wieder zurück zum User geschickt. Dadurch wird die Latenz erheblich erhöht und die User Experience entsprechend beeinträchtigt. Virtuelle Firewalls in der Cloud lösen das Problem nicht. Auch sie befinden sich nicht in den Anwendungsservern und der Traffic muss wie bei physischen Rechenzentren zu ihnen umgeleitet werden.

Cloud-Anwendungen funktionieren am besten, wenn der Zugriff auf sie direkt mit möglichst wenigen Hops erfolgt. Viele SaaS-Anbieter (wie Microsoft 365) raten daher ausdrücklich vom Einsatz von Firewalls ab.

Zero Trust zur Behebung von Performanceproblemen

Eine Zero-Trust-Architektur empfiehlt sich als zukunftsfähige Alternative zu herkömmlichen Hub-and-Spoke-Netzwerken mit Sicherheitsperimeter im Stile einer Festung mit Burggraben. Durch direkte Verbindungen zu Anwendungen lassen sich bei gleichzeitiger Verbesserung der User Experience Risiken reduzieren.

Eine effektive Zero-Trust-Plattform setzt Richtlinien inline am Edge durch, sodass keine zusätzlichen Hops erforderlich sind. Durch direktes Peering mit Anwendungsunternehmen können basierend auf Verfügbarkeit und Kapazität Direktverbindungen gewährleistet werden. Die Ausführung der Zero-Trust-Plattform im Datenpfad ermöglicht zudem eine Überwachung sämtlicher Verbindungen. Leistungsabfälle werden automatisch erkannt und behoben – eine unverzichtbare Voraussetzung für die reibungslose Funktion von Anwendungen mit geringer Latenz, z. B. UCaaS-Anwendungen (Unified Communications as a Service) wie Microsoft Teams und Zoom. DEM-Funktionen (Digital Experience Monitoring) zur Überwachung dieser Anwendungen und zur Fehlerbehebung tragen zur Steigerung der Produktivität und verbesserten virtuellen Zusammenarbeit bei. So werden Probleme erkannt und behoben, bevor sie den Usern überhaupt auffallen.

Messung der User Experience

Ein branchenführendes Monitoring-Tool zur Messung der User Experience liefert datengestützte Erkenntnisse, die Unternehmen eine effektive Erkennung, Diagnose und Behebung von Problemen in Bezug auf die digitale User Experience ermöglichen. Mithilfe maschineller Lernalgorithmen werden Performance-Abweichungen identifiziert und entsprechende Warnmeldungen mit Handlungsempfehlungen ausgegeben.

Hoher Betriebs- und Kostenaufwand

Ein Zero-Trust-Konzept mit Firewalls, MPLS und VPNS oder virtuellen Appliances umsetzen zu wollen, ist kein realistischer Ansatz. Die Verwaltung und Bereitstellung von Perimeter-Firewalls zur Gewährleistung eines einheitlichen Sicherheitsniveaus für alle User, Anwendungen, Geräte und Standorte ist mit einem sehr hohen Betriebs- und Kostenaufwand verbunden. Zur Verwaltung der erforderlichen Policy-Deployments, Updates und Patches müsste der Personalbestand bei einem Wachstum erheblich aufgestockt werden. Hinzu kommen die Anschaffung und Bereitstellung physischer und virtueller Firewalls zur Bewältigung von Worst-Case-Szenarien. Die Beanspruchung unnötiger Bandbreite und Sicherheitskapazitäten durch Backhauling des Traffics zu einem zentralen Security-Stack ist ein weiteres Argument, das gegen diesen Ansatz spricht.

Eine präzise Kapazitätsplanung setzt voraus, dass CIOs und CISOs sowohl die zukünftigen Hardwareanforderungen als auch die Kosten für den Bandbreitenverbrauch genau abschätzen können, die entstehen, wenn der gesamte Traffic über MPLs zur Überprüfung an das Rechenzentrum weitergeleitet wird. Eine Unterschätzung des Netzwerkbedarfs führt zu Performanceverlusten, eine Überschätzung zu unnötig hohen Kosten und ungenutzten Geräten. Davon abgesehen ist es in der Praxis kaum machbar, an jedem Standort einen identischen Appliance-Stack bereitzustellen. Wahrscheinlicher ist, dass die Infrastruktur durch ein unübersichtliches Sammelsurium verschiedener Einzelprodukte belastet wird. Die Erfassung und Verwaltung von Protokollen für alle diese Geräte stellt dann eine weitere Herausforderung dar – und kann schnell zum Sicherheitsrisiko werden, wenn wichtige Protokolle versehentlich ignoriert werden. Kein Wunder also, dass 75 % (!) der Netzwerkbetreiber die Verwaltung von Hardware, Upgrades und Deployments für Firewalls als Herausforderung empfinden.[2]

Erschwerend hinzu kommt, dass dieser fragmentierte Ansatz eine Reihe weiterer Probleme mit sich bringt. So müssen zur Implementierung der unterschiedlichen Richtlinien und zur Verwaltung der unterschiedlichen Zonen für die Netzwerksegmentierung separate Management-Plattformen eingesetzt werden, für die jeweils eigene Abonnements bzw. Lizenzen erforderlich sind. Auch die Gewährleistung einer möglichst lückenlosen Transparenz über alle User, Anwendungen und Standorte hinweg ist mit hohem Aufwand verbunden. IT-Fachkräfte müssen ihre gesamte Arbeitszeit für die Implementierung von Patches, Sicherheitsupdates, Hardwareaktualisierungen und die Verwaltung von Richtlinien für das Sammelsurium an Firewalls und Sicherheitsappliances aufwenden. Die Folge sind eine mittel- bis langfristig untragbare Verschwendung von Finanzmitteln und die Beeinträchtigung der Mitarbeiterproduktivität.

Zero Trust zur Reduzierung der Komplexität

Als effizientere Alternative zum Einsatz mehrerer hardwarebasierter Lösungen oder Cloud-basierter Einzelprodukte empfiehlt sich eine integrierte Zero-Trust-Lösung. Da sämtliche SaaS-, webbasierten und privaten Anwendungen über eine zentrale Plattform geschützt werden, profitieren Unternehmen von einem sehr viel geringeren Verwaltungs- und Wartungsaufwand. Zero Trust macht kostspielige MPLS-Netzwerke überflüssig, die komplexes Routing, Switching, Netzwerksegmentierung usw. erfordern. Stattdessen werden schnelle und sichere Direktverbindungen zur Cloud bzw. Konnektivität zwischen unterschiedlichen Cloud-Instanzen ermöglicht. Damit entfällt im Wesentlichen die Notwendigkeit, den Traffic zur Überprüfung ins Rechenzentrum umzuleiten. Eine zentrale Zero-Trust-Plattform mit einer einzigen Verwaltungskonsole lässt sich nicht nur viel schneller konfigurieren und einfacher verwalten als herkömmliche perimeterbasierte Sicherheitslösungen, sondern überzeugt auch durch vereinfachte Richtlinien bei höherem Sicherheitsniveau.

Eine Cloud-basierte Zero-Trust-Lösung stellt Sicherheitskontrollen dort bereit, wo sich die User und Anwendungen befinden: in der Cloud. Sie gewährleistet transparente Einblicke in sämtliche Verbindungen zwischen Usern, Clouds und Workloads, wodurch sie den Betrieb erleichtert und die Fehlerbehebung vereinfacht. Die Verlagerung in die Cloud bedeutet eine erhebliche Entlastung des IT-Teams, da die Anschaffung, Verwaltung, Wartung und Überwachung von Firewalls und sonstiger Security-Hardware entfallen. So werden Kapazitäten für neue Projekte freigesetzt. Vor allem ermöglicht eine Cloud-basierte Zero-Trust-Lösung jedoch eine flexible Skalierung bei einer zunehmenden Anzahl von Usern und Anwendungen.

Kostenbewusstsein

Im 2021 veröffentlichten VPN Risk Report von Cybersecurity Insiders werden die Herausforderungen im Zusammenhang mit der Bereitstellung einer Remote-Access-Lösung untersucht. Für die befragten Unternehmen rangierten die hohen Kosten für Sicherheitsappliances und -infrastruktur dabei an zweiter Stelle. Die Erfahrungen mit der Zero Trust Exchange wurden indes insgesamt als positiv bewertet: Organisationen, die die Zscaler-Plattform nutzen, konnten durchschnittlich einen ROI von 139 % und einen Geschäftsnutzen von 4,1 Mio. USD erwirtschaften. Ebenso verzeichneten sie einen Anstieg der Produktivität bei weniger Sicherheitsvorfällen und konnten die Anzahl der eingesetzten Appliances reduzieren.[3]

RISIKO Nr. 4

Laterale Ausbreitung von Bedrohungen

Angreifer verschaffen sich auf verschiedenen Wegen Zugang zum Netzwerk einer Organisation. Häufig kommen dabei Phishing-Angriffe oder Malware-Infektionen zum Einsatz. Anschließend suchen sie nach Möglichkeiten, sich lateral im Netzwerk zu bewegen. So machen sie sensible Daten ausfindig, die dann exfiltriert bzw. für Lösegeldforderungen verschlüsselt werden, oder verursachen anderweitige Störungen. Durch laterale Bewegungen können Angreifer sich der Entdeckung entziehen und behalten weiterhin den Zugriff auf das Netzwerk, auch wenn der ursprünglich infizierte Rechner vom Netzwerk getrennt wird. Teilweise liegen zwischen der ursprünglichen Sicherheitsverletzung und dem eigentlichen Datendiebstahl mehrere Wochen oder gar Monate.

Zum Schutz ihrer Daten vor Angriffen verlassen Unternehmen sich bislang auf sogenannte Sicherheitsperimeter, die nach dem Prinzip mittelalterlicher Festungen mit Burggraben, Wachtürmen und Zugbrücke funktionieren. Entsprechend wird massiv in Firewalls und ähnliche Schutzbefestigungen zur Abwehr externer Eindringlinge investiert. Perimeterbasierte Lösungen überwachen die Eingangs- und Ausgangspunkte des Netzwerks, indem alle ein- und ausgehenden Datenpakete überprüft werden. Auch User müssen erst ihre Identität nachweisen, um Zugang zum Netzwerk zu erhalten oder es wieder verlassen zu dürfen. Alle Aktivitäten innerhalb dieses geschützten Perimeters werden hingegen als tendenziell sicher eingestuft.

Herkömmliche Sicherheitsarchitekturen sind zur Abwehr raffinierter Angriffe ungeeignet, denn jeder User, der sich Zugriff zum „gesicherten" Netzwerk verschafft, wird automatisch als vertrauenswürdig eingestuft und kann entsprechend auf sämtliche Anwendungen zugreifen – auch wenn er böse Absichten hat. Laterale Bewegungen innerhalb perimeterbasierter Architekturen lassen sich nur durch Netzwerksegmentierung (interne Perimeter) einschränken – eine in jeder Hinsicht suboptimale Lösung, die die Bereitstellung und Verwaltung zusätzlicher Firewalls mit weiteren Richtlinien erforderlich macht, ohne das zugrunde liegende Problem zu beheben.

Zero Trust zur Einschränkung lateraler Bewegungen

Zero Trust lässt keine lateralen Bewegungen zu, da User und Workloads direkt mit Anwendungen verbunden werden und niemals Zugang zum Unternehmensnetzwerk erhalten. So wird auch ohne komplexe Netzwerksegmentierung verhindert, dass Bedrohungen sich lateral verbreiten und andere Geräte bzw. Anwendungen infizieren können. Das gilt nicht nur für Verbindungen zwischen Usern und Anwendungen, sondern möglicherweise auch für sämtliche Verbindungen innerhalb der Organisation, von IoT-Geräten bis hin zur Kommunikation zwischen Anwendungen an beliebigen Standorten (in der Cloud oder im Rechenzentrum). Da sichere Verbindungen immer nur einzeln hergestellt werden, wird das Risiko lateraler Bewegungen ausgeschlossen.

Das Zero-Trust-Modell beruht auf der Annahme, dass jeder User und jede Anwendung eine potenzielle Bedrohung darstellen. Verbindungen werden ausschließlich auf der Basis von Identität und Kontext genehmigt. Das heißt, es wird sowohl die Identität der Entitäten überprüft, die sich verbinden, als auch der Kontext ihrer Verbindungen. Nach dem Prinzip der minimalen Rechtevergabe wird so immer nur Zugriff auf die jeweils benötigten Ressourcen gewährt. Das bedeutet eine erhebliche Entlastung der Sicherheits- und IT-Beauftragten, da die Vergabe bzw. Verweigerung von Zugriffsberechtigungen automatisch erfolgt und ggf. dynamisch an veränderte Bedingungen bei Entitäten und ihren Verbindungen angepasst wird.

Als weiteren Vorteil ermöglicht Zero Trust die Einrichtung granularer Kontrollen mit bedingtem Zugriff. Richtlinien können so konfiguriert werden, dass der Zugriff auf bestimmte Anwendungen nur von einem vertrauenswürdigen Standort aus möglich ist – z. B. dem Unternehmensnetzwerk – und eine mehrstufige Authentifizierung voraussetzt. Umgekehrt können Administratoren den User-Traffic blockieren, der von bestimmten Standorten bzw. geografischen Regionen oder nicht vertrauenswürdigen Geräten ausgeht. Auch kann der Zugriff auf angeforderte Daten verweigert werden, die nicht ausdrücklich im Umfang der jeweiligen User-Berechtigung enthalten sind. Alle Verbindungen werden kontextbasiert hergestellt. Entsprechend macht jede Kontextänderung eine Neubewertung erforderlich.

Eine effizientere Methode zur Segmentierung

Der finanzielle, zeitliche und personelle Aufwand für die Netzwerksegmentierung mithilfe virtueller Firewalls steht in keinem Verhältnis zu ihrem Sicherheitsvorteil. Die Workload-Segmentierung ist eine neue Methode zur Segmentierung von Anwendungs-Workloads und Optimierung der Sicherheit mit einem einzigen Klick. Workload-Segmentierung deckt Risiken auf und wendet identitätsbasierten Schutz auf Workloads an, ohne dass Veränderungen am Netzwerk erforderlich sind. Die Technologie der Workload-Segmentierung beruht auf einem identitätsbasierten Modell und bietet lückenlosen Schutz mit Richtlinien, die sich automatisch an Veränderungen der Umgebung anpassen.

RISIKO Nr. 5

Datenverluste

Daten sind für jede Organisation eine unverzichtbare Ressource mit strategischer, finanzieller und sicherheitstechnischer Bedeutung. Manchmal steht sogar die nationale Sicherheit auf dem Spiel. Selbst wenn das Netzwerk durch Sicherheitsperimeter geschützt ist, kann es zu Datenverlusten oder -pannen kommen, sei es aufgrund mangelnder Aufklärung der Mitarbeiter, unbeabsichtigter Aktionen der User, Systemstörungen oder Aktivitäten zunehmend raffinierter Krimineller. Die möglichen Folgen reichen von Geldstrafen über den Verlust von Kunden, rechtliche Komplikationen, Verstöße gegen Vorschriften bis hin zur Schädigung der Marke. Abhängig vom jeweiligen Status der Daten ergeben sich unterschiedliche Risiken:

- **Bei der Übertragung:** Hierbei handelt es sich heutzutage hauptsächlich um webbasierte Datenübertragung. Unabhängig davon, ob die Bereitstellung über SaaS, im Rechenzentrum oder in öffentlichen Clouds erfolgt, wird heutzutage in der Mehrzahl der Fälle über das Internet auf Anwendungen zugegriffen. Dadurch erhöht sich das Risiko einer Exfiltration sensibler Unternehmensdaten beim Zugriff auf riskante Adressen. Firewalls folgen den Usern nicht nach außen und bieten keinen Schutz für Web-Traffic außerhalb des Netzwerks. Je mehr die Bereitstellung von Anwendungen bzw. Speicherung von Daten auf Endgeräten an Relevanz verliert, desto mehr Bedeutung kommt dem Schutz des Datenverkehrs zwischen Endgeräten, Cloud-Anwendungen und Speicherorten durch geeignete Lösungen für die Übertragung zu.
- **Im Ruhezustand:** Ruhende Daten sind überwiegend im Rechenzentrum, in SaaS-Anwendungen oder in öffentlichen Clouds gespeichert. Geschäftskritische Priorität hat insbesondere der Schutz von Daten in SaaS-Anwendungen wie Microsoft One Drive, die mit wenigen Klicks für unbefugte User freigegeben werden können. Firewalls richten hier wenig aus. Hinzu kommt das Risiko von Cloud-Sicherheitsverletzungen, die durch Fehlkonfigurationen oder Fehler bei der Vergabe von Berechtigungen verursacht werden. Aufgrund des hochgradig dynamischen Charakters von SaaS- und IaaS-Anwendungen, die zudem häufig nicht von Sicherheitsexperten konfiguriert werden, kann es schnell passieren, dass die dadurch entstehenden Schwachstellen übersehen und ausgenutzt werden.

Das letztendliche Ziel von Sicherheitstechnologie ist der Schutz sensibler Daten. Firewalls können heutzutage weder bei der Übertragung noch im Ruhezustand eine effiziente Identifizierung und Kontrolle ermöglichen, weshalb Organisationsdaten gefährdet sind. Ein weiterer entscheidender Nachteil liegt in der fehlenden Kapazität zur Überprüfung des mit SSL/TLS verschlüsselten Traffics, der inzwischen 90 % des Gesamtvolumens ausmacht.[1]

Zero Trust zur Verhinderung von Datenverlusten

Im Gegensatz zu Firewalls, die verschlüsselten Traffic ungeprüft weiterleiten, kann eine echte Zero-Trust-Plattform den gesamten – verschlüsselten und unverschlüsselten – Traffic innerhalb und außerhalb des Netzwerks untersuchen. Sie schließt Transparenzlücken und gewährleistet eine hundertprozentige Überprüfung, damit das Unternehmen zuverlässig vor Datenverlusten und Cyberbedrohungen geschützt ist. Eine Zero-Trust-Plattform kann alle Daten entschlüsseln und auf Unversehrtheit überprüfen. Basierend auf Kontextdaten (Geolocation, IP-Adresse, Gerätestatus, Uhrzeit usw.) werden User als vertrauenswürdig bzw. nicht vertrauenswürdig eingestuft und Verbindungen entsprechend genehmigt oder verweigert. Zum Schutz von Daten bei der Übertragung wendet die Plattform DLP-Richtlinien (Data Loss Prevention) an. Unabhängig vom Standort wird für alle User ein identisches Sicherheitsniveau ohne Beeinträchtigung der Anwendererfahrung gewährleistet.

Mit einer Inline-Zero-Trust-Lösung lässt sich die gesamte Shadow-IT zuverlässig erkennen und kontrollieren. Der Zugriff mit nicht verwalteten Geräten wird ohne Abstriche an Performance und User Experience durch Browser Isolation geschützt. Dadurch können webbasierte Bedrohungen abgewehrt und Unternehmensdaten effektiv geschützt werden. Browser Isolation bedeutet, dass Daten in Form von Pixeln aus einer isolierten Browsersitzung in eine Containerumgebung gestreamt werden. So wird die Verwendung von Privatgeräten (BYOD) ermöglicht, Datenverluste durch Herunterladen, Kopieren, Einfügen bzw. Drucken werden jedoch verhindert. Out-of-band-DLP und ATP-Funktionen (Advanced Threat Protection) unterstützen die Behebung riskanter Dateifreigaben und Erkennung von ruhender Malware in der Cloud. Zum Schutz von Cloud-Daten werden auch potenziell riskante Fehlkonfigurationen, Compliance-Verstöße und Fehler bei der Vergabe von Berechtigungen behoben. Kurz gesagt: Zero Trust bietet auch bei hohem Traffic-Volumen ein konsistentes, einheitliches Sicherheitsniveau für alle verschlüsselten und unverschlüsselten Daten im Ruhezustand und bei der Übertragung. Dabei spielt es keine Rolle, ob die betroffenen Anwendungen im Internet, über SaaS oder in öffentlichen Clouds bereitgestellt werden. Zero Trust unterstützt den Zugriff auf Anwendungen unabhängig vom Standort und Gerätetyp des Users.

Webbrowser als Sicherheitsrisiko

Seit 2014 hat der Anteil des verschlüsselten Traffics im Internet von 50 % auf heute 95 % zugelegt.[1] Der Beliebtheit von Webbrowsern als Angriffsziel hat dies keinen Abbruch getan – nach Angaben von Gartner laufen 98 % aller Angriffe über das öffentliche Internet und bei 80 % davon handelt es sich um Angriffe, die über Browser gegen Enduser ausgeführt werden. Durch Browser Isolation mit Tools wie Cloud Browser Isolation lassen sich diese Sicherheitsrisiken zumindest teilweise reduzieren. Insbesondere für den Zugriff auf Unternehmensressourcen über nicht verwaltete Geräte empfiehlt sich der Einsatz von Lösungen, die ohne Softwareinstallationen auf dem Endgerät des Users auskommen.

Zscaler gewährleistet die konsequente Umsetzung von Zero Trust

Die Zero Trust Exchange von Zscaler wird als Cloud-native Plattform in 150 Rechenzentren global bereitgestellt. Die weltweit größte Security Cloud gewährleistet standortunabhängig schnelle und sichere Verbindungen, sodass Mitarbeiter von überall mit jedem beliebigen Gerät sicher arbeiten und das Internet als Unternehmensnetzwerk nutzen können. Im Unterschied zu Firewalls und VPNs beruht die Zero Trust Exchange auf dem Prinzip der minimalen Rechtevergabe. Entsprechend wird keinem User und keiner Anwendung automatisch vertraut. Stattdessen werden Verbindungen basierend auf der Identität des Users sowie auf Kontextdaten genehmigt (Standort des Users, Sicherheitsstatus des Geräts, angeforderte Anwendung, Art der ausgetauschten Daten/Inhalte ...).

In der Praxis bedeutet das Folgendes: Die Zero Trust Exchange trennt im ersten Schritt die Verbindung, um eine gründliche Inhaltsprüfung des gesamten verschlüsselten und unverschlüsselten Traffics mit Daten- und Bedrohungsanalyse zu ermöglichen. Dann werden Zugriffsberechtigungen anhand von Useridentität, Gerätestatus sowie Unternehmensrichtlinien unter Berücksichtigung von Kontextdaten zum User, Gerät, der angeforderten Anwendung und dem Inhaltstyp überprüft. 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 erfahren

Auf der Produktseite der **Zero Trust Exchange** erhalten Interessenten weitere Informationen zum Zero-Trust-Konzept und den einschlägigen Lösungen und Leistungsangeboten von Zscaler.

Quellen

[1] *Google Transparenzbericht* https://transparencyreport.google.com/https/overview?hl=de
[2] *Zscaler-Umfrage zur Netzwerksicherheit (2020)*
[3] *Studie ESG Economic Validation (2021)*

Über Zscaler

Zscaler ermöglicht Organisationen eine sichere Transformation ihrer Netzwerke und Anwendungen für eine mobile Cloud-First-Welt. Zscaler verbindet Benutzer unabhängig von ihrem Gerät, Standort oder Netzwerk mit Anwendungen und Cloud-Services und bietet gleichzeitig umfassende Sicherheit und eine schnelle Nutzererfahrung. All dies ohne kostspielige, komplexe Gateway-Appliances.

zscaler™