Akamai

WHITEPAPER

Blueprint für die Umsetzung einer Zero-Trust-Architektur

Inhaltsverzeichnis

Einführung

Zero Trust ist seit 2009 ein Begriff, als Forrester Research zum ersten Mal für dieses Konzept warb und Organisationen warnte, dass die Zeit des ungehinderten Netzwerkzugriffs für alle Nutzer und Anwendungen, die den Netzwerkrand passieren, vorbei sei. Stattdessen sollte jeder Geräte-, Nutzer- und Netzwerkfluss überprüft werden, bevor vollständiger Zugriff gewährt wird. In den folgenden Jahren hat die Dringlichkeit, das Zero-Trust-Konzept umzusetzen, aufgrund vieler Faktoren zugenommen. Die COVID-19-Pandemie führte zu einem Anstieg der Zahl der Remotemitarbeiter, die außerhalb des Netzwerks arbeiten. Ransomware-Angriffe sind immer häufiger und ausgeklügelter geworden. Dadurch steigt die Wahrscheinlichkeit, dass ein Angreifer Ihre Abwehrmechanismen durchbricht und dabei kostspieligen Schaden anrichtet. Laut dem Bericht IBM Cost of a Data Breach 2022 erreichten die durchschnittlichen Kosten einer Datenschutzverletzung in den USA Rekordhöhen von 9,44 Millionen US-Dollar. Darüber hinaus haben die Zunahme vernetzter Geräte wie IoT-Geräte (Internet of Things) sowie zusätzliche Anforderungen für den Zugriff von Partnern und Kunden auf das Netzwerk die Angriffsfläche von Unternehmen insgesamt erheblich erweitert. Aufgrund dieser sich ständig verändernden Cybersicherheitslandschaft sind Anbieter von Netzwerk- und Sicherheitssoftware bestrebt, ihre bestehenden Produkte als Zero Trust zu vermarkten oder neue Produkte einzuführen, während Berater und Analysten laufend neue Akronyme und Marktdefinitionen in Umlauf bringen. Sicherheitsteams haben daher oft Schwierigkeiten, diese manchmal komplexen Konzepte nachzuvollziehen und Kaufentscheidungen zu treffen, die den Grundstein für eine Zero-Trust-Strategie legen.

Dieses Whitepaper soll Sicherheitsteams einen Plan für Investitionen in Zero-Trust-Technologie liefern, indem es die ersten Schritte definiert und die wichtigsten Unterscheidungsfaktoren erläutert.

Wie Remotearbeit und Cloudanwendungen das Verständnis von Netzwerksicherheit verändern

Wann, wie und wo Mitarbeiter ihre Arbeit erledigen, ist nicht mehr auf die vier Wände eines Büros beschränkt.

Das abgeschlossene Netzwerk gibt es also nicht mehr – zumindest nicht in irgendeiner erkennbaren Form. Viele Nutzer befinden sich heute nämlich mit hoher Wahrscheinlichkeit außerhalb Ihres Unternehmensnetzwerks. Gleichzeitig werden auch die Anwendungen, die sie als SaaS (Software as a Service) und Multicloud-Implementierungen verwenden, immer zahlreicher. Und bei hoch entwickelten und hartnäckigen Bedrohungen ist es sehr wahrscheinlich, dass Cyberkriminelle plötzlich uneingeschränkten Zugriff auf Ihre wertvollsten Ressourcen haben, wenn sie in Ihr Netzwerk eingedrungen sind. Wenn Sie kein umfassendes Zero-Trust-Programm aufgebaut haben, können Cyberkriminelle dann tun und lassen, was immer sie möchten.

Das ist nicht nur bloße Theorie. Der Beweis sind die Unmengen von kostspieligen Datenschutzverletzungen der letzten Jahre, von denen viele auf einen ausgenutzten Vertrauensstatus innerhalb des Netzwerks zurückzuführen sind.

Anwendungen, die für die Nutzung innerhalb eines Netzwerks entwickelt wurden, bieten oft nur unzureichende Sicherheit. Schließlich wurden sie entwickelt, als man noch davon ausging, dass nur autorisierte Mitarbeiter mit guten Absichten auf Ihr System zugreifen können. Welcher Entwickler ahnte damals schon, dass ganze Armeen von Hackern versuchen würden, Schwachstellen in den jeweiligen Internetanwendungen zu finden und auszunutzen?

Die Lösung für diese Herausforderungen auf dem Markt ist Zero Trust.

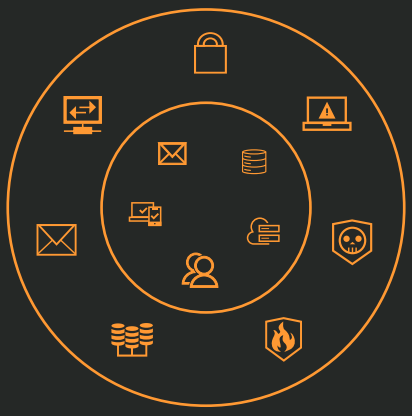
Eine Zero-Trust-Sicherheitsarchitektur

Das Prinzip hinter Zero Trust ist einfach, aber effektiv: Vertrauen sollte nichts mit dem Standort zu tun haben. Sie sollten niemandem einfach vertrauen, nur weil er sich innerhalb Ihrer Firewall befindet. Stattdessen sollte jede Aktion, unabhängig davon, wo sie stattfindet, nur dann als vertrauenswürdig eingestuft werden, wenn sie explizit zugelassen wurde. Letztendlich kann dann nur das geschehen, was auch geschehen *sollte*. Organisationen müssen implizites Vertrauen für alle Aktionen beseitigen, die nicht unbedingt erforderlich sind. Wenn Sie beispielsweise allen Nutzern Ihres Buchhaltungsteams Zugriff auf das Finanzsystem gewähren, obwohl nur wenige Nutzer ihn tatsächlich brauchen, entsteht ein unnötiges Risiko.

Als Nachweis dienen starke Authentifizierungs- und Autorisierungsmethoden, und eine Datenübertragung findet erst dann statt, wenn der Vertrauensstatus hergestellt wurde. Darüber hinaus dienen Analysen und Protokollierung dazu, Verhaltensregeln durchzusetzen und den Traffic durchgehend auf Bedrohungen zu überwachen.

Durch diese umfassende Änderung des Sicherheitsmodells lassen sich viele der im letzten Jahrzehnt aufgetretenen Probleme beheben. Angreifer können keine Schwachstellen mehr in Ihrer Firewall ausnutzen und dann vertrauliche Daten stehlen, nur weil sie es in Ihr Netzwerk geschafft haben. Denn das klassische Netzwerk gibt es nicht mehr. Es gibt nur Anwendungen und Nutzer, die vor jedem Zugriff authentifiziert und autorisiert werden müssen.

Herkömmliche Sicherheitsarchitektur



Moderne Realität

Wie können Unternehmen eine Zero-Trust-Architektur umsetzen?

Unternehmen müssen zunächst eine Strategie für ihre bestehende Umgebung entwickeln und herausfinden, ob und wann sie neue Mitarbeiter einstellen müssen. Wir könnten diesem wichtigen Schritt ein eigenes Whitepaper widmen. Die Produkte, die zur Umsetzung einer Zero-Trust-Strategie beitragen, sollten jedoch im Wesentlichen drei Ziele verfolgen:

1. **Vertrauen Sie niemanden, überprüfen Sie jeden.** „Niemandem vertrauen und jeden überprüfen" klingt in der Theorie viel einfacher als es ist. Wenn Sie einfach den Zugriff auf alle Systeme und Daten sperren, ist Ihr Netzwerk sicher. Die eigentliche Herausforderung besteht darin, kontinuierlich zu überprüfen, ohne dass es dabei zu massiven Geschäftsunterbrechungen kommt. Dies gilt insbesondere, da die meisten Systeme mit implizitem Vertrauen entwickelt wurden. Sie benötigen umfassende Transparenz und Kontrolle für alle Arten von Zugriff sowie einfache und praktische Mittel zur Durchsetzung und Verwaltung von Richtlinien.
2. **Gewähren Sie nach der Überprüfung nur minimalen Zugriff.** In einer Zero-Trust-Umgebung darf ein Nutzer nach erfolgreicher Überprüfung nur Zugriff auf die für seine Rolle erforderlichen Ressourcen erhalten.
3. **Überwachen Sie Ihre Umgebungen kontinuierlich auf Bedrohungen.** Die meisten Branchenexperten werden zustimmen, dass Zero Trust ein nie abgeschlossener Prozess ist. Cyberkriminelle unternehmen zusehends raffiniertere Angriffsversuche auf die Verteidigungsmechanismen von Unternehmen, weshalb der Zugriff auf Unternehmensressourcen kontinuierlich überwacht, überprüft und eingeschränkt werden muss. Einer der Vorteile eines Zero-Trust-Modells besteht darin, dass es sich nicht darauf konzentriert, was Cyberkriminelle tun, sondern darauf, was das Unternehmen selbst tut. Mit einer echten Zero-Trust-Richtlinie sind Angriffsketten gezwungen, alle Ressourcen, die Ihr Unternehmen zum reibungslosen Geschäftsablauf braucht, auf einmal zu beeinträchtigen. Sie werden jeden Angriff an irgendeinem Punkt in der Kette aufhalten können. Dazu gehört auch die Fähigkeit, Angriffe zu stoppen, die noch gar nicht stattgefunden haben. Auch wenn es ein Zero-Day-Angriff ist, mit Zero Trust können Sie ihn abwehren.

Die dunkle Seite von Zero Trust

Wenn ein Unternehmen jedoch mit der Implementierung von Zero Trust beginnt, muss es auch die Kehrseite dieses Misstrauens und der Zugangsbeschränkungen berücksichtigen. Ein grundlegender Aspekt von Zero Trust ist die Beschränkung des Zugriffs, hauptsächlich durch sogenannte Allow-Listen. Hier wird festgelegt, was passieren darf – alles andere wird standardmäßig abgelehnt. Wenn wir jedoch die Möglichkeiten von Cyberkriminellen einschränken, ihre Angriffskampagnen durchzuführen, kann es vorkommen, dass auch legitime Nutzer daran gehindert werden, ihre Arbeit zu erledigen. Außerdem können wiederholte Überprüfungen von Workloads und Geräten zu Verzögerungen und Frustrationen führen. Eine Zero-Trust-Strategie, die Mitarbeiter davon abhält, ihre Arbeit effektiv zu erledigen, ist überhaupt keine Strategie.

Eine starke Zero-Trust-Strategie muss daher ein Gleichgewicht zwischen Sicherheit und Zugriff schaffen. Außerdem muss ein Gleichgewicht zwischen dem, was tatsächlich erreicht werden kann, und den Ressourcen Ihres Sicherheitsteams gefunden werden – sowohl im Budget als auch im Personal.

Elemente von Zero Trust

Es ist über zehn Jahre her, dass Forrester das Konzept von Zero Trust zum ersten Mal umriss. Viele Unternehmen beginnen gerade erst mit der Umsetzung von Zero Trust und stehen nun vor einem unübersichtlichen Markt für Softwareprodukte. Einige Produkte gibt es schon seit Jahren und beziehen sich auf Teile einer Zero-Trust-Architektur, andere neue Produkte sind entstanden, und viele Softwareanbieter haben ihre Angebote einfach unter der Zero-Trust-Bezeichnung neu vermarktet. Viele Analysten und Branchenbeobachter betonen, dass Zero Trust kein Produkt sondern eine umfassende Strategie und kein Ziel sondern ein kontinuierlicher Prozess ist, doch diese oft wiederholten Behauptungen helfen denjenigen wenig, die mit Kaufentscheidungen für Zero-Trust-Lösungen konfrontiert sind. Im Gegenteil, sie können sogar noch mehr Verwirrung stiften.

Da es kein einzelnes Produkt gibt, das ein Unternehmen zu Zero Trust bringt, und Unternehmen unterschiedliche Prioritäten und Schwachstellen haben, ist der Ausgangspunkt für jedes Unternehmen ein anderer. Doch dank technologischer Fortschritte und Branchenkonsolidierung sind Unternehmen nun in der Lage, die erforderlichen Tools für die Implementierung einer Zero-Trust-Richtlinie aus einer Hand zu beziehen. Auch Analyseunternehmen erkennen das langsam. Gartner verfolgt das so genannte Secure Service Edge (SSE), eine Kombination aus Secure Web Gateways, Cloud Access Security Brokers und Zero-Trust-Netzwerkzugriff (Zero Trust Network Access, ZTNA). Im Bericht What Are Practical Projects for Implementing Zero Trust? erwähnt Gartner auch die Mikrosegmentierung (oder Segmentierung von Workload zu Workload) und empfiehlt, dass Unternehmen, die auf eine praktische Implementierung umstellen möchten, sich auf zwei Hauptthemen konzentrieren: Segmentierung von Nutzer zu Anwendung (ZTNA) und Segmentierung von Workload zu Workload (identitätsbasierte Segmentierung).

Auf ähnliche Weise gliedert IDC Zero Trust in die Komponenten Secure Access und Segmentierung und definiert es als umfassenden Überblick über neue und alte Technologien, die zum Schutz von Computersystemen, Ressourcen und Daten durch logische Segmentierung, Zugriffskontrolle und Bedrohungserkennung dienen.

Die meisten Experten erwarten, dass der Markt diesem Beispiel folgt und Anbieter zunehmend mehrere Zero-Trust-Anwendungen einführen. Dem Bericht Predicts 2022: Consolidated Security Platforms Are the Future von Gartner zufolge werden bis 2025 80 % der Unternehmen auf eine Strategie setzen, die den Zugriff auf Websites, Cloudservices und private Anwendungen auf der SSE-Plattform (Security Service Edge) eines einzigen Anbieters vereint.

Die Grundsätze von Zero Trust

Zero-Trust-Netzwerkzugriff

ZTNA ist ein grundlegender Bestandteil des Technologiestacks und wird manchmal mit dem Gesamtansatz für Zero Trust verwechselt. Secure Access ist der erste wichtige Schritt in einem Zero-Trust-Framework. Leider wird es, wie so viele Elemente dieses Prozesses, schnell komplexer als es klingt. Secure Access ist keine binäre Entscheidung. Die Bereitstellung des richtigen Zugriffsniveaus auf die richtige Anwendung für den richtigen Nutzer zum richtigen Zeitpunkt ist mit der zunehmenden Verteilung von Nutzern und Anwendungen viel komplizierter geworden. Tatsächlich ist ein Nutzer heute weit mehr als nur ein Mitarbeiter und kann auch Kunden, Lieferanten und Partner umfassen. Gleichzeitig gehören auch veraltete Anwendungen, SaaS oder Apps zu den Anwendungen und erfordern den Zugriff auf das Rechenzentrum, das Internet oder Cloudumgebungen.

Eine effektive ZTNA-Lösung überprüft die Identität des Nutzers und seines Geräts und verifiziert, ob der Nutzer unabhängig von seinem Standort auf die benötigten Anwendungen zugreifen kann. Dadurch wird der mögliche Angriffsbereich verringert und die Flexibilität und Überwachung verbessert. Jahrzehntelang verwendeten Unternehmen virtuelle private Netzwerke (VPNs), die von Identity Providers unterstützt werden, um Zugriff zu ermöglichen. Diese VPNs, die für eine andere Ära konzipiert wurden, reichen nicht mehr für die Größe und den Umfang der heutigen verteilten Belegschaft aus. ZTNA hat sich zu mehr als nur einem Ersatz für VPNs entwickelt und gewährt nun nicht nur durch die Überprüfung der Identität des Nutzers und seines Geräts Zugriff, sondern auch auf der Grundlage von Attributen wie Datum, Uhrzeit, Standort und Gerätestatus, um das angemessene Maß an Vertrauen zu gewährleisten.

Wichtige Überlegungen beim Kauf von Zero-Trust-Netzwerkzugriffslösungen

Wenn Unternehmen beginnen, ihre älteren VPNs durch ausgereiftere Identitätsmanagement-Lösungen zu ersetzen, gibt es eine Reihe von Bereichen, die berücksichtigt werden müssen. Moderne Lösungen sollten Identitäts- und Zugriffsmanagement, Anwendungssicherheit, Multi-Faktor-Authentifizierung (MFA) und Single Sign-on sowie transparente Verwaltung und Steuerung über eine einzige Schnittstelle kombinieren. Unternehmen, die Zero-Trust-Initiativen verfolgen, sollten nach Lösungen suchen, die ihren aktuellen Anforderungen gerecht werden, aber auch mit dem Unternehmen skaliert werden können. So wird die schnelle Integration von Mitarbeitern aus einer Fusion oder einem übernommenen Unternehmen, die Befähigung zur Fertigung oder Produktion in verschiedenen Märkten oder Regionen, einfaches Hinzufügen und Entfernen von Vertragspartnern für die Anpassung an immer neue Geschäftsanforderungen sowie der kosteneffiziente Umzug von Anwendungen in die Cloud ohne Verzicht auf Sicherheit ermöglicht.

Unternehmen sollten nach Lösungen suchen, die sich direkt in vorhandene Identitätsinfrastrukturen integrieren lassen, selbst wenn sie mehrere Verzeichnisse und Identity Service Provider umfassen. Dadurch kann der ZTNA-Service schnell bereitgestellt werden, ohne dass die vorhandene Identitätsinfrastruktur oder -architektur geändert werden muss.

Ein Blick an die Edge

Es gibt auch ein wichtiges Unterscheidungsmerkmal zwischen den Produkten auf dem Markt, das Sicherheitsteams auf jeden Fall berücksichtigen sollten, wenn sie Zero-Trust-Kaufentscheidungen treffen. Lösungen, die mit Edge-Cloud-Plattformen kombiniert werden, können zusätzliche Vorteile bieten, da sie als identitätsbasierter Proxy fungieren, der die Konnektivität von der Edge-Plattform ablenkt und somit sicherstellt, dass die gesamte Authentifizierung an der Edge und außerhalb des Rechenzentrums erfolgt. Einige Unternehmen nutzen zwar Architekturen mit Zugangs-Proxy, die innerhalb der DMZ laufen, nutzen dabei jedoch nicht die Fähigkeit der Cloud, Angriffe besser abzuwehren, Bandbreite für Caching bereitzustellen und bei Bedarf automatisch zu skalieren. Ein in die Cloud integrierter identitätsbasierter Proxy kann nach Bedarf skalieren, CPU-intensive Ressourcen ausführen und Angriffe abwehren. Darüber hinaus befindet er sich auf einer privaten IP-Adresse, die nicht direkt über das Internet erreichbar ist. Die Aktivitäten, die das höchste Maß an Performance und Sicherheit erfordern, finden an der Edge so nah wie möglich am Nutzer statt. Darüber hinaus wird der Pfad zu vertraulichen Daten für die Anwendung über einen Reverse-Anwendungstunnel bereitgestellt. So ist die IP des Netzwerks nicht sichtbar, und das Risiko volumetrischer Angriffe wird minimiert.

> **Lösungen, die mit Edge-Cloud-Plattformen kombiniert werden, können zusätzliche Vorteile bieten, da sie als identitätsbasierter Proxy fungieren.**

Überlegungen zur Multi-Faktor-Authentifizierung bei dem Erstellen eines Zero-Trust-Blueprints

Aufgrund der zunehmenden Remotearbeit und des Bedarfs an erweitertem Zugriff haben die meisten Unternehmen MFA eingeführt und verfügen bereits über irgendeine Lösung. Es ist jedoch wichtig, anzuerkennen, dass die Kombination aus unternehmensweitem Zugang und MFA größer ist als die Summe ihrer Teile. MFA ist ein zentraler Bestandteil des Zero-Trust-Konzepts, da für den Zugriff mehr als nur ein Passwort benötigt wird. Eine zweite Überprüfung ist notwendig, um sicherzustellen, dass die Anmeldedaten nicht missbraucht werden – einer der am häufigsten ausgenutzten Vertrauensbereiche. Man sollte ebenso bedenken, dass nicht alle MFA-Lösungen gleich effektiv sind.

Bei der Bewertung von MFA-Lösungen als Teil einer Zero-Trust-Strategie sollten Unternehmen nach Lösungen suchen, die folgende Eigenschaften bieten:

- Integration in Identitätsmanagement und Unternehmenszugriff
- Compliance mit FIDO2, um sicherzustellen, dass Nutzeranmeldedaten dezentral, isoliert und auf den persönlichen Geräten der Nutzer verschlüsselt werden, was besonders wichtig ist, um Phishing-Angriffe abzuwehren
- Nutzer können über ihr Smartphone verifiziert werden, ohne sich auf einen physischen Schlüssel verlassen zu müssen

Mikrosegmentierung

Es gibt keinen perfekten Zero-Trust-Zustand. Unweigerlich gibt es Lücken, die die hartnäckigsten Angreifer finden und ausnutzen können. Jeder umfassende Zero-Trust-Ansatz erfordert daher Mikrosegmentierung. Heutzutage haben die meisten Netzwerke entweder keine oder nur sehr wenige Segmente. Tatsächlich haben Unternehmen ihre kritischen Anwendungen traditionell mit Firewalls geschützt, doch dies erweist sich inzwischen aus einer Reihe von Gründen als schwierig. Firewalls erfordern im Grunde die Durchsetzung von Netzwerkrichtlinien, wodurch ein Engpass entsteht. Netzwerkverbindungen müssen eine Firewall durchlaufen, die schnell teuer werden kann, viele der Risiken des modernen Netzwerktraffics übersieht und extrem schwer anzupassen ist. Stattdessen setzen Unternehmen zunehmend auf softwarebasierte Mikrosegmentierung, die viele dieser arbeitsintensiven Prozesse vereinfacht.

Unterscheidungsmerkmale von Mikrosegmentierungs-lösungen

Obwohl dies eine Kernanforderung jeder Zero-Trust-Strategie ist, wurde die Mikrosegmentierung häufig getrennt von den ZTNA-Kernlösungen betrachtet. Und obwohl Mikrosegmentierung sowohl von Anbietern von Sicherheitsplattformen als auch als eigenständige Lösung verkauft wird, gibt es einige grundlegende Unterschiede, die Käufer verstehen müssen.

Wo kann Mikrosegmentierung eingesetzt werden? Potenzielle Käufer sollten sich unbedingt von Mikrosegmentierungslösungen fernhalten, die als Netzwerktools statt mit einem Security-First-Ansatz entwickelt wurden, oder solchen, die ausschließlich für lokale Systeme gedacht sind. Die heutigen Tools sollten in der Cloud, in lokalen Umgebungen, auf Geräten (einschließlich solcher, auf denen keine Agenten installiert werden können) und zwischen Containern in hybriden Umgebungen bereitgestellt werden können. Dazu ist in der Regel cloudbasierte Software erforderlich. Wenn eine Mikrosegmentierungslösung nur 80 % Ihrer Umgebung abdecken kann, reicht das nicht aus.

Wie viel Transparenz bietet Mikrosegmentierung? Obwohl Mikrosegmentierungslösungen den Zugriff einschränken, können zu viele Einschränkungen die Geschäftsprozesse unterbrechen und damit zu Frustration führen. Mikrosegmentierung erfordert ein tiefgreifendes Verständnis Ihrer Umgebung. Welche Server können auf welche Server zugreifen? Können Richtlinien zwischen einem Kubernetes-Cluster und einem Windows-2008-Server definiert werden? Viele Tools verfügen nicht über Agenten, die bis 2008 zurückreichen, oder sind nicht fortschrittlich genug, um Richtlinien für Kubernetes durchzusetzen. Ihre Mikrosegmentierungssoftware muss jedoch in der Lage sein, diese Art von Komplexität zu bewältigen, wenn Sie Zero Trust effektiv einsetzen wollen. Darüber hinaus müssen Käufer von Mikrosegmentierungslösungen die Granularität der Richtlinien berücksichtigen, die das Produkt unterstützt. Die meisten Systeme setzen Richtlinien auf Anwendungsebene über Ports und Prozesse hinweg durch. Ausgereiftere Produkte können Richtlinien auf der Microservice-Ebene durchsetzen. Angreifer können beispielsweise einige der Services von svchost (wie task scheduler) verwenden, um sich lateral durch das Netzwerk zu bewegen. Unternehmen können svchost jedoch nicht einfach blockieren, da es wichtige Ausgaben ausführt. Hier kann eine Mikrosegmentierungslösung, die Richtlinien auf der Mikroservice-Ebene durchsetzt, einen Unterschied bewirken.

Wie schwierig ist die Implementierung? Wie einfach es ist, die Richtlinien zu formulieren, die Sie jetzt benötigen, und – was ebenso wichtig ist – in der Zukunft benötigen werden, sollte bei jeder Mikrosegmentierungslösung eine zentrale Rolle spielen. Ganz gleich, ob es sich um Richtlinien für die ruhigen Zeiten der Planungsphase oder um Richtlinien für den Ernstfall handelt, wenn Ihre Umgebung angegriffen wird und Sie diese abriegeln müssen – die Engine, in die Sie investieren, muss beide Situationen problemlos unterstützen können. Das Erstellen von Allow-Listen in einem Mikrosegmentierungsprojekt kann für Sicherheitsteams beispielsweise eine große Herausforderung darstellen, da schnell einem benötigter Service oder einer benötigten Anwendung fälschlicherweise der Zugriff verweigert werden kann. Eine ausgeklügelte Mikrosegmentierungslösung sollte daher mit Vorlagen für Deny-Listen ausgestattet sein, die Teams schnell und einfach einführen können, um sofort Erfolge für das Projekt zu erzielen. Sobald dies erreicht ist, können Unternehmen den Weg hin zu einem umfassenden Schutz durch Allow-Listen fortsetzen, der Funktionen für die genaue Abhängigkeits- und kontextbezogene Bestandszuordnung umfasst.

> **Potenzielle Käufer sollten sich unbedingt von Mikrosegmentierungslösungen fernhalten, die als Netzwerktools statt mit einem Security-First-Ansatz entwickelt wurden, oder solchen, die ausschließlich für lokale Systeme gedacht sind.**

Secure Web Gateway

In einer Zero-Trust-Umgebung sind nicht nur Menschen nicht vertrauenswürdig, sondern auch das Internet an sich. Mitarbeiter benötigen Zugang zum Internet, und mit der zunehmenden Verteilung von SaaS und Apps, Cloudservices, Remotearbeit und IoT-Geräten wächst auch die Angriffsfläche des Unternehmens. So wird der Schutz von Unternehmen und Nutzern vor Bedrohungen wie Malware, Ransomware, Phishing und Datenextraktion zusehends komplexer. Unternehmen verfügen nur über begrenzte Ressourcen, um die Herausforderungen und die Komplexität von Kontrollpunkten sowie Sicherheitslücken in älteren lokalen Lösungen zu bewältigen.

Die Durchsetzung von Zero Trust zwischen einer Person und dem Internet erfordert ein Secure Web Gateway (SWG), was eine zentrale Funktion jeder Zero-Trust-Initiative ist.

Die wichtigsten Zero-Trust-Anforderungen für Secure Web Gateways

Obwohl es scheinbar einfach ist, gibt es Anforderungen, die Technologiekäufer berücksichtigen müssen, wenn sie in ein SWG investieren. Viele Unternehmen haben lokale SWGs implementiert, müssen diesen Schutz jedoch auf alle Nutzer unabhängig von ihrem Standort ausweiten. Ähnlich wie beim Identitätsmanagement verfügen Anbieter mit zuverlässigen Edge-Plattformen dank der intelligenten Funktionen der erweiterten Plattform in der Regel über eine höhere SWG-Sicherheit. Entscheidungsträger sollten diese Kernanforderungen sorgfältig prüfen.

DNS-Untersuchung. Anbieter sollten in der Lage sein, Untersuchungen aller Domains in Echtzeit und mit detaillierten Bedrohungsinformationen durchzuführen und schädliche Domains automatisch zu blockieren. Die Lösungen sollten außerdem über alle Ports und Protokolle hinweg aktiv sein, sodass Sie auch vor Malware schützen können, die sich nicht auf standardmäßige Webports und -protokolle verlässt. Die Qualität der DNS-Untersuchung kann je nach Anbieter sehr unterschiedlich sein, und Käufer sollten nach Personen suchen, die Erfahrung auf dem Markt und etablierten Kundenerfolg bieten.

URL-Untersuchung. Auch HTTP- und HTTPS-Anfragen müssen in Echtzeit geprüft und schädliche URLs automatisch blockiert werden.

Payload-Analyse. Alle Payloads sollten mithilfe verschiedener Techniken auf Malware überprüft werden, um umfassenden Zero-Day-Schutz vor schädlichen Dateien zu bieten. Idealerweise sollten die Signale Ihrer SWG-Produkte mit anderen Sicherheitsprodukten geteilt werden, um die Isolierung gefährdeter Ressourcen sowie die Beschränkung des Zugriffs darauf zu gewährleisten.

Bedrohungsüberwachung

Die letzte Komponente der Zero-Trust-Technologie ist die Bedrohungsüberwachung. Obwohl Zero Trust davon ausgeht, dass nichts implizit vertrauenswürdig ist und Ihr SWG Ransomware und Malware blockiert, müssen Unternehmen wachsam bleiben, um fortlaufende und aufkommende Angriffe sowie potenzielle Risiken (wie Fehlkonfigurationen oder allzu freizügige Zugriffsrechte) aufzudecken. Bei der Auswahl der passenden Software sollten Sicherheitsteams die folgenden drei Überlegungen für eine effektive Bedrohungsüberwachung berücksichtigen.

Wichtige Überlegungen

- **Effektive Algorithmen**
  Fortschrittliche Algorithmen, die nachweislich erfolgreich Anomalien der Nutzer- und Netzwerkaktivität erkennen und Analysen, Protokollanalysen und mehr ausführen, sollten Teil jedes Services zur Bedrohungsüberwachung sein.

- **Starke Signalerkennung**
  Obwohl Software und künstliche Intelligenz für die Bedrohungsüberwachung unverzichtbar sind, sollten die Entscheidungsträger von Zero Trust dennoch das interne Fachwissen der Anbieter bewerten, mit denen sie zusammenarbeiten. Die Services zur Bedrohungsüberwachung müssen in der Lage sein, gute und schlechte Signale voneinander zu trennen, um Ermüdungserscheinungen durch unnötige Warnmeldungen zu vermeiden, und bei Vorfällen sofortige Benachrichtigungen auszulösen. Unternehmen sollten außerdem regelmäßige Berichte mit Analysen aller maßgeblichen Angriffe erhalten.

- **Erfahrene Mitarbeiter**
  Sicherheitsteams sollten aus Personen mit aus verschiedenen Bereichen wie militärische Aufklärung, offensive Sicherheit, Incident Response und Data Science bestehen und rund um die Uhr verfügbar sein. Dies ist ein Bereich, in dem Content-Delivery-Anbieter einen erheblichen Vorteil bieten können. Die Erkenntnisse aus der Überwachung von Hunderten Terabyte pro Sekunde tragen zu einer einzigartigen Perspektive bei der Signalerkennung bei.

Erste Schritte

Eine Zero-Trust-Initiative ist nie abgeschlossen, daher lautet die Hauptfrage für diejenigen, die nach der passenden Software, Hardware und den richtigen Anforderungen an neue Mitarbeiter suchen, oft: „Mit welcher Technologie fangen wir an?“

Wie bei so vielen Dingen hängt die Antwort von den individuellen Bedürfnissen, Risikobewertungen und relativen Stärken und Schwächen eines Unternehmens ab. Für viele Branchenbeobachter besteht die Antwort darin, mit der Implementierung von ZTNA zu beginnen. Tatsächlich kann der Schutz des Unternehmens vor schädlichem North-South-Traffic ein guter Ausgangspunkt sein. Es besteht jedoch auch die Überzeugung, dass ein East-West-Ansatz mit Mikrosegmentierung, insbesondere softwaredefinierter Mikrosegmentierung, der bessere Weg ist.

Gute Gründe für Mikrosegmentierung

Wenn Sie wie die meisten Experten der Meinung sind, dass es keine perfekte Verteidigung gibt und ein schädlicher Angriff irgendwann zwangsläufig durch Ihre Abwehr gelangen wird, dann müssen Sie in der Lage sein, Ihre wertvollsten Ressourcen zu schützen. Genau das bietet Ihnen Mikrosegmentierung.

Viele Unternehmen zögern möglicherweise, eine Mikrosegmentierungslösung zu implementieren, weil sie unglaublich komplex wirken. Mikrosegmentierung ist jedoch kein Alles-oder-Nichts-Ansatz. Wie auch Zero Trust kann sie in mehreren Phasen durchgeführt werden. Unternehmen können damit beginnen, ihre wertvollsten Ressourcen zu identifizieren. Dabei sollten Sie sich auf das Wesentliche konzentrieren. Stellen Sie sicher, dass Ihr Unternehmen nicht zum

Erliegen kommt, wenn jemand in Ihr System eindringt. Die Bedeutung einer Ressource kann auf den Daten innerhalb dieser Ressource oder auf dem bereits vorhandenen Schutzniveau basieren. In vielen Fällen sind das Ihre älteren Systeme, da Sicherheitsanbieter sie nicht unterstützen.

Zweitens beseitigt die softwaredefinierte Mikrosegmentierung einen Großteil der wahrgenommenen Komplexität. Sie müssen sich nicht mehr mit der Hardware beschäftigen oder sich wiederholt mit Ihren Netzwerk- und Sicherheitsarchitekten in Verbindung setzen. Sie führen einfach die Software ein und verringern so die Einstiegsbarrieren deutlich.

Sobald eine Mikrosegmentierungsinitiative begonnen wurde, werden die frühen Vorteile klar und können dazu beitragen, den Rest des Projekts voranzutreiben. So haben Sie jetzt beispielsweise direkte Einblicke in das, was in Ihrer Umgebung passiert. Darauf haben Sie sofort Zugriff, auch wenn Sie noch keine Richtlinien durchgesetzt haben, und so erlangen Sie ein tieferes Verständnis für die Datenströme in Ihrem Netzwerk.

Sobald ein Unternehmen mit dem Ringfencing von Anwendungen beginnt, können wichtige Anwendungen schnell und einfach gesperrt werden, sodass sie nur über bestimmte Ports und Prozesse kommunizieren. Alternativ könnte es ein guter Einstieg sein, sich auf bedrohungsspezifische Richtlinien zu konzentrieren. Ausgereifte Mikrosegmentierungsplattformen verfügen über integrierte Funktionen für Deny-Listen. Das bedeutet, dass Sie schnell eine Richtlinie erstellen können, um unnötige Verbindungen zwischen Remote-Desktopservices und dem Internet zu stoppen. Unternehmen können so beispielsweise die Art von Schwachstelle, die zum Angriff auf die Colonial Pipeline geführt hat, schnell abwehren.

Unabhängig vom Ausgangspunkt ist der Schlüssel zu einem kontinuierlichen Zero-Trust-Prozess das Gleichgewicht. Ein erstklassiges Identitätsmanagement mit unzureichender Segmentierung oder unzureichendem Schutz des Webzugriffs bietet beispielsweise keine gute Sicherheit.

Plattform vs. Spezialisierte Tools

Wie bei vielen Technologieentscheidungen liegt auch beim Kauf von Zero-Trust-Software häufig die Wahl zwischen einzelnen spezialisierten Lösungen und einer Plattform, die mehrere Komponenten kombiniert. Die Auswirkungen von Zero Trust auf Sicherheitsteams, Integratoren, Architekten sowie Analysten und deren Anforderung, Richtlinien über mehrere Konsolen, verschiedene Agenten und mehrere Integrationen hinweg zu verwalten, sind ein überzeugendes Argument für Plattformlösungen. Dies gilt insbesondere in einem angespannten Arbeitsmarkt mit einem Mangel an qualifizierten Cybersicherheitsexperten. Die Verwaltung von Lösungen verschiedener Anbieter kann die Personalkosten erheblich erhöhen, da Lösungen, die nicht effektiv miteinander kommunizieren, Fehlalarme erzeugen, die Endnutzer belasten und zusätzlichen Support und Schulungen erfordern können.

Darüber hinaus erleichtert ein einzelner Plattformanbieter die einheitliche Implementierung von Zero Trust, ganz besonders wenn es um Support- und Vertragsverhandlungen geht.

> **Viele Unternehmen zögern möglicherweise, eine Mikrosegmentierungslösung zu implementieren, weil sie unglaublich komplex wirken.**

Zusammenfassung der Zero-Trust-Elemente

Wissen, wer Ihre Nutzer sind Überprüfung jedes Nutzers sicherstellen

Schutz Ihrer Ressourcen Alle Transaktionen authentifizieren/ autorisieren

Schutz Ihrer Nutzer Malware-Infektionen bei Nutzern verhindern

Fazit

Letztendlich erkennen die meisten Unternehmen, die sich mit dem Schutz vor Cyberangriffen befassen, die Notwendigkeit, so schnell wie möglich mit der Umstellung auf eine Zero-Trust-Architektur zu beginnen. Viele haben als Reaktion auf die Zunahme von Remotearbeit bereits allmählich oder plötzlich mit der Implementierung begonnen. Da Angreifer jedoch immer raffinierter werden, die Angriffsflächen größer werden und immer mehr Nutzer Remotezugriff fordern, wächst der Bedarf an einem umfassenden Portfolio von Anwendungen, die zusammenarbeiten.

Weitere Informationen zu den einzelnen Elementen des Zero-Trust-Ansatzes von Akamai erhalten Sie von einem unserer Experten.