WHITEPAPER

Kurzanleitung: Zero-Trust-Sicherheitstransformation

Akamai

Zusammenfassung

In der heutigen Geschäftswelt kann man sich nicht mehr auf die klassische Vorstellung von einem Netzwerk verlassen, bei der alle Personen außerhalb des Unternehmens-Kontrollbereichs schlechte Absichten verfolgen und alle Personen im Inneren ehrlich sind und gute Absichten haben. Aufgrund der umfassenden Einführung von SaaS-Anwendungen, der Migration auf cloudbasierte Architekturen, einer wachsenden Anzahl von Remotenutzern sowie der zunehmenden Verbreitung von BYOD-Geräten gehört die klassische Netzwerksicherheit der Vergangenheit an. Darüber hinaus sind beim klassischen Netzwerkschutz die Verwaltung von Anwendungs- und Sicherheitsrichtlinien sowie häufige Software-Upgrades erforderlich, was zu einem komplexeren Betrieb und einer noch höheren Belastung der IT-Teams führt. Angesichts der Tatsache, dass die Angriffsfläche beständig wächst und die IT-Ressourcen eine immer kompliziertere Netzwerkarchitektur verwalten müssen, agieren Cyberkriminelle zunehmend versierter und raffinierter, um Sicherheitsmaßnahmen zu umgehen. Diese besonderen Herausforderungen können nur mit einem strategischen Sicherheitsframework bewältigt werden.

Was ist Zero-Trust-Sicherheit und warum ist sie wichtig?

Ein Zero-Trust-Modell ersetzt die klassische Netzwerksicherheitsarchitektur. Es sorgt dafür, dass Sicherheits- und Zugriffsentscheidungen dynamisch auf der Grundlage von Identität, Gerät und Nutzerkontext durchgesetzt werden. Außerdem haben in einem Zero-Trust-Sicherheitsframework nur authentifizierte und autorisierte Nutzer und Geräte Zugriff auf Anwendungen und Daten. Gleichzeitig werden diese Anwendungen und Nutzer vor hochentwickelten Bedrohungen im Internet geschützt.

Wenn Sie Fortschritte auf Ihrem Weg hin zu Zero Trust machen und Ihre Nutzer, Anwendungen und die Zukunft Ihres Unternehmens schützen möchten, empfehlen wir Folgendes:

Gewähren Sie Nutzern nur Anwendungszugriff, keinen Netzwerkzugriff.

Ältere Technologien für den Remotezugriff wie Virtual Private Networks (VPNs) können die wachsenden Anforderungen der heutigen digitalen Unternehmen, die nicht über eine klassische Netzwerkarchitektur verfügen, nicht erfüllen. Das herkömmliche VPN stellt eine Bedrohung für die Unternehmenssicherheit dar, da es die Firewall von Natur aus durchlässig macht und somit uneingeschränkten Netzwerkzugriff ermöglicht. Sobald sich ein Angreifer im Netzwerk befindet, kann er lateral auf jedes System und jede Anwendung innerhalb des Netzwerks zuzugreifen und diese ausnutzen. Herkömmliche VPNs stellen nicht nur Sicherheitsrisiken für das Unternehmen dar, sondern sind darüber hinaus komplexe Lösungen, für die erhebliche IT-Ressourcen zur Hardware- und Softwareverwaltung erforderlich sind. Auch Wartung und Skalierung sind kostspielig.

Die Netzwerksegmentierung, die manchmal als Gegenmaßnahme für einen uneingeschränkten Zugriff angesehen wird, hat sich als teuer, schwierig zu implementieren und umständlich zu verwalten erwiesen. Und letztendlich wird dadurch nicht das Risiko verringert. Mit der Funktion „Alle zulassen“ sind laterale Bewegungen innerhalb des Netzwerks nach wie vor möglich. Der Ost-West-Traffic innerhalb eines Subnetzes wird durch die Netzwerksegmentierung zwar aufgeteilt, aber die horizontale Ausbreitung innerhalb desselben Subnetzes kann dadurch nicht gestoppt werden.

Um Ihr Unternehmen zu schützen und das Zero-Trust-Konzept umzusetzen, sollten Sie Nutzern nur Zugriff auf die Anwendungen gewähren, die sie für ihre Rolle benötigen. Dieser Zugriff muss auf Berechtigungen, Nutzeridentität, Gerätestatus, Authentifizierung und Autorisierung beruhen. Durch diese bewährten Methoden können Sie laterale Angriffe reduzieren und die Netzwerkgefährdung einschränken. Durch den Wegfall herkömmlicher VPNs lassen sich zudem das Nutzererlebnis verbessern, die Produktivität der Mitarbeiter steigern und die Anzahl der Helpdesk-Tickets senken. Und die Abkehr von Firewalls, Hardware und Software bedeutet niedrigere IT-Wartungskosten. Darüber hinaus verbessern reine Anwendungsberechtigungen die Governance und bieten Transparenz und Einblicke in den Zugriff auf Anwendungen, den Speicherort der Daten und die Art des Zugriffs auf diese Daten.

Gewähren Sie Nutzern nur Zugriff auf die von ihnen benötigten Anwendungen, wobei dieser Zugriff auf Berechtigungen, Nutzeridentität, Gerätestatus, Authentifizierung und Autorisierung beruhen muss.

Trennen Sie Ihre Netzwerkinfrastruktur vom öffentlichen Internet

Durch Offenlegung interner Anwendungen und der Zugriffsinfrastruktur für das Internet werden diese anfällig für DDoS-, SQL-Injection- und andere Angriffe auf Anwendungsebene. Cyberkriminelle setzen immer raffiniertere Maschen ein. Anhand fortlaufend weiterentwickelter Techniken scannen sie die Netzwerkkonfigurationen von Unternehmen und können so anfällige Anwendungen und wertvolle Daten ermitteln. Daher müssen Unternehmen die Anwendungs- und Zugriffsarchitektur vom öffentlichen Internet isolieren, damit sie nicht von Cyberkriminellen über offene Überwachungsports angegriffen werden kann. Wenn Cyberkriminelle das Netzwerk nicht finden oder nicht feststellen können, welche Anwendungen und Services das Zielgerät ausführt, können sie es auch nicht angreifen.

Aktivieren Sie WAF zum Schutz von Unternehmensanwendungen

Moderne Cyberangriffe sind äußerst zielgerichtet. Angreifer nutzen Social Engineering, z. B. E-Mails, Social Media, Instant Messaging und SMS, um Einzelpersonen mit für sie relevanten und personalisierten Nachrichten zu ködern. Cyberkriminelle suchen nach bestimmten Nutzern mit wünschenswerten Positionen im Unternehmen, Kenntnissen und Zugriffsebenen und starten dann Anwendungsangriffe, die speziell auf die Berechtigungen dieser Nutzer ausgerichtet sind.

Ein infizierter Computer wird häufig als „Zombiegerät" eingesetzt, mit dem dann ohne Wissen des Nutzers Angriffe auf angeblich hinter der Firewall geschützte Unternehmensanwendungen durchgeführt werden. Die meisten Unternehmen setzen zwar eine Web Application Firewall (WAF) ein, um ihre extern genutzten Anwendungen vor solchen Angriffen zu schützen, aber oft erstreckt sich dieser Schutz nicht auf Unternehmensanwendungen innerhalb des Netzwerks. Mithilfe einer WAF können interne Anwendungen und die zugehörigen Daten vor Attacken auf Anwendungsebene und Injection-Angriffen geschützt werden, wie z. B. SQL Injection, Malicious File Execution, Cross Site Request Forgery (CSRF) und Cross-Site Scripting.

Cyberkriminelle nehmen ein Gerät ins Visier, wandeln es in einen „Zombiecomputer" um und greifen damit angeblich hinter einer Firewall geschützte Anwendungen an.

Richten Sie Identität, Authentifizierung und Autorisierung vor der Zugriffsbereitstellung ein

Digitale Systeme gewähren jeder Person Zugriff, die das richtige Passwort eingibt, ohne dass die Identität verifiziert wird. Schwache Anmeldedaten und die Wiederverwendung von Passwörtern erhöhen die Angriffsfläche und das Risiko eines Unternehmens erheblich. In der heutigen Bedrohungslandschaft reicht es nicht mehr aus, sich nur auf eine einfache Authentifizierung wie einen Nutzernamen und ein Passwort zu verlassen. Die Multi-Faktor-Authentifizierung (MFA) bietet ein zusätzliches Maß an Verifizierung und Sicherheit und sorgt dafür, dass nur validierte Nutzer Zugriff auf geschäftskritische Anwendungen erhalten.

Multi-Faktor-Authentifizierung ist ein Muss. Schwache Anmeldeinformationen sowie die Wiederverwendung von Nutzernamen und Passwörtern in verschiedenen Anwendungen erhöhen die Angriffsfläche eines Unternehmens erheblich.

Sobald Nutzer über MFA authentifiziert und autorisiert wurden, können sie sich per Single Sign-on (SSO) mit ihren jeweiligen Anmeldedaten bei allen Anwendungen anmelden. Da die Nutzeridentität nicht mehr für jede Anwendung erneut bestätigt werden muss und es keine Synchronisierungsprobleme zwischen Anwendungen gibt, erhöht sich auch die Produktivität. Durch eine fortlaufende Entscheidungsfindung anhand einer Vielzahl von Signalen – einschließlich MFA und SSO für IaaS-, lokale und SaaS-Anwendungen – profitiert Ihr Unternehmen von einem erhöhten Schutz bei gleichzeitig komfortabler Anmeldung für Endnutzer.

Nutzen Sie Advanced Threat Protection zum Schutz vor Phishing, Zero-Day-Malware und DNS-basierter Datenextraktion

Obwohl die mehrschichtige Sicherheit in Unternehmen inzwischen weit verbreitet ist, erhalten Cyberkriminelle nach wie vor Zugriff auf Unternehmensdaten, indem sie vorhandene Sicherheitslücken einfach ausnutzen. Selbst mit Firewalls, Secure Web Gateways, Sandboxes, Intrusion-Prevention-Systemen und Endpoint-Antivirenlösungen sind Unternehmen nicht vor Phishing, Zero-Day-Malware und DNS-basierter Datenextraktion geschützt und werden zum leichten Opfer solcher Angriffe. Wie lässt sich dafür Abhilfe schaffen?

DNS ist ein häufig übersehener Vektor. Cyberkriminelle haben Malware entwickelt, die speziell auf die Ausnutzung dieser Sicherheitslücke ausgerichtet ist. Dabei werden vorhandene Sicherheitsebenen umgangen, um das Netzwerk zu infiltrieren und Daten zu stehlen. Die Implementierung einer zusätzlichen Sicherheitsebene, die das DNS-Protokoll nutzt, ist daher äußerst wichtig. Durch den Einsatz dieser ersten Abfragephase als Sicherheitskontrollpunkt kann eine DNS-Sicherheitslösung Cyberangriffe schon früh in der Kill Chain erkennen und stoppen und so das Unternehmen proaktiv schützen.

Unternehmen sollten das DNS-Protokoll als Sicherheitskontrollpunkt nutzen, um Cyberangriffe schon früh in der Kill Chain zu erkennen und zu stoppen.

Überwachen Sie Traffic und Aktivitäten im Internet

Unternehmen müssen immer davon ausgehen, dass sie in einer feindlichen Umgebung arbeiten. So lautet das Credo von Zero Trust. Daher dürfen Aktivitäten im Unternehmen nicht einfach blind zugelassen werden, sondern müssen unbedingt überprüft und bestätigt werden. Dazu benötigen Unternehmen einen Einblick in die Vorgänge in ihren Netzwerken, wobei genügend Traffic und Informationen bereitgestellt werden müssen, um relevante Vergleiche anzustellen.

Unternehmen müssen alle DNS-Anfragen von Geräten im und außerhalb des Unternehmensnetzwerks überwachen und überprüfen, ganz gleich, ob diese von Laptops, Mobiltelefonen, Desktops, Tablets, Gast-WLANs oder IoT-Geräten stammen. Nur so können sie sicherstellen, dass Anfragen nicht zu schädlichen oder inakzeptablen Websites führen. Außerdem müssen Unternehmen in der Lage sein, das Trafficverhalten im Hinblick auf verdächtige Aktivitäten zu überwachen und zu analysieren – beispielsweise die Kommunikation mit CnC-Servern (Command and Control) oder Datenextraktion – und das IT-Team bei entsprechenden Ereignissen sofort zu warnen. Ein Überblick über das globale Trafficvolumen und die Bedrohungstrends erleichtert es der IT-Abteilung, Unregelmäßigkeiten oder gefährliche Muster zu erkennen.

Unterstützen Sie die Integration mit SIEM (Security Information and Event Management) und die Orchestrierung mit RESTful APIs.

In Unternehmen werden möglicherweise Hunderte oder sogar Tausende von Anwendungen eingesetzt. Diese müssen per API konfiguriert werden, damit sie schnell in großen Mengen bereitgestellt werden können. Gleichzeitig muss das Festlegen von Richtlinienkontrollen für den Anwendungszugriff möglich sein. Dies ist eine wichtige Funktion in allen umfangreichen Anwendungsumgebungen, bei denen ein schneller Umstieg von einem herkömmlichen VPN-Zugriff auf einen anwendungsspezifischen Zugriff erfolgen soll. APIs werden sich in Unternehmen auch weiterhin durchsetzen, da diese aufgrund der zunehmenden Nutzung von DevSecOps nach Überwachungs- und Konfigurationsaufgaben suchen, die über RESTful API verfügbar sind. Außerdem werden Plug-ins benötigt, um Bedrohungs- und Ereignisdaten in das SIEM zu integrieren und so weitere Untersuchungen und Korrelationen durchführen zu können. Ein skalierbares System muss zudem in Plattformen zur Workflow-Automatisierung und zur Abwehr von Bedrohungen integriert sein, sodass es mit Endpoint-Erkennungs- und Reaktionslösungen von Drittanbietern zusammenarbeitet.

Fazit

Die digitale Transformation ist heute Realität und Unternehmen müssen ein Zero-Trust-Sicherheitsmodell einführen, um das Geschäft erfolgreich weiterzuentwickeln und Innovation und Flexibilität zu ermöglichen, ohne die Sicherheit zu beeinträchtigen. Ein fortschrittlicher Bedrohungsschutz, Anwendungsbeschleunigung, MFA und SSO für alle Anwendungen – ob SaaS, lokal oder IaaS – sind einige der Hauptvorteile, die der Betrieb in einer Zero-Trust-Umgebung mit sich bringt. Ein Zero-Trust-Sicherheitsmodell ermöglicht die Orchestrierung über API sowie die Integration in SIEM- und Workflow-Automatisierungsplattformen und sorgt so für Transparenz bei Nutzern und Anwendungen. Gleichzeitig ist die Bereitstellung in großem Umfang in einem Bruchteil der Zeit möglich.

Akamai kann Sie bei der Entwicklung Ihres Netzwerks und Ihrer Sicherheitslösungen unterstützen. Führen Sie anhand von sieben Fragen eine Zero-Trust-Bewertung durch, und finden Sie heraus, ob Ihr Unternehmen für die Einführung eines Zero-Trust-Sicherheitsframeworks gerüstet ist. Anschließend erhalten Sie Informationen zu den nächsten Schritten für die Transformation Ihres Netzwerks. Oder besuchen Sie akamai.com/3waystozerotrust, um Ressourcen für einen schnellen Start abzurufen.

Akamai

Akamai stellt sichere digitale Erlebnisse für die größten Unternehmen der Welt bereit. Die Intelligent Edge Platform umgibt alles – vom Unternehmen bis zur Cloud –, damit unsere Kunden und ihre Unternehmen schnell, intelligent und sicher agieren können. Führende Marken weltweit setzen auf die agilen Lösungen von Akamai, um die Performance ihrer Multi-Cloud-Architekturen zu optimieren. Akamai hält Angriffe und Bedrohungen fern und bietet im Vergleich zu anderen Anbietern besonders nutzernahe Entscheidungen, Anwendungen und Erlebnisse. Das Akamai-Portfolio für Website- und Anwendungsperformance, Cloudsicherheit, Unternehmenszugriff und Videobereitstellung wird durch einen herausragenden Kundenservice, Analysen und Rund-um-die-Uhr-Überwachung ergänzt. Warum weltweit führende Unternehmen auf Akamai vertrauen, erfahren Sie unter akamai.de, im Blog blogs.akamai.com/de oder auf Twitter unter @AkamaiDACH sowie @Akamai. Unsere globalen Standorte finden Sie unter akamai.de/locations. Veröffentlicht: Juni 2019