

Akamai implementiert das Zero-Trust-Sicherheitsmodell - ganz ohne VPN



Hintergrund

Das öffentliche Internet und SaaS-Anwendungen werden immer geläufiger und die Angriffsflächen ändern sich ständig. Daher wird es zunehmend unpraktisch, den Zugriff auf Anwendungen abhängig vom Standort zu gewähren. Die Anforderungen an die Konnektivität und eine zunehmende Menge an Daten üben zudem einen nie da gewesenen Druck auf die Netzwerkinfrastruktur aus. Ältere Lösungen können da nicht mithalten, vor allem, da Mitarbeiter vollständige Mobilität sowie schnellen und zuverlässigen Zugriff auf Unternehmensanwendungen erwarten - überall und jederzeit. Unternehmen müssen sich weiterentwickeln, um den sich ändernden Anforderungen der heutigen IT- und Geschäftsumgebungen gerecht zu werden.

Geschäftssituation

Die IT-Abteilung von Akamai war der Ansicht, dass ein netzwerkbasierter Ansatz für Sicherheit und Zugriff nicht mehr ausreichte, um die Ressourcen des Unternehmens zu schützen. Herkömmliche VPNs bergen Sicherheitslücken: Eines der größten Risiken ist der unbefugte Remotezugriff auf vertrauliche Daten und der Zugriff auf alle Anwendungen im Unternehmensnetzwerk von jedem authentifizierten Gerät aus. Dieser Ansatz für den Remotezugriff bringt unnötige Sicherheitsrisiken mit sich. Mit VPN können im Allgemeinen alle Nutzer auf dieselben Anwendungen zugreifen.

Akamai entschied sich für die Einführung einer Zero-Trust-Sicherheitsstrategie, die das herkömmliche Unternehmens-VPN überflüssig macht und von einem klassischen Netzwerksicherheitsmodell Abstand nimmt. Das Ziel bestand darin, die Unternehmensanwendungen und -daten von Akamai zu schützen, laterale Bewegungen im Unternehmensnetzwerk zu verhindern und gleichzeitig ein verbessertes Nutzererlebnis zu bieten.

 Das Ziel bestand darin, die Unternehmensanwendungen und -daten von Akamai zu schützen, laterale Bewegungen im Unternehmensnetzwerk zu verhindern und gleichzeitig das Nutzererlebnis zu verbessern.

Im Rahmen der Zero-Trust-Transformation hat Akamai eine Reihe von Grundprinzipien aufgestellt:

- Umstellung auf eine Umgebung ohne klassische Netzwerkarchitektur, in der das Internet zum Unternehmensnetzwerk wird
- Jedes Büro muss ein WLAN-Hotspot werden
- Der Zugriff auf Anwendungen wird dynamisch und kontextbezogen gewährt. Grundlage dafür sind Identität, Umgebungs faktoren wie Standort und Tageszeit sowie Gerätesignale wie clientseitige Zertifikate oder Compliance der Geräte mit den Sicherheitsrichtlinien des Unternehmens.

Das IT-Team von Akamai hat außerdem die Sicherheitsrichtlinien aktualisiert, damit sie den Grundsätzen von Zero Trust entsprechen. Grundsätzlich ist kein Computer oder Nutzer vertrauenswürdig. Dieser Ansatz kam durch die Suche nach kostengünstigen Technologien zustande, die Mobilität, verbesserte Sicherheit, flexiblen Zugriff und Virtualisierung unterstützen und gleichzeitig die einfache Handhabung der Cloud nutzen.

Problempunkte

- Mitarbeiter an unterschiedlichen Standorten**
Die weltweit verstreute und vielfältige Belegschaft von Akamai, bestehend aus Vollzeitmitarbeitern, Auftragnehmern und Partnern, benötigte einen leistungsstarken Anwendungszugriff.
- Mobilgeräte**
Eine wachsende Anzahl von Geräten und Gerätetypen benötigte Zugriff auf Unternehmensanwendungen.
- Übernahmen**
Die Komplexität und Kosten dafür, neu übernommenen Mitarbeitern Zugriff auf Unternehmensanwendungen zu gewähren, nahmen zu.
- Verschiedene Anwendungen**
Die Vermeidung von Betriebsunterbrechungen und Datenverlusten durch Angriffe war von höchster Bedeutung, unabhängig von der Art der Anwendungen (lokal, IaaS und SaaS).
- Helpdesk-Tickets**
Die IT-Ressourcen von Akamai wurden zunehmend für die Fehlerbehebung beim Remote-, Auftragnehmer- und Partnerzugriff auf interne Anwendungen in Anspruch genommen.
- Architekturmanagement**
Die Vielfalt an Geräten und die zunehmende Anzahl und Größe von Last-Mile-Links sorgen dafür, dass das Netzwerk komplexer und teurer wird, die administrativen Anforderungen steigen und die Anwendungsperformance leidet.
- Latenz**
Bestehende Architekturen und VPN-Verbindungen führen zu langsamem und inkonsistentem Anwendungszugriff.

Lösung

Die IT-Abteilung von Akamai führte Enterprise Application Access ein – eine cloudbasierte Zugriffslösung, die das VPN vollständig ersetzt. Sie isoliert das Unternehmensnetzwerk mithilfe von „Dial-out only“-Zugriff auf Anwendungen hinter der Firewall. Mit der Technologie von Akamai basiert der Anwendungszugriff – unabhängig von den Hosting-Standorten der Anwendungen (lokal, IaaS, SaaS) – ausschließlich auf Berechtigungen, Identität, Authentifizierung und Autorisierung pro Anwendung. Durch den Einsatz von Enterprise Application Access für Anwendungszugriff und -kontrolle ermöglicht Akamai Agilität, Einfachheit und ein besseres Nutzererlebnis für alle Mitarbeiter, einschließlich der IT- und Sicherheitsteams.

Der Zugriff basiert ausschließlich auf Berechtigungen, Identität, Authentifizierung und Autorisierung pro Anwendung, unabhängig davon, wo Anwendungen gehostet werden (lokal, IaaS, SaaS).



Für zusätzliche Sicherheit nutzt das IT-Team von Akamai Kona Site Defender, die Web Application Firewall von Akamai, in Verbindung mit Enterprise Application Access. So werden interne Anwendungen vor SQL-Injection-Angriffen und anderen Insider-Bedrohungen durch zuvor „vertrauenswürdige“ Hosts geschützt. Dadurch wird das Risiko weiter verringert und die allgemeine Sicherheitslage von Akamai verbessert sich. Dank Enterprise Application Access in Kombination mit Ion – der Performanceoptimierungsengine von Akamai – kann das IT-Team von Akamai den Endnutzern nun unabhängig von ihrem Gerät, Netzwerk und geografischen Standort ein erstklassiges Webanwendungserlebnis bieten.

Der Ansatz von Akamai senkt die Kosten und die Komplexität, die normalerweise mit der Sicherung des Zugriffs auf Anwendungen verbunden sind. Anstatt zu versuchen, den Remotezugriff verschiedener Endpunkte auf das Unternehmensnetzwerk zu kontrollieren oder zu beschränken, war es für Akamai sinnvoller, eine Lösung zu implementieren, mit der die IT den Zugriff überwachen und nur für die Anwendungen gewähren kann, die tatsächlich benötigt werden. Der Umstieg aller Mitarbeiter vom VPN und Unternehmensnetzwerk und die Verwendung eines Zero-Trust-Ansatzes sorgen für Transparenz und Kontext des gesamten Traffics (aller Nutzer, Geräte, Standorte und Anwendungen). Damit hat das Unternehmen nicht nur die Risiken deutlich verringert, sondern auch den Bereitstellungsprozess für Unternehmensanwendungen optimiert.

Die Nutzung des Gerätetestatus für dynamische Zugriffentscheidungen ist eine weitere wichtige Komponente der Umstellung auf ein Zero-Trust-Modell bei Akamai. Der Gerätetestatus ergänzt und verbessert vorhandene Authentifizierungs-, Autorisierungs- und Zugriffskontrollregeln sowie Reportingfunktionen, da er zusätzlichen Kontext und ein weiteres Signal bereitstellt. So kann das Unternehmen jederzeit dynamische Entscheidungen über den Anwendungszugriff treffen.

Akamai implementiert das Zero-Trust-Sicherheitsmodell – ganz ohne VPN: Akamai-Fallstudie

Problempunkte

- **Mitarbeiter an unterschiedlichen Standorten**
Die weltweit verstreute und vielfältige Belegschaft von Akamai, bestehend aus Vollzeitmitarbeitern, Auftragnehmern und Partnern, benötigte einen leistungsstarken Anwendungszugriff.
 - **Mobilgeräte**
Eine wachsende Anzahl von Geräten und Gerätetypen benötigte Zugriff auf Unternehmensanwendungen.
 - **Übernahmen**
Die Komplexität und Kosten dafür, neu übernommenen Mitarbeitern Zugriff auf Unternehmensanwendungen zu gewähren, nahmen zu.
 - **Verschiedene Anwendungen**
Die Vermeidung von Betriebsunterbrechungen und Datenverlusten durch Angriffe war von höchster Bedeutung, unabhängig von der Art der Anwendungen (lokal, IaaS und SaaS).
 - **Helpdesk-Tickets**
Die IT-Ressourcen von Akamai wurden zunehmend für die Fehlerbehebung beim Remote-, Auftragnehmer- und Partnerzugriff auf interne Anwendungen in Anspruch genommen.
 - **Architekturnagement**
Die Vielfalt an Geräten und die zunehmende Anzahl und Größe von Last-Mile-Links sorgen dafür, dass das Netzwerk komplexer und teurer wird, die administrativen Anforderungen steigen und die Anwendungsperformance leidet.
 - **Latenz**
Bestehende Architekturen und VPN-Verbindungen führen zu langsamem und inkonsistentem Anwendungszugriff.

Lösung

Die IT-Abteilung von Akamai führte Enterprise Application Access ein – eine cloudbasierte Zugriffslösung, die das VPN vollständig ersetzt. Sie isoliert das Unternehmensnetzwerk mithilfe von „Dial-out only“-Zugriff auf Anwendungen hinter der Firewall. Mit der Technologie von Akamai basiert der Anwendungszugriff – unabhängig von den Hosting-Standorten der Anwendungen (lokal, IaaS, SaaS) – ausschließlich auf Berechtigungen, Identität, Authentifizierung und Autorisierung pro Anwendung. Durch den Einsatz von Enterprise Application Access für Anwendungszugriff und -kontrolle ermöglicht Akamai Agilität, Einfachheit und ein besseres Nutzererlebnis für alle Mitarbeiter, einschließlich der IT- und Sicherheitsteams.

Der Zugriff basiert ausschließlich auf Berechtigungen, Identität, Authentifizierung und Autorisierung pro Anwendung, unabhängig davon, wo Anwendungen gehostet werden (lokal, IaaS, SaaS).



Für zusätzliche Sicherheit nutzt das IT-Team von Akamai Kona Site Defender, die Web Application Firewall von Akamai, in Verbindung mit Enterprise Application Access. So werden interne Anwendungen vor SQL-Injection-Angriffen und anderen Insider-Bedrohungen durch zuvor „vertrauenswürdige“ Hosts geschützt. Dadurch wird das Risiko weiter verringert und die allgemeine Sicherheitslage von Akamai verbessert sich. Dank Enterprise Application Access in Kombination mit Ion - der Performanceoptimierungsengine von Akamai - kann das IT-Team von Akamai den Endnutzern nun unabhängig von ihrem Gerät, Netzwerk und geografischen Standort ein erstklassiges Webanwendungserlebnis bieten.

Der Ansatz von Akamai senkt die Kosten und die Komplexität, die normalerweise mit der Sicherung des Zugriffs auf Anwendungen verbunden sind. Anstatt zu versuchen, den Remotezugriff verschiedener Endpunkte auf das Unternehmensnetzwerk zu kontrollieren oder zu beschränken, war es für Akamai sinnvoller, eine Lösung zu implementieren, mit der die IT den Zugriff überwachen und nur für die Anwendungen gewähren kann, die tatsächlich benötigt werden. Der Umstieg aller Mitarbeiter vom VPN und Unternehmensnetzwerk und die Verwendung eines Zero-Trust-Ansatzes sorgen für Transparenz und Kontext des gesamten Traffics (aller Nutzer, Geräte, Standorte und Anwendungen). Damit hat das Unternehmen nicht nur die Risiken deutlich verringert, sondern auch den Bereitstellungsprozess für Unternehmensanwendungen optimiert.

Die Nutzung des Gerätetestatus für dynamische Zugriffsentscheidungen ist eine weitere wichtige Komponente der Umstellung auf ein Zero-Trust-Modell bei Akamai. Der Gerätetestatus ergänzt und verbessert vorhandene Authentifizierungs-, Autorisierungs- und Zugriffskontrollregeln sowie Reportingfunktionen, da er zusätzlichen Kontext und ein weiteres Signal bereitstellt. So kann das Unternehmen jederzeit dynamische Entscheidungen über den Anwendungszugriff treffen.

AKAMAI-FALLSTUDIE



Akamai implementiert das Zero-Trust-Sicherheitsmodell – ganz ohne VPN: Akamai-Fallstudie

Geschäftliche Vorteile des Umstiegs auf Zero-Trust-Sicherheit

- Minimale Risiken, da nur Zugriff auf die erforderlichen Anwendungen gewährt wird - nicht auf das gesamte Unternehmensnetzwerk
- Weniger Netzwerkkomplexität, die mit älteren Technologien zusammenhängt, einschließlich Zurückleiten des VPN-Traffics an ein zentrales Rechenzentrum
- Höhere Produktivität durch optimierten Zugriff für die Mitarbeiter von Akamai und für Dritte
- Niedrigere Kosten für IT-Geräte und -Prozesse, die damit verbunden sind, Mitarbeitern neu übernommener Unternehmen Zugriff zu gewähren

- Automatisierung, Orchestrierung, Transparenz und Analyse von Workloads, Netzwerken, Personen und Geräten zur Sicherung von Daten
- Besseres Nutzererlebnis auf verschiedenen Geräten, einschließlich Mobilgeräten, mit schnellerer und zuverlässigerer Anwendungsbereitstellung
- Niedrigere Kosten durch effizientere Zuweisung von IT-Ressourcen - weniger Zeitaufwand für die Aktualisierung, Verwaltung und Wartung von Hardware und Software bedeutet mehr Zeit für strategische Ziele
- Weniger Helpdesk-Anfragen zum Anwendungszugriff

Besuchen Sie akamai.com/zerotrust und erfahren Sie mehr darüber, wie Ihr Unternehmen von einem Zero-Trust-Sicherheitsmodell profitieren kann. Oder [wenden Sie sich an einen Sicherheitsspezialisten von Akamai](#), um einen individuellen Maßnahmenplan für die Sicherheitstransformation aufzustellen.

Was ist Enterprise Defender?

Enterprise Defender nutzt die Akamai Intelligent Edge Platform, um Schutz für alle Unternehmensanwendungen und -nutzer und somit größtmögliche Sicherheit zu bieten und die Komplexität zu verringern, ohne dabei die Performance zu beeinträchtigen. Mit dieser Lösung können Sie sicher auf Anwendungen zugreifen, die in Ihrer Kontrolle liegen, und gleichzeitig die Risiken verringern, die mit dem Zugriff Ihrer Nutzer auf Anwendungen verbunden sind, die sich Ihrer Kontrolle entziehen.

Enterprise Defender umfasst die folgenden Funktionen in einem nutzerfreundlichen Abonnementservice pro Nutzer und Monat:

Malwareschutz: Das Secure Internet Gateway (SIG) von Akamai erkennt und blockiert proaktiv gezielte Bedrohungen wie Malware, Ransomware, Phishing, DNS-Datenextraktion und fortschrittliche Zero-Day-Angriffe.

Sicherer Anwendungszugriff: Akamai stellt sicher, dass nur autorisierte Nutzer und Geräte Zugriff auf die von ihnen benötigten Unternehmensanwendungen haben, und nicht auf das gesamte Netzwerk.

Web Application Firewall: Akamai bietet umfassenden Schutz für wichtige Webanwendungen vor den größten und komplexesten DDoS- und Webanwendungsangriffen.

Anwendungsbeschleunigung: Akamai ermöglicht Unternehmen die Bereitstellung schneller, zuverlässiger und sicherer Anwendungen - und das auch noch kostengünstig. Die Funktionen zur Anwendungsbereitstellung befinden sich an der Edge - nahe an den Nutzern, der Cloud und lokalen Workloads. Überall auf der Welt.

Enterprise Defender ist die ideale Kombination von Malware-Schutz mit adaptivem Anwendungszugriff, Sicherheit und Beschleunigung in einem nutzerfreundlichen Sicherheitsservice an der Edge.



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 www.akamai.com, im Blog blogs.akamai.com oder auf Twitter unter [@Akamai](https://twitter.com/Akamai) sowie [@Akamai](https://twitter.com/Akamai). Unsere globalen Standorte finden Sie unter www.akamai.com/locations. Veröffentlicht: Juli 2019

Akamai implementiert das Zero-Trust-Sicherheitsmodell - ganz ohne VPN: Akamai-Fallstudie