Come Akamai ha implementato un modello di sicurezza Zero Trust senza una VPN

Background

Con il prevalere dell'Internet pubblico e delle applicazioni SaaS insieme al continuo cambiamento delle superfici soggette agli attacchi, concedere l'accesso in base alla posizione diventa sempre più impraticabile. Anche le richieste di connettività e l'utilizzo intensivo di dati esercitano una pressione senza precedenti sull'infrastruttura di rete. Le soluzioni legacy non riescono a stare al passo, soprattutto perché i lavoratori si aspettano una mobilità totale, nonché un accesso rapido e affidabile alle applicazioni aziendali, ovunque si trovino. Le aziende devono evolversi per soddisfare le mutevoli esigenze degli odierni ambienti IT e aziendali.

La situazione aziendale

Il reparto IT di Akamai riteneva che un approccio alla sicurezza e all'accesso incentrato sulla rete non fosse più sufficiente per proteggere le risorse aziendali. Le VPN tradizionali presentano risvolti negativi per la sicurezza, incluso il crescente rischio di accesso remoto non autorizzato ai dati sensibili e di accesso a tutte le applicazioni presenti sulla rete aziendale da qualsiasi dispositivo autenticato. Questo approccio all'accesso remoto crea inutili rischi per la sicurezza; con la VPN, ogni utente può generalmente accedere alle stesse applicazioni a cui può accedere qualsiasi altro utente.

Akamai ha deciso di adottare una strategia di sicurezza Zero Trust in grado di eliminare la tradizionale VPN aziendale, abbandonando un modello di sicurezza basato sul perimetro. L'obiettivo era proteggere le applicazioni e i dati aziendali di Akamai ed evitare il movimento laterale sulla rete aziendale, fornendo, al contempo, una user experience migliorata.

L'obiettivo era proteggere le applicazioni e i dati aziendali di Akamai ed evitare il movimento laterale sulla rete aziendale, migliorando, al contempo, la user experience.

Akamai ha basato la trasformazione Zero Trust su un insieme di principi fondamentali:

- *Passaggio a un ambiente meno perimetrale, in cui Internet diventa la rete aziendale*
- *Ogni ufficio deve diventare un hotspot Wi-Fi*
- *L'accesso alle applicazioni viene concesso in modo dinamico e contestuale in base all'identità, a fattori ambientali, quali la posizione e l'orario del giorno, e ai segnali del dispositivo, ad esempio certificati lato client o conformità del dispositivo a policy di sicurezza aziendali*

Il reparto IT di Akamai ha, inoltre, aggiornato le linee guida sulla sicurezza allineandole ai principi del modello Zero Trust: nessun dispositivo o utente va considerato automaticamente attendibile. Questo approccio era basato sulla ricerca di tecnologie convenienti in grado di supportare mobilità, sicurezza avanzata, accesso flessibile e virtualizzazione, sfruttando, al contempo, la semplicità del cloud.

Problematiche

- ***Forza lavoro distribuita***
  La forza lavoro di Akamai diversificata, distribuita a livello globale e composta da dipendenti a tempo pieno, collaboratori e partner richiedeva l'accesso ad applicazioni altamente funzionanti
- ***Dispositivi mobili***
  Un crescente numero di dispositivi anche di vario tipo doveva accedere alle applicazioni aziendali
- ***Acquisizioni***
  Fornire ai neoassunti l'accesso alle applicazioni aziendali stava aumentando in termini di complessità e costi
- ***Applicazioni diversificate***
  La prevenzione delle interruzioni delle attività aziendali e della perdita di dati derivanti dagli attacchi era di vitale importanza, indipendentemente dal tipo di applicazione utilizzata (in sede, IaaS e SaaS)
- ***Ticket di assistenza all'help desk***
  Le risorse IT di Akamai venivano sempre più rallentate dalla risoluzione di problemi associati all'accesso alle applicazioni interne da remoto e da parte di collaboratori e partner
- ***Gestione dell'architettura***
  La diversità dei dispositivi e il numero e le dimensioni crescenti dei collegamenti dell'ultimo miglio stavano aumentando la complessità e i costi della rete, incrementando i requisiti amministrativi e influenzando negativamente le performance delle applicazioni.
- ***Latenza***
  Le architetture esistenti e la connettività VPN hanno causato il rallentamento e l'incoerenza dell'accesso alle applicazioni

Soluzione

Il reparto IT di Akamai ha adottato Enterprise Application Access per la transizione dalla VPN. Questa soluzione di accesso basata sul cloud blocca la rete aziendale con un accesso esclusivamente di tipo "dial-out" alle applicazioni che si trovano dietro il firewall. Con la tecnologia di Akamai, l'accesso alle applicazioni, indipendentemente dalla posizione in cui le applicazioni vengono ospitate (in sede, IaaS, SaaS), è basato solo sui diritti, sull'identità, sull'autenticazione e sull'autorizzazione per singola applicazione. Utilizzando Enterprise Application Access per l'accesso e il controllo specifici per le applicazioni, Akamai offre flessibilità, semplicità e una migliore user experience all'intera forza lavoro, inclusi i team IT e addetti alla sicurezza.

L'accesso è basato esclusivamente sui diritti, sull'identità, sull'autenticazione e sull'autorizzazione per singola applicazione, indipendentemente dalla posizione di hosting dell'applicazione (in sede, IaaS, SaaS).

Per una maggiore sicurezza, il reparto IT di Akamai ha utilizzato Kona Site Defender, la soluzione WAF (Web Application Firewall) di Akamai in combinazione con Enterprise Application Access per proteggere le applicazioni interne dagli attacchi SQL injection e altre minacce ritenute in precedenza "affidabili". Ciò ha ridotto ulteriormente i rischi e ha aumentato il livello di sicurezza generale di Akamai. Enterprise Application Access in combinazione con Ion, il motore di ottimizzazione delle performance di Akamai, ha aiutato il reparto IT di Akamai a fornire experience delle applicazioni web di livello superiore per gli utenti finali, indipendentemente dal dispositivo, dalla rete o dalla posizione geografica in questione.

L'approccio di Akamai ha ridotto i costi e le complessità generalmente associati alla protezione dell'accesso alle applicazioni. Anziché tentare di controllare o limitare l'accesso remoto di vari endpoint alla rete aziendale, secondo Akamai era più sensato adottare una soluzione in grado di consentire all'IT di monitorare e controllare l'accesso solo alle applicazioni effettivamente necessarie per gli utenti. Lo spostamento di tutti gli utenti dalla VPN e dalla rete aziendale, utilizzando un approccio Zero Trust per ottenere visibilità e contesto per tutto il traffico (per utenti, dispositivi, posizioni e applicazioni), non solo ha ridotto significativamente i rischi, ma ha anche semplificato il processo di distribuzione delle applicazioni aziendali.

Basarsi sul comportamento del dispositivo per le decisioni relative all'accesso dinamico è un altro componente fondamentale per completare la transizione di Akamai verso un modello Zero Trust. Il comportamento del dispositivo integra e migliora le regole di autenticazione, autorizzazione e controllo degli accessi esistenti, nonché le funzionalità di reporting, fornendo un contesto e segnali aggiuntivi tali da favorire le decisioni relative all'accesso alle applicazioni.

Il percorso di Akamai verso il modello Zero Trust

2000

Controlli di rete e delle applicazioni

- *Certificati client per tutti*
- *Rete dot1x - 2FA*
- *Autenticazione federata SAML*
- *Senza rete wireless interna*
- *Bastion host di gestione*
- *Senza Internet in uscita per predefinito*

2011

Utilizzo delle soluzioni Akamai esistenti

- *Applicazioni disponibili esternamente tramite una soluzione creata dal reparto IT di Akamai (proxy in ingresso)*
- Global Traffic Management *(gestione intelligente del traffico)*
- Site Shield *(restrizione dell'accesso diretto all'origine dell'applicazione)*

2016

Eliminazione della maggior parte delle password per gli utenti

- *Il 2FA si evolve in certificati e MFA con push*
- *Le password vengono largamente eliminate dall'ambiente*
- Enterprise Application Access *(accesso di terze parti)*

2017

Introduzione alle soluzioni per la sicurezza aziendale di Akamai

- *Enterprise Application Access elimina la soluzione IT interna di Akamai*
- Enterprise Threat Protector *(protezione dalle minacce basata su DNS)*

ORA

Zero Trust

- *I client Enterprise Application Access ed Enterprise Threat Protector distribuiti correttamente a migliaia di utenti interni*
- *Centinaia di applicazioni abilitate su Enterprise Application Access in combinazione con* Ion *(ottimizzazione delle performance)*
- *Funzionalità relativa al comportamento del dispositivo abilitata con Enterprise Application Access*
- Kona Site Defender *(Web Application Firewall)*
- Bot Manager *(protezione dai bot)*

I vantaggi aziendali del passaggio a un sistema di sicurezza Zero Trust

- *Riduzione al minimo dei rischi fornendo l'accesso solo alle applicazioni necessarie, non a tutta la rete aziendale*
- *Rimozione della complessità della rete associata alle tecnologie legacy, incluso il backhaul del traffico VPN a un data center centrale*
- *Aumento della produttività con un accesso semplificato per la forza lavoro di Akamai, nonché per terze parti*
- *Riduzione dei costi associati alle appliance e ai processi IT fornendo l'accesso ai dipendenti delle aziende recentemente acquisite*
- *Automazione, orchestrazione, visibilità e analisi di carichi di lavoro, reti, utenti e dispositivi per proteggere i dati*
- *Miglioramento della user experience sui dispositivi, inclusi dispositivi mobili, con una delivery delle applicazioni più rapida e affidabile*
- *Taglio dei costi con un'allocazione efficiente delle risorse IT; la riduzione delle ore impiegate per l'aggiornamento, la gestione e la manutenzione di hardware e software significano un aumento del tempo dedicato alle attività strategiche più importanti*
- *Riduzione delle richieste associate all'accesso alle applicazioni per l'help desk*

Visitate il sito web **akamai.com/zerotrust** per saperne di più sulla transizione dell'azienda verso un modello di sicurezza Zero Trust. In alternativa, **contattate un esperto Akamai** per valutare un piano di azione personalizzato per la trasformazione del sistema di sicurezza.

Cos'è Enterprise Defender?

Enterprise Defender sfrutta l'Akamai Intelligent Edge Platform per proteggere tutte le applicazioni e gli utenti aziendali, offrendo una sicurezza ottimale e riducendo la complessità senza influire sulle performance. Vi consente di proteggere l'accesso alle applicazioni da voi controllate, mitigando i rischi associati all'accesso degli utenti alle applicazioni che esulano dal vostro controllo.

Enterprise Defender include le seguenti funzionalità in un servizio di sottoscrizione mensile, per singolo utente, di facile utilizzo:

Prevenzione dei malware: la soluzione SIG (Secure Internet Gateway) di Akamai consente di identificare, bloccare e mitigare in maniera proattiva minacce mirate come malware, ransomware, phishing, esfiltrazione di dati che sfruttano il DNS e attacchi zero-day avanzati.

Accesso sicuro alle applicazioni: Akamai assicura che solo gli utenti e i dispositivi autorizzati possano accedere alle applicazioni aziendali di cui necessitano e non all'intera rete.

Web Application Firewall: Akamai offre un'ampia protezione per le applicazioni web di importanza critica dagli attacchi DDoS e web più vasti e sofisticati.

Enterprise Defender affianca a un sistema di prevenzione dei malware un modello di accesso alle applicazioni adattivo e funzioni di sicurezza e accelerazione, il tutto integrato in un servizio dedicato e facile da utilizzare sull'edge.

Accelerazione delle applicazioni: Akamai consente alle aziende di fornire applicazioni rapide, affidabili e sicure in modo conveniente. Le funzionalità di delivery delle applicazioni sono collocate sull'edge, più vicino agli utenti, al cloud e ai carichi di lavoro in sede, ovunque nel mondo.

Akamai

Akamai garantisce experience digitali sicure per le più grandi aziende a livello mondiale. L'Akamai Intelligent Edge Platform permea ogni ambito, dalle aziende al cloud, permettendovi di lavorare con rapidità, efficacia e sicurezza. I migliori brand a livello globale si affidano ad Akamai per ottenere un vantaggio competitivo grazie a soluzioni agili in grado di estendere la potenza delle loro architetture multicloud. Più di ogni altra azienda, Akamai avvicina agli utenti app, experience e processi decisionali, tenendo lontani attacchi e minacce. Il portfolio Akamai di soluzioni per l'edge security, le web e mobile performance, l'accesso aziendale e la delivery di contenuti video è affiancato da un servizio clienti di assoluta qualità e da un monitoraggio 24/7/365. Per scoprire perché i principali brand del mondo si affidano ad Akamai, visitate il sito www.akamai.com o blogs.akamai.com e seguite @Akamai su Twitter. Le informazioni di contatto internazionali sono disponibili all'indirizzo www.akamai.com/locations. Data di pubblicazione: 07/19.