4 motivi per cui le aziende hanno bisogno della sicurezza Zero Trust

Sommario

Introduzione

Man mano che gli attacchi diventano più sofisticati, i gruppi di ransomware proliferano e i progressi compiuti in campo tecnologico introducono nuove vulnerabilità, un numero sempre maggiore di organizzazioni sta adottando un modello di sicurezza Zero Trust. Fondamentalmente, questo approccio elimina la fiducia implicita nei confronti di utenti, applicazioni e dispositivi, un principio centrale dei precedenti approcci alla sicurezza. In termini pratici, sono quattro le situazioni principali in cui un'organizzazione può trarre vantaggio da un modello di sicurezza Zero Trust: un attacco ransomware sferrato contro la vostra azienda, il passaggio allo smart working, la protezione di un ambiente cloud o una verifica imminente.

Queste situazioni sono il risultato delle recenti tendenze (l'aumento degli attacchi ransomware, il passaggio a una forza lavoro ibrida, la migrazione verso il cloud computing e l'aumentata richiesta di verifiche di sicurezza), che richiedono un approccio alla sicurezza basato sulla verifica dell'identità, a prescindere dalla posizione, e in grado di prendere misure proattive rispetto alle violazioni. L'approccio Zero Trust è l'unico che richiede un'efficace gestione dell'identità dell'utente per accedere ai dati e che fornisce una mitigazione proattiva una volta che si verifica un attacco.

L'implementazione di una strategia Zero Trust può sembrare onerosa per i team addetti alla sicurezza già sovraccarichi di lavoro, ma non necessariamente è così. Adottando un approccio graduale e concentrandovi sui risultati immediati, potete ridurre alcune delle complessità e dei rischi associati alle soluzioni di sicurezza tradizionali e migliorare la vostra strategia di sicurezza.

Non dovete rinnovare completamente la tecnologia esistente. Potete iniziare allineando gli investimenti Zero Trust alle vostre esigenze aziendali più pressanti. Accordate la vostra preferenza a un fornitore Zero Trust attendibile piuttosto che affidarvi a chi ha ribrandizzato la sua soluzione come Zero Trust da un giorno all'altro. Vi consigliamo vivamente di cercare un fornitore in grado di riunire più elementi del modello di sicurezza Zero Trust (Zero Trust Network Access, firewall DNS, microsegmentazione, ecc.) in un'unica piattaforma. Qualunque sia il motivo alla base della sua adozione, il modello Zero Trust vi consentirà di ottenere flessibilità aziendale, ottimizzazione dei costi e consolidamento degli strumenti, migliorando, al contempo, le vostre operazioni complessive.

I 4 motivi principali per cui le organizzazioni adottano il modello Zero Trust

Aumento degli attacchi ransomware

Forza lavoro ibrida

Adozione di risorse di cloud computing

Requisiti di conformità rigorosi

01

Aumento degli attacchi ransomware

Maggiore protezione dai ransomware

Negli ultimi anni, gli attacchi ransomware hanno interrotto le operazioni aziendali delle organizzazioni in tutto il mondo, dagli ospedali e dalle banche alle pipeline e ad altre infrastrutture critiche. In effetti, **Cybersecurity Ventures** prevede che tali attacchi costeranno alle loro vittime circa 265 miliardi di dollari all'anno entro il 2031 e che gli autori di ransomware riusciranno a sferrare un nuovo attacco (contro consumatori o aziende) ogni due secondi man mano che perfezionano i propri payload di malware e le attività di estorsione correlate.

Senza una tecnologia Zero Trust, i gruppi di ransomware possono sfruttare i seguenti punti deboli:

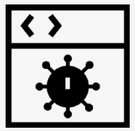
- ☑ Fiducia implicita nei confronti di utenti, applicazioni e reti, che consente ai criminali che hanno violato la rete di spostarsi lateralmente e diffondere i malware
- ☑ Policy di accesso eccessivamente permissive, che permettono infezioni da poter usare, in seguito, per iniettare il ransomware
- ☑ Sistemi che si affidano solo alle password, il che rappresenta un'opportunità per il furto di credenziali

In che modo il modello Zero Trust può essere di aiuto

Le aziende che si affidano a un'architettura Zero Trust, hanno implementato appropriate policy per il controllo degli accessi e utilizzano la microsegmentazione riducono i danni che il ransomware può causare. I criminali non solo hanno difficoltà a violare il sistema, ma hanno anche meno possibilità di espandersi.

In che modo Akamai spezza la kill chain del ransomware

Un attacco ransomware, di solito, prevede un'infezione iniziale, un movimento laterale e operazioni di crittografia ed esfiltrazione di dati. Con l'approccio Zero Trust, le organizzazioni possono affrontare ciascuno di questi passaggi non appena avvengono, se non prima.



Infezione iniziale

La piattaforma Akamai Guardicore aiuta ad impedire a un attacco di diffondersi oltre il punto di accesso iniziale, mentre Akamai MFA evita che le credenziali degli utenti vengano rubate o violate.

Prevenzione del movimento

La piattaforma Akamai Guardicore riduce i percorsi di propagazione e aiuta a prevenire il movimento laterale. Akamai Guardicore Access limita la possibilità di un criminale di spostarsi e infettare l'applicazione che sperava di sfruttare. Akamai Hunt rileva e mitiga le minacce elusive e avanzate nella rete.

Esfiltrazione e crittografia dei dati

La piattaforma Akamai Guardicore limita l'accesso alle applicazioni critiche, impedendo ai criminali di accedere ai dati sensibili all'interno di una rete violata. Akamai Secure Internet Access Enterprise blocca le richieste indirizzate a siti di phishing e a siti CnC (Command and Control). Infine, Akamai Hunt rileva i comportamenti anomali, impedendo ai criminali di crittografare dati preziosi e di restituirli dietro pagamento di un riscatto.

02

Forza lavoro ibrida

Protezione della nuova forza lavoro ibrida

Mettere al sicuro una forza lavoro nuova e ibrida, cresciuta ed ampliatasi durante la pandemia del COVID-19, è più complicato quando le organizzazioni si affidano a strumenti di sicurezza obsoleti, quali firewall e VPN. Quando sono state introdotte le VPN per l'accesso remoto, circa 30 anni fa, tutto era diverso, Internet era ancora agli esordi, le applicazioni venivano eseguite nei data center e un minor numero di utenti si connettevano da remoto. Continuare ad autenticare gli utenti con una VPN per poi concedere l'accesso all'intera rete aumenta la superficie di attacco aprendo le porte a molte delle vulnerabilità zero-day correlate alle VPN tradizionali. Qualsiasi utente dotato delle credenziali necessarie può accedere a una VPN aziendale e, una volta all'interno, spostarsi lateralmente nella rete e accedere alle risorse che la VPN dovrebbe proteggere.

In che modo il modello Zero Trust può essere di aiuto

Basato sul principio dell'accesso con privilegi minimi, l'approccio Zero Trust presume che nessun utente o applicazione debba essere considerato affidabile. La tecnologia ZTNA (Zero Trust Network Access) utilizza un approccio completamente diverso rispetto alle VPN per consentire l'accesso ai lavoratori remoti. Anziché mettere a rischio l'intera rete, gli utenti vengono connessi direttamente solo alle applicazioni e ai dati di cui hanno bisogno, in questo modo si impedisce il movimento laterale da parte di utenti malintenzionati che potrebbero sfruttare un accesso oltremodo permissivo a dati e risorse sensibili. Un'efficace soluzione di microsegmentazione Zero Trust può segmentare l'intera rete in modo che un'eventuale violazione non si diffonda e non danneggi altre componenti della rete. Secondo **Gartner**, entro il 2025, almeno il 70% delle nuove implementazioni di accesso remoto saranno servite principalmente dalla tecnologia ZTNA, anziché dai servizi VPN, partendo da meno del 10% alla fine del 2021.

In che modo Akamai facilita il lavoro ibrido e lo smart working

La piattaforma Zero Trust completa di Akamai soddisfa le esigenze della vostra forza lavoro ibrida. I vantaggi includono:

Riduzione dei rischi

Akamai connette direttamente l'utente giusto all'applicazione giusta, riducendo la superficie di attacco e limitando il movimento laterale.

Miglioramento delle user experience

Gli utenti remoti accedono alle risorse a prescindere dall'applicazione, dal dispositivo o dalla posizione, eliminando la necessità di connettersi e disconnettersi dalla VPN.

Incremento della flessibilità

Dal momento che la soluzione di Akamai viene utilizzata come servizio, le organizzazioni non devono distribuire alcun hardware né preoccuparsi della scalabilità nel caso in cui aumenti la domanda, il che riduce costi e complessità.

03

Adozione di risorse di cloud computing

Migrazione nel cloud facilitata

Le organizzazioni stanno spostando le loro app sul cloud per ottenere flessibilità e agilità e per modernizzare la loro infrastruttura. Tuttavia, questi ambienti cloud stanno espandendo la superficie di attacco e introducendo nuovi requisiti di sicurezza. Le integrazioni tra diversi ambienti cloud e on-premise possono danneggiare le applicazioni e mettere a rischio la sicurezza. Quando le organizzazioni cercano di migrare le applicazioni sul cloud usando strutture di rete tradizionali, quali VPN e firewall, spesso si trovano a dover affrontare un maggior rischio di minacce laterali, scarsa scalabilità e costi elevati. Anche dopo il completamento della migrazione, le risorse devono comunque essere protette e gli utenti devono essere autenticati in base a ruoli e autorizzazioni. In genere, gli utenti di un'infrastruttura cloud godono di un accesso a risorse, servizi e diritti di gestione più ampio di quello di cui godrebbero con ambienti on-premise, il che introduce un ulteriore rischio e il potenziale per l'interruzione.

In che modo il modello Zero Trust può essere di aiuto

Le strategie Zero Trust facilitano la migrazione verso il cloud. Il modello Zero Trust rimuove la fiducia implicita intrinseca di molte applicazioni basate sul cloud, in particolare le applicazioni di terze parti, che possono introdurre delle vulnerabilità. Le soluzioni Zero Trust consentono alle organizzazioni di implementare le loro applicazioni basate sul cloud più facilmente e con protezioni più robuste. Alcuni dei vantaggi dell'implementazione di una strategia Zero Trust per il cloud includono:

- ☑ Migliore visibilità su risorse e rischi
- ☑ Superficie di attacco ridotta con la segmentazione Zero Trust e l'accesso con privilegi minimi alle risorse cloud
- ☑ Infrastruttura di rete modernizzata che offre velocità e flessibilità
- ☑ Riduzione dei costi operativi e della complessità

In che modo Akamai migliora la migrazione nel cloud

Le soluzioni Zero Trust di Akamai possono aiutarvi a migrare automaticamente le vostre risorse e le rispettive policy. Nessun downtime e nessuna interruzione delle attività aziendali. Akamai offre:

Maggiore visibilità

Con una migliore comprensione delle dipendenze delle app, potete creare policy di segmentazione cloud efficaci per ridurre la superficie di attacco e i rischi.

Zero Trust Network Access

Gli utenti possono connettersi solo alle app per le quali dispongono di autorizzazione, in base a un solido sistema di autenticazione.

Ricerca delle minacce

Il team di addetti alla ricerca delle minacce di Akamai studia continuamente i comportamenti di attacco anomali negli ambienti cloud e avvisa i clienti Akamai di eventuali rischi per la loro rete.

04

Requisiti di conformità rigorosi

Conformità semplificata e meno rischi

Sebbene i responsabili della sicurezza sappiano che soddisfare i requisiti di conformità non equivale ad avere un'organizzazione davvero sicura, le verifiche di sicurezza sono comunque prioritarie per i team dirigenti. È risaputo che le verifiche non riuscite possono portare a importanti interruzioni delle attività e incidere sui profitti. La valutazione della conformità è una delle attività più dispendiose in termini di tempo e risorse per i team di sicurezza. Inoltre, il passaggio ad ambienti digitali senza perimetro e la prevalenza dello smart working hanno reso il processo di conformità ancora più difficile. Solitamente, le organizzazioni devono isolare i loro ambienti e le loro risorse regolamentate per soddisfare standard di conformità quali il Payment Card Industry Data Security Standard (PCI DSS), l'Health Insurance Portability and Accountability Act (HIPAA) e il Society for Worldwide Interbank Financial Telecommunication (SWIFT).

In più, devono gestire utenti remoti, utenti aziendali on-premise, partner, fornitori e altri, il che rende il perimetro dell'ambiente di un'organizzazione quasi impossibile da definire. Nel prepararsi per le verifiche in cui il controllo degli accessi è un fattore determinante del successo, i team addetti alla sicurezza devono porsi le seguenti domande:

- Come possiamo limitare l'accesso alle informazioni sensibili solo agli utenti autorizzati?
- Come possiamo esaminare l'ambiente di verifica?
- Come possiamo rendere il processo di verifica più semplice e meno caotico?

In che modo il modello Zero Trust può essere di aiuto

Fortunatamente, un approccio Zero Trust può aiutare a rispondere a tutte queste e a molte altre domande. I due pilastri chiave di una strategia Zero Trust, ossia la possibilità di verificare esplicitamente e di supportare l'accesso con privilegi minimi, semplificano enormemente il processo di conformità. Le organizzazioni possono isolare le loro risorse regolamentate dall'altro traffico nel data center o nel cloud e consentire l'accesso in base alle identità, a prescindere dalla posizione. Una maggiore visibilità mostra ciò che entra ed esce dall’ambiente regolamentato e aiuta ad identificare ciò che è rilevante. Ciò riduce di gran lunga la complessità e il costo delle verifiche e facilita il lavoro dei revisori.

In che modo Akamai facilita la conformità

Il portfolio completo di soluzioni Zero Trust di Akamai aiuta a prepararvi per qualsiasi verifica, che si tratti di normative quali PCI DSS, HIPAA, di verifiche da parte dell'ISO (Organizzazione internazionale di standardizzazione), di controlli Sarbanes-Oxley (SOX) o di qualsiasi altra normativa. Akamai Enterprise Application Access controlla l'accesso da parte di terze parti ai dati personali sensibili, rispettando i requisiti del Regolamento generale sulla protezione dei dati (GDPR). Akamai Guardicore Segmentation migliora la comprensione delle risorse regolamentate ai sensi del PCI DSS, isola le funzioni del centro di smistamento per soddisfare le direttive HIPAA, limita l'accesso a Internet e isola i sistemi critici per soddisfare le normative SWIFT. Akamai MFA protegge le informazioni sui pazienti ai sensi della legge HIPAA da criminali che hanno ottenuto le password per accedere ai sistemi sanitari e rafforza la conformità alle normative SWIFT impedendo la violazione delle credenziali.

Una banca globale ottiene la conformità SWIFT in due settimane

Alcune autorità di regolamentazione esterne hanno imposto a un cliente di Akamai, una banca globale, di isolare tutte le sue applicazioni critiche al fine di soddisfare i requisiti delle normative SWIFT per trasferire soldi in modo sicuro tra gli istituti finanziari. In genere, una simile applicazione richiede l'implementazione di più di 100 server in posizioni diverse, inclusi server bare-metal e virtuali. In media, la pianificazione e l'esecuzione di questo processo avrebbe richiesto a una banca di queste dimensioni da 8 a 12 mesi, perché si sarebbe dovuta creare una rete VLAN (Virtual Local Area Network) per il segmento su più posizioni. Individuare le dipendenze dell'applicazione SWIFT e assicurarsi la correttezza e la funzionalità del set di regole avrebbe aggiunto solo ulteriore tempo. Un simile progetto avrebbe inoltre richiesto l'acquisto di nuove attrezzature firewall. Inoltre, poiché l'applicazione SWIFT è critica per il settore bancario, eventuali problemi di downtime non sarebbero stati tollerati. Nel complesso, si prevedeva che il progetto di segmentazione avrebbe richiesto un enorme sforzo da parte di molte persone. Ma, con Akamai, l'intero processo ha richiesto l'intervento di un solo Security Engineer ed è stato completato in circa due settimane; non sono state necessarie modifiche alla rete e la banca ha evitato qualsiasi modifica o downtime.

Semplifica e accelera la conformità

Banca globale

- Necessità di isolare l'applicazione SWIFT
- Ambiente complesso con server bare-metal, VMware e OpenStack

Segmentazione tradizionale

- Difficoltà a definire i segmenti in un'infrastruttura complessa
- Nessuna visibilità su applicazioni e dipendenze
- Downtime necessario
  Tempo: 8 - 12 mesi
  Persone: almeno 5

Akamai Guardicore Segmentation

- Mappatura dell'applicazione SWIFT completata in poche ore
- Policy di segmentazione suggerite e ottimizzate automaticamente
- Nessuna necessità di acquistare e implementare nuovi hardware e firewall
- Nessun downtime
  Tempo: 2 settimane
  Persone: 1 architetto

Scoprite di più su come soddisfare le esigenze aziendali con il portfolio Zero Trust di Akamai

Ulteriori informazioni

Akamai Security protegge le applicazioni che danno impulso alle vostre attività aziendali e rafforzano le interazioni, senza compromettere le performance o le customer experience. Tramite la scalabilità della nostra piattaforma globale e la visibilità delle minacce, possiamo prevenire, rilevare e mitigare le minacce informatiche in ambienti ransomware affinché voi possiate rafforzare la fiducia nel brand e realizzare la vostra visione. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito **akamai.com** o **akamai.com/blog** e seguite Akamai Technologies su **X** (in precedenza Twitter) e **LinkedIn**. Data di pubblicazione: 09/24.