DESCRIZIONE DELLA SOLUZIONE AKAMAI

Semplificazione e sicurezza con un modello Zero Trust end-to-end

Il modello Zero Trust è un approccio strategico alla cybersecurity che protegge un'organizzazione rimuovendo la fiducia implicita tra utenti, dispositivi, reti, dati e applicazioni. Invece di presumere che tutto ciò che si trova dietro il firewall aziendale è sicuro, l'approccio Zero Trust presuppone una violazione in qualsiasi momento e applica l'accesso con privilegi minimi a ogni richiesta, indipendentemente da dove ha origine.

Perché ora è importante il modello Zero Trust?

Il modello Zero Trust è diventato la priorità assoluta per le organizzazioni che devono adattarsi in modo più efficace all'ambiente moderno in continua evoluzione. Le organizzazioni sono alla ricerca di un nuovo modello di sicurezza che supporti una forza lavoro ibrida e protegga utenti, dispositivi e app ovunque si trovino.

I principi della moderna architettura Zero Trust

- Verificare esplicitamente, sempre nel contesto
- Rafforzare il principio del privilegio minimo esplicitamente
- Monitorare di continuo

Il consolidamento è essenziale

Approccio end-to-end integrato

Un approccio olistico al modello Zero Trust deve essere esteso a tutte le entità dell'organizzazione, incluse identità, rete e app. Il modello Zero Trust funge da strategia end-to-end, motivo per cui richiede l'integrazione in tutti gli elementi. L'adozione di soluzioni puntuali multiple e scarsamente integrate non è in linea con questo approccio strategico.

Akamai ha assemblato un solido portfolio olistico per fornire tutte le soluzioni Zero Trust fondamentali per l'organizzazione moderna. Invece di installare, eseguire e correggere più prodotti per la sicurezza, le organizzazioni possono fare affidamento su un unico fornitore per fornire tutte le tecnologie necessarie e usufruire di costi ridotti e di una maggiore efficienza operativa.

Condivisione del segnale tra le soluzioni

Akamai ha integrato l'automazione in tutto il suo portfolio Zero Trust, riducendo notevolmente la complessità e la personalizzazione. In questo modo, tutti i prodotti del portfolio possono condividere tra loro le informazioni sulle minacce, rendendo ogni prodotto più sicuro. Se un prodotto identifica una minaccia, un altro prodotto può essere avvisato per mitigarla.

Vantaggi

- **Forza lavoro distribuita**
  Consente agli utenti di lavorare in modo più sicuro ovunque, in qualsiasi momento e su qualsiasi dispositivo
- **Migrazione nel cloud**
  Consente di fornire un controllo degli accessi sicuri in ambienti cloud e cloud ibridi
- **Mitigazione dei rischi**
  Consente di bloccare le minacce e minimizzare il movimento laterale dei ransomware e di altri tipi di malware
- **Conformità**
  Consente di garantire la conformità con microperimetri intorno ai dati sensibili

Akamai

Un portfolio end-to-end olistico: utenti, applicazioni e reti

Protezione del carico di lavoro

Akamai Guardicore Segmentation: Zero Trust per le applicazioni

Akamai Segmentation fornisce la soluzione di microsegmentazione leader del settore, concepita per limitare la diffusione del ransomware e di altri malware. Il prodotto offre visibilità e comprensione dei carichi di lavoro, dei processi e delle applicazioni, nonché l'applicazione delle policy di accesso.

Protezione della rete

Enterprise Application Access: Accesso alla rete Zero Trust

La tecnologia Zero Trust Network Access di Akamai è stata concepita per sostituire la tradizionale tecnologia VPN per un'efficace identità dell'utente. Invece di mettere a rischio l'intera rete, Enterprise Application Access consente l'accesso degli utenti in base all'app specifica a cui devono accedere per svolgere un ruolo. Enterprise Application Access offre visibilità sull'identità degli utenti e un'efficace applicazione dell'identificazione e dell'autenticazione.

Protezione degli utenti

Secure Internet Access: Accesso a Internet Zero Trust

Secure Internet Access è una soluzione SWG (Secure Web Gateway) basata sul cloud, che ispeziona ogni richiesta web degli utenti e applica l'intelligence sulle minacce in tempo reale e tecniche di analisi del malware avanzate per garantire che venga distribuito solo contenuto sicuro. Le richieste e i contenuti dannosi vengono bloccati in modo proattivo.

Autenticazione multifattore: efficace identità Zero Trust

Akamai MFA protegge gli account dei dipendenti dal phishing e da altri attacchi di tipo MITM (Machine-In-The-Middle). Ciò garantisce che solo i dipendenti con un'efficace autenticazione possano accedere ai propri account, che gli altri accessi vengano negati e che venga impedito il controllo dell'account dei dipendenti

Tracciamento e monitoraggio

Ricerca: servizi di sicurezza

Poiché non smette mai di presupporre uno stato di violazione, il team scelto di addetti alla sicurezza di Akamai è alla continua ricerca di comportamenti di attacco anomali e di minacce avanzate, che spesso sfuggono alle soluzioni di sicurezza standard. I nostri addetti alla sicurezza vi informano immediatamente di qualsiasi incidente critico rilevato nella vostra rete e poi lavorano a stretto contatto con il vostro team per rimediare alla situazione.

Il vantaggio di Akamai

Akamai offre alcuni vantaggi che la distinguono dagli altri fornitori di soluzioni Zero Trust. Offriamo una copertura più ampia: legacy e moderna; per Windows e Linux; on-premise e virtualizzata, container e altro ancora. Grazie alle nostre impareggiabili funzionalità di visibilità, gli utenti sono in grado di sapere cosa sta facendo ogni carico di lavoro con tutto il relativo contesto. Inoltre, i nostri servizi interni per la ricerca di minacce all'avanguardia ampliano le funzionalità dei team di sicurezza e impediscono alla vostra organizzazione di restare indietro.

Per ulteriori informazioni sul modello Zero Trust e su come iniziare, visitate il sito akamai.com.

 | Supporto | | Data di pubblicazione 06/22