STORIE DI CLIENTI AKAMAI

Azienda di infrastrutture di comunicazione

blocca tempestivamente i ransomware con Akamai

Prevenzione di potenziali perdite pari a 1 milione di dollari

Prevenzione di potenziali attività IT nascoste

Visibilità del traffico est-ovest

Il cliente

Questo fornitore di infrastrutture di comunicazione negli Stati Uniti garantisce alle aziende e ai residenti di rimanere collegati nel mondo frenetico di oggi. È responsabile di un'ampia rete di ripetitori cellulari e reti in fibra a cui i clienti si affidano ogni giorno.

Le sfide

Visibilità e controllo limitati degli endpoint

Con oltre 6.000 laptop distribuiti in tutta l'organizzazione, il team di sicurezza IT era preoccupato per i rischi posti dal parco di dispositivi all'ambiente IT. Inoltre, era necessario affrontare i problemi inerenti all'attività IT nascosta di alcuni utenti esperti dell'azienda.

Le misure di sicurezza attuate dal team dei sistemi informatici degli utenti finali non ovviavano il problema, essendo incapaci di controllare in modo granulare l'accesso ai sistemi per gli utenti e limitare la comunicazione peer-to-peer per bloccare in modo efficace la propagazione del malware, una minaccia che preoccupava particolarmente l'organizzazione.

Per colmare queste lacune, occorreva migliorare la strategia di sicurezza dell'azienda con una soluzione che consentisse di estendere la visibilità e i controlli di segmentazione granulari ai dispositivi dei dipendenti, permettendo di osservare e prevenire i movimenti laterali non autorizzati.

La scelta di una soluzione

Gli esperti della sicurezza stavano prendendo in considerazione da tempo la soluzione Akamai Guardicore Segmentation, mostrandosi interessati ad utilizzarla per molteplici casi d'uso di sicurezza informatica. L'organizzazione ha optato per un approccio graduale osservando un elevato potenziale nella visibilità granulare e nel semplice processo di creazione delle policy.

Azienda di infrastrutture di comunicazione

Sede
Stati Uniti

Settore
Infrastrutture di comunicazione

Soluzione
Akamai Guardicore Segmentation

Risultati principali
- Prevenzione dei ransomware
- Blocco delle attività IT nascoste
- Visibilità del traffico est-ovest

Poiché le policy di segmentazione definita dal software di Akamai non sono legate all'infrastruttura sottostante, il fornitore ha avuto la possibilità di gestire una serie di iniziative di sicurezza. Tuttavia, con il parco di laptop dei dipendenti considerato ad alto rischio, il team ha dato la priorità all'implementazione degli agenti Akamai sui propri endpoint.

Akamai Guardicore Segmentation

Una volta iniziato il progetto, l'implementazione dell'agente Windows ottimizzato di Akamai sui computer dell'organizzazione è avvenuta rapidamente, incrementando la visibilità a livello di processi sull'accesso degli utenti e l'attività dei laptop.

Il team di sicurezza IT è stato quindi in grado di creare e gestire a livello centralizzato i controlli di sicurezza per gli endpoint, il tutto sulla base di dati ambientali accurati. Ha quindi introdotto diverse policy, incluso un avviso su attività specifiche del protocollo RDP (Microsoft Remote Desktop Protocol), completo dei tentativi di accesso non riusciti.

Visibilità granulare in azione

Poco tempo dopo l'implementazione, la policy configurata per segnalare attività insolite relative a RDP ha generato una serie di avvisi. Era chiaramente in corso un attacco di forza bruta, caratterizzato da una serie di accessi non riusciti.

Il team di sicurezza IT ha monitorato da vicino la situazione e, mentre gli autori dell'attacco continuavano il loro assalto, ha deciso di effettuare la chiamata e bloccare l'RDP su ogni endpoint con un agente Akamai. In pochi clic, è stata creata e applicata una nuova policy di segmentazione che ha disabilitato RDP, bloccando l'aggressore prima che venisse compromesso un singolo endpoint.

Blocco immediato del ransomware

Durante le analisi successive all'evento, il team di sicurezza si è rapidamente reso conto che tutti gli indicatori identificavano un importante e noto autore di minacce ransomware.

Se la campagna avesse avuto successo, gli aggressori avrebbero probabilmente tentato di procedere con le consuete tattiche, crittografando qualsiasi cosa a portata di mano e richiedendo un riscatto. Viste le dimensioni organizzative del fornitore e le tendenze attuali, le richieste dei malintenzionati avrebbero sicuramente superato il milione di dollari. Ciò avrebbe comportato notevoli interruzioni e tempi di inattività aggiuntivi in caso di compromissione delle risorse aziendali più importanti, come il sistema ERP.

Tuttavia, grazie alla tempestività del team di sicurezza e ad Akamai, il tentativo di attacco non ha avuto alcun impatto sull'organizzazione.

Blocco delle attività IT nascoste

Oltre a bloccare le minacce esterne, utilizzando la piattaforma il team è stato anche in grado di affrontare le sfide interne. Prima di Akamai, la visibilità limitata degli endpoint rendeva più facile per alcuni utenti aggirare i processi ufficiali, eseguendo autonomamente attività non conformi alle policy dell'organizzazione. Le nuove informazioni e la possibilità di applicare i controlli di sicurezza sugli endpoint hanno consentito alla sicurezza IT di contenere le attività IT nascoste. È stato quindi possibile impedire ai membri dell'organizzazione DevOps di creare autonomamente nuove risorse eludendo i canali ufficiali per l'autorizzazione.

Una maggiore protezione con Akamai

Per l'azienda di infrastrutture di comunicazione, la protezione degli endpoint è solo l'inizio. L'organizzazione prevede di esplorare nuove funzionalità e implementare Akamai nel proprio data center, proteggere l'ambiente Citrix e applicare controlli degli accessi di terze parti per fornitori esterni.

Grazie alla natura flessibile della piattaforma, il team ha la certezza di poter estendere la protezione contro le minacce avanzate ovunque all'interno dell'ambiente, indipendentemente da come svilupperà la propria strategia di fusione e acquisizione o le iniziative di trasformazione digitale in futuro.

Per ulteriori informazioni, visitate il sito akamai.com/guardicore.