Storia di un cliente Akamai

Un'azienda sanitaria statunitense riesce a respingere 4000 attacchi informatici in un giorno

I suoi ingegneri di rete hanno usato la visibilità sul livello 7 e policy intelligenti tramite la microsegmentazione per ridurre i rischi informatici

Blocco dei ransomware | Maggiore visibilità | Policy ottimizzate

Fornire ai pazienti l'assistenza sanitaria essenziale

Immaginate di cercare di proteggere una rete che influisce direttamente sulla vita dei pazienti, rimanendo, al contempo, al passo con gli attacchi informatici sempre più sofisticati. Questa era la realtà di un'azienda sanitaria di medie dimensioni. Trovandosi ad affrontare l'aumento dei ransomware e avendo bisogno di una maggiore visibilità, il team addetto alla progettazione della rete si è affidato alla soluzione Akamai Guardicore Segmentation per migliorare il livello di sicurezza dell'azienda.

Estendere l'architettura Zero Trust

L'azienda si proponeva di conseguire un audace obiettivo: rafforzare il suo ambiente IT con i principi Zero Trust e soddisfare, al contempo, i requisiti di conformità dell'HIPAA e del SOC 2. Poiché la posta in gioco era alta, il team addetto alla progettazione della rete si proponeva di:

- Mantenere le applicazioni critiche online anche durante gli incidenti di sicurezza
- Ridurre l'impatto esercitato dagli attacchi ransomware contenendo la loro diffusione
- Ottenere una visibilità sulla rete molto più dettagliata di quanto consentito con i firewall tradizionali

L'azienda aveva bisogno di una soluzione di microsegmentazione economica in grado di scalare senza richiedere di copiare e sostituire l'infrastruttura IT esistente. Inoltre, la soluzione doveva essere abbastanza semplice da gestire per un team agile e scalabile per crescere insieme all'azienda.

Come ha spiegato uno degli ingegneri di rete: "I ransomware prendono di mira il settore sanitario, quindi più velocemente riusciamo ad isolare e ad eliminare queste minacce, meglio è".

Healthcare Company

Sede

Stati Uniti

Settore

Settore scientifico-sanitario

Soluzione

Akamai Guardicore Segmentation

Akamai

Trovare la giusta soluzione di microsegmentazione

Dopo aver velocemente ignorato la possibilità di adottare un approccio containerizzato, l'azienda ha valutato alcune soluzioni di microsegmentazione. "Volevamo disporre delle stesse funzionalità offerte dai firewall di nuova generazione, nello specifico della visibilità a livello di applicazioni", ha spiegato l'ingegnere di rete

Dopo aver valutato molte soluzioni, l'azienda ha provato Akamai Guardicore Segmentation. La demo ci ha colpito favorevolmente e, grazie al supporto pratico offerto dagli ingegneri di Akamai, l'accordo è stato concluso. La soluzione ha soddisfatto tutti i requisiti, tra cui:

- **Visibilità approfondita:** ispezione al livello 7 e informazioni complete sulla rete
- **Facilità di implementazione:** agenti basati su software senza alcun hardware aggiuntivo
- **Resilienza:** nessun single point of failure nella rete principale
- **Flessibilità:** supporto di diversi sistemi operativi

Secondo il vicepresidente del reparto di sicurezza delle informazioni e dell'infrastruttura IT, Akamai Guardicore Segmentation offre enormi vantaggi ai team agili. "Subito dopo aver avviato l'implementazione, abbiamo osservato i vantaggi apportati dalla soluzione in termini di visibilità e controllo.

Non dobbiamo acquistare né gestire diversi firewall est-ovest, il che ci fa risparmiare notevolmente in termini di costi, e possiamo ottenere anche un livello di visibilità non consentito dai firewall tradizionali", ha aggiunto il responsabile dell'infrastruttura IT.

Bloccare il percorso dei ransomware

I risultati sono stati immediati e straordinari. Isolando meglio le sue app e utilizzando le policy di prevenzione dei ransomware immediatamente disponibili nella soluzione Akamai Guardicore Segmentation, il team ha neutralizzato 4000 attacchi informatici in un solo giorno. La soluzione dispone, persino, di policy personalizzate per soddisfare le specifiche esigenze dell'azienda.

"Per le policy intersettoriali, abbiamo usato una modalità di generazione degli avvisi per segnalare gli incidenti senza causare problemi di downtime. È un modo eccellente per ridefinire le policy senza creare interruzioni", ha affermato l'ingegnere di rete.

> Akamai Guardicore Segmentation ci ha aiutato non solo a risolvere i nostri problemi con gli attacchi ransomware, ma anche a migliorare il nostro approccio alla cybersecurity.
>
> - Ingegnere di rete

> "Scalare la vetta della montagna Zero Trust è molto impegnativo, ma Akamai Guardicore Segmentation ha accelerato la nostra salita, riducendo i problemi legati ai costi e alle complessità".

- Vicepresidente del reparto di sicurezza delle informazioni e dell'infrastruttura IT

Informazioni impareggiabili sul livello 7

Secondo il responsabile dell'infrastruttura IT, Akamai Guardicore Segmentation fornisce un'eccellente visibilità sui flussi di traffico tra le varie app, offrendo una quantità di dati preziosi al team, che ora può ispezionare i dettagli granulari superando i limiti dei registri del livello 4: ID utente, input della riga di comando e, persino, correlazioni dei servizi.

"Il nostro team addetto alla rete può esaminare il flusso del traffico per risolvere i problemi e fornire al nostro team addetto alla sicurezza le informazioni necessarie per compiere un'analisi completa degli incidenti", ha sottolineato l'ingegnere di rete.

Questa visibilità è tornata utile durante la violazione imprevista di una policy. Un nuovo dipendente aveva connesso un PC direttamente al dispositivo CPE (Customer-Premises Equipment) del suo gestore anziché ad una porta LAN protetta da un router domestico. Questa operazione non era consentita perché il dispositivo CPE aveva assegnato al PC un indirizzo IP pubblico, rendendolo quindi soggetto alle scansioni su Internet.

Come ha spiegato l'ingegnere di rete dell'azienda: "Akamai Guardicore Segmentation ha rilevato immediatamente il problema, consentendoci di isolare il PC e di risolvere la situazione prima che arrecasse danni al sistema. Inoltre, ci ha stimolato a creare una policy concepita per prevenire il ripetersi di questo tipo di incidenti in futuro".

Etichette più intelligenti con policy migliori

Grazie alle etichette intuitive e alla creazione di policy, il team addetto alla progettazione della rete ha potuto mappare il traffico e applicare le regole di sicurezza in modo semplice. Secondo l'ingegnere di rete: "Abbiamo scelto la soluzione ideale per il nostro ambiente. Questa capacità ci ha favorevolmente colpito molto più di quanto ci aspettassimo e ci ha aiutato a creare le policy in modo efficiente".

Ad esempio, il team ha limitato l'accesso ai server di stampa, consentendo di accedere solo a zone attendibili: un vantaggio immediato che ha migliorato il livello di sicurezza complessivo dell'azienda. "In tal modo, abbiamo potuto raggiungere immediatamente questo facile obiettivo", ha continuato l'ingegnere.

Una visibilità che ispira fiducia

Un vantaggio non previsto? La visibilità completa sul flusso del traffico interno e sul comportamento delle applicazioni. Questa nuova visibilità ha migliorato la collaborazione con i proprietari delle applicazioni e ha agevolato le finestre di manutenzione. Ad esempio, il team può mostrare ai proprietari delle applicazioni se il loro traffico è bloccato.

"In passato, la risoluzione dei problemi e la protezione dall'obsolescenza erano difficili da eseguire. Ora durante le transizioni, abbiamo potuto verificare tranquillamente se il traffico è passato dai vecchi server a quelli nuovi, il che ci ha consentito di ritirare i sistemi tradizionali con la massima sicurezza", ha affermato l'ingegnere di rete.

Il vicepresidente del reparto di sicurezza delle informazioni e dell'infrastruttura IT ha concluso: "Akamai Guardicore Segmentation ha già influito sulla nostra azienda, diventando un prodotto essenziale nelle nostre attività legate alla sicurezza. Non vediamo l'ora di espandere la sua implementazione a tutta la nostra azienda".