STORIE DI CLIENTI AKAMAI

Un'azienda di servizi per la risoluzione delle violazioni utilizza le soluzioni Akamai per la risposta e il ripristino dai ransomware

Visibilità completa della rete

La segmentazione nelle infrastrutture IT

Risposta alle minacce ransomware

Il cliente

Una società statunitense che offre servizi per la risoluzione delle violazioni è stata ingaggiata da un produttore di apparecchiature globali dopo un importante incidente di sicurezza.

La sfida

Ransomware a rapida diffusione

Dopo un attacco malware che si è propagato con successo influendo sulle operazioni aziendali, il produttore globale ha iniziato a collaborare con la società di servizi per la risoluzione delle violazioni per ripristinare e migliorare la sicurezza del suo ambiente. L'attacco, partito dal computer portatile di un dipendente, si era rapidamente diffuso e aveva colpito la maggior parte delle sedi operative, oltre a penetrare nei server di backup dell'organizzazione.

La scelta di una soluzione

I metodi di contenimento iniziali, come l'applicazione di regole di restrizione dell'accesso a Internet attraverso i firewall, sono stati lenti nel contenere la violazione in rapido peggioramento. La complessità dell'ambiente e la realtà del networking in un'azienda distribuita rendevano l'implementazione e l'applicazione delle regole di restrizione con i firewall un processo lento e inefficace.

Inoltre, la visibilità nei computer preesistenti era un problema significativo per gli addetti alla sicurezza responsabili dell'indagine e del contenimento della violazione. Considerando l'urgenza e la necessità di accelerare la segmentazione prima che la diffusione laterale avesse un impatto su un numero ancora maggiore di risorse, il fornitore di servizi per la risoluzione delle violazioni ha consigliato Akamai Guardicore Segmentation.

Azienda di servizi per la risoluzione delle violazioni

Settore
Tecnologie dell'informazione

Soluzione
Akamai Guardicore Segmentation

Vantaggi principali

- Mitiga la diffusione del ransomware tramite il movimento laterale
- Fornisce una visibilità granulare dei flussi di rete
- Protegge computer moderni e preesistenti
- Consente una risposta rapida agli incidenti

Vantaggi di Akamai Guardicore Segmentation

Visibilità immediata

In tre ore, la società di servizi per la risoluzione delle violazioni ha tempestivamente effettuato il provisioning degli agenti Akamai su oltre 3.000 server aziendali. Pochi minuti dopo l'implementazione, è iniziata a emergere una visibilità granulare dei flussi di rete e di comunicazione, fornendo al team di risposta agli incidenti il contesto e i dati precisi necessari per indagare sulla violazione e convalidare il contenimento.

Rapido time-to-policy

Poco dopo aver ottenuto la necessaria visibilità, i team hanno intrapreso le azioni necessarie per segmentare le risorse critiche, partendo dall'ambiente più ampio. Due applicazioni di produzione cruciali, responsabili dell'unica linea di produzione funzionante, sono state rapidamente identificate e protette. Utilizzando Akamai Guardicore Segmentation, è stata immediatamente introdotta una policy che limitava le connessioni alle applicazioni dalle sottoreti e dalle parti del data center infette, un'attività che avrebbe richiesto settimane con i firewall tradizionali.

Una semplice query ha, inoltre, rivelato che i computer preesistenti che si connettevano a Internet, bypassando i firewall preesistenti, tentavano di superare le restrizioni di contenimento. Dopo aver scoperto comunicazioni non conformi, il team ha creato policy che hanno limitato efficacemente l'accesso a Internet per tutti i server, inclusi i computer preesistenti, in pochi minuti.

Prevenzione del movimento laterale durante il ripristino

Durante la fase successiva del processo di ripristino, il team ha ricreato i cluster delle applicazioni del produttore, inserendo gli agenti Akamai e ha configurato una policy iniziale che bloccava tutte le connessioni in entrata utilizzando Akamai Guardicore Segmentation per identificare le dipendenze. Quindi, le comunicazioni sono state inserite nell'elenco degli elementi consentiti in base alla necessità, solo dopo aver convalidato i requisiti e compreso il contesto. Questo approccio ha permesso al team di ripristinare e riportare online le applicazioni colpite dall'attacco ransomware, senza il rischio di nuova infezione.

Protezione futura

Akamai Guardicore Segmentation ha permesso alla società di servizi per la risoluzione delle violazioni di dimostrare un significativo valore aggiunto per il suo cliente, ossia il produttore, aiutandolo a riprendersi dall'attacco ransomware. Ciò ha aperto all'azienda di servizi l'opportunità di aumentare i ricavi, espandere la sua presenza e aiutare meglio i clienti a raggiungere gli obiettivi di sicurezza e IT.

La segmentazione interna del data center introdotta durante il ripristino graduale ha ridotto in modo significativo la superficie di attacco. Oggi la strategia di sicurezza dell'organizzazione è migliorata e l'impatto di eventuali violazioni future è stato notevolmente ridotto.

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

> [Akamai] ci ha consentito di bloccare la diffusione dell'attacco e di ripristinare le linee di produzione interrotte in un segmento di rete "sterile" in quattro ore senza modificare alcuna rete sottostante. Il tutto mentre erano in corso le indagini e il contenimento IR.
>
> CISO di un'azienda di servizi per la risoluzione delle violazioni