STORIE DI CLIENTI AKAMAI

Una grande società di servizi finanziari protegge l'accesso remoto con Akamai dopo un attacco ransomware

Visibilità completa della rete

Rapido time-to-policy

Protezione dei dipendenti remoti

Il cliente

Una grande società di servizi finanziari con sede in Brasile.

La sfida

Aumento di accessi remoti

Analogamente a molte organizzazioni, la pandemia di COVID-19 ha comportato un aumento delle esigenze di accesso remoto di questo fornitore di servizi finanziari e gran parte del personale IT della banca è passato allo smart working su dispositivi gestiti dall'azienda. Quando gli utenti hanno iniziato ad accedere ai dati e alle applicazioni che richiedevano i loro ruoli principalmente al di fuori della rete aziendale sicura, la superficie di attacco dell'organizzazione è cresciuta rapidamente.

Incidente ransomware riuscito

Poco dopo il passaggio a un modello di smart working, un attacco ransomware riuscito ha colpito un database Oracle Cloud critico della banca, che in seguito avrebbero scoperto essere stato originato da un ambiente VDI. La sicurezza e l'IT sapevano di dover agire rapidamente per limitare la perdita di dati finanziari sensibili. Inoltre, hanno capito che se non fossero stati in grado di determinare e proteggere il vettore di attacco originale, c'era un rischio reale che il ransomware si diffondesse lateralmente sia ai server di backup che all'ambiente di produzione dell'organizzazione. In tal caso, la banca avrebbe sicuramente subito significative perdite di dati e finanziarie.

La scelta di una soluzione

Akamai Guardicore Segmentation era già ampiamente utilizzato in altre aree della banca. Prima dell'attacco ransomware, la piattaforma era responsabile della gestione e dell'applicazione delle policy di segmentazione di oltre 23.000 server con carichi di lavoro che si estendevano su infrastrutture locali, virtuali, bare-metal e VDI, nonché ambienti container Azure e OpenShift.

Grande società di servizi finanziari

Settore
Servizi finanziari

Soluzione
Akamai Guardicore Segmentation

Risultati principali

- Mitiga la diffusione del ransomware tramite il movimento laterale
- Fornisce una visibilità granulare dei flussi di rete
- Protegge l'accesso remoto segmentando gli ambienti VDI
- Consente una risposta rapida agli incidenti

Akamai

Come soluzione di segmentazione basata su software, era stata utilizzata dalla banca in precedenza per realizzare diverse iniziative di sicurezza e conformità, tra cui la gestione dell'accesso alla jumpbox dell'amministratore e la segmentazione delle applicazioni Swift. Conoscendo la reputazione della piattaforma nel fornire un'eccellente visibilità e un rapido time-to-policy, il team di risposta si è rapidamente mosso per sfruttare le funzionalità di Akamai Guardicore Segmentation e affrontare la violazione.

Vantaggi di Akamai Guardicore Segmentation

Visibilità a livello di processi

Utilizzando la piattaforma, il team di risposta della banca ha esaminato i flussi di comunicazione storici. Ha tracciato l'introduzione iniziale del ransomware dalla connessione VDI remota di un amministratore di database che comunicava con un database Oracle Cloud.

Rapido time-to-policy

Dopo aver identificato il vettore di attacco, il team ha accelerato la segmentazione VDI, rendendola una priorità assoluta. Il processo di pianificazione delle policy è iniziato di sabato, utilizzando le funzionalità di visibilità di Akamai Guardicore Segmentation per individuare potenziali esigenze di policy. Entro il martedì successivo, la banca disponeva di policy applicabili per le oltre 3.000 connessioni VDI a Oracle Cloud.

Recupero dal ransomware

Il team ha implementato gli agenti Akamai sull'applicazione di backup e ha configurato l'isolamento dell'applicazione, definendo, fino al livello di processo, cosa poteva comunicare con la risorsa. È stata quindi eseguita l'implementazione nell'area violata, impedendo al ransomware di propagarsi ulteriormente, utilizzando regole di negazione globali.

Per ridurre il rischio aggiuntivo derivante dall'accesso dei lavoratori remoti, sono state inoltre impostate policy per le due soluzioni VDI utilizzate dai dipendenti del call center, impedendo ulteriormente il movimento laterale non autorizzato tra gli endpoint della banca.

L'applicazione della policy di segmentazione in soli tre giorni ha consentito all'organizzazione di servizi finanziari di ridurre considerevolmente l'impatto dell'incidente ransomware e di migliorare notevolmente la sicurezza dell'accesso remoto in futuro.

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

> La visibilità fornita da [Akamai Guardicore Segmentation] è stata come uno splendente raggio di luce che ha illuminato l'oscurità!
>
> Responsabile della sicurezza delle infrastrutture presso una grande società di servizi finanziari