DESCRIZIONE DELLA SOLUZIONE AKAMAI

Deloitte rafforza la risposta agli incidenti e la mitigazione dei ransomware con Akamai Guardicore Segmentation

Le sfide del cliente

Le categorie di prodotti per la sicurezza di comprovata validità promettono livelli sempre maggiori di protezione dalle minacce più recenti per le reti aziendali. Tuttavia, poche soluzioni sono riuscite ad offrire un metodo completo e unificato per ridurre la superficie di attacco garantendo la protezione dal movimento laterale dannoso, sia indirizzato o proveniente dai dispositivi hardware on-premise che originato da carichi di lavoro ospitati nel cloud, dispositivi degli utenti finali o container. Inoltre, il completamento dei primi progetti di segmentazione Zero Trust ha richiesto, storicamente, mesi, se non anni, di lavoro da parte delle aziende, a causa dei vincoli tecnologici e delle scarse competenze degli addetti all'esecuzione di progetti volti a bloccare gli attacchi nel caso in cui vengano bypassati i prodotti di sicurezza tradizionali, come firewall legacy, EDR e molti altri.

Durante l'approccio ai progetti di segmentazione, le aziende, di solito, si trovano ad affrontare i seguenti problemi:

- Mancanza di visibilità su tutte le risorse, i flussi di rete, gli utenti e le connessioni in tutti gli ambienti
- Limitazione dei controlli di sicurezza sulle varie tecnologie e infrastrutture utilizzate, come infrastrutture del cloud ibrido, sistemi operativi tradizionali e OT/IoT
- Necessità di garantire la continuità operativa evitando i problemi di downtime, che spesso si accompagnano con le tecniche di segmentazione tradizionali
- Carenza di talenti e risorse in tema di sicurezza in grado di creare, implementare e gestire i progetti che supportano il modello Zero Trust

Punti salienti della soluzione

Akamai Guardicore Segmentation è una soluzione di microsegmentazione basata su host che fornisce il modo più semplice, rapido e intuitivo per applicare i principi del modello Zero Trust alle reti. Usando un mix di sensori basati su agenti, strumenti di raccolta dei dati basati sulla rete e registri di flussi cloud privati e virtuali per mappare la vostra rete, Akamai Guardicore Segmentation è progettato per offrire un'unica vista di tutte le vostre risorse e infrastrutture, inclusi i sistemi operativi, la tecnologia operativa e i dispositivi IoT legacy e moderni. Da qui, potete facilmente creare e applicare policy in grado di limitare le comunicazioni indesiderate, ridurre la superficie di attacco e garantire la continuità operativa.

I principali casi di utilizzo

- **Controlli del traffico est-ovest**
  Separate ambienti, applicazioni, utenti e infrastrutture che non devono comunicare tra loro
- **Mitigazione dei ransomware**
  Implementate modelli di policy con AI/ML in grado di bloccare i percorsi degli attacchi che vengono utilizzati da vari tipi di attacchi ransomware
- **Isolamento delle applicazioni**
  Focalizzatevi sulle specifiche dipendenze delle vostre applicazioni business-critical per creare rigorosi controlli di sicurezza

- **Segmentazione basata sugli utenti**
  Impedite agli utenti non autorizzati di accedere ad applicazioni, ambienti e dispositivi che non sono essenziali per il loro lavoro
- **Isolamento dei dispositivi infettati**
  Limitate la diffusione di una violazione nel caso in cui siano stati compromessi uno o più dispositivi
- **Conformità**
  Preparatevi a dimostrare immediatamente la vostra conformità con una profonda comprensione contestuale della rete, dei dispositivi e dei percorsi dei potenziali attacchi

Vantaggi per il cliente

- Risolvere i problemi di visibilità con una visione unificata della vostra rete e delle vostre connessioni, inclusi server, endpoint, cloud, container, utenti e molto altro
- Applicare le policy Zero Trust per mitigare la possibilità di riuscita di un attacco ransomware
- Ridurre i tempi di risposta agli incidenti tramite l'intelligence sulle minacce e complete funzionalità di individuazione e rilevamento delle violazioni
- Semplificare l'analisi di rete e i progetti di conformità tramite funzioni cronologiche e in tempo reale

Le competenze di Deloitte

1. **Consulenza**
   L'esperienza di Deloitte nel supporto decisionale in materia di cybersicurezza nelle analisi delle lacune di sicurezza e nella creazione di una roadmap di implementazione garantisce ai clienti aziendali di prendere decisioni oculate durante le violazioni e per le future pianificazioni
2. **Servizi professionali**
   Provate i servizi di implementazione totalmente gestiti, nonché le operazioni di integrazione personalizzate per le vostre soluzioni di sicurezza, ITSM e cloud
3. **Servizi gestiti di risposta agli incidenti**
   Un'eccellente assistenza immediata fornita dal team di risposta agli incidenti di Deloitte per limitare l'impatto delle violazioni e aiutare a prevenire incidenti futuri
4. **Sottoscrizioni licenze**
   Deloitte offre un'ampia gamma di sottoscrizioni di licenze da acquistare

Case study dei clienti - In che modo Akamai e Deloitte risolvono i problemi dei clienti legati ai ransomware

La maggior parte degli attacchi ransomware hanno costretto i clienti a cercare consulenza e soluzioni in grado di aiutarli immediatamente nel momento critico. Le funzionalità dei team di sicurezza e risposta agli incidenti di Deloitte, che utilizzano la visibilità della rete, l'analisi delle violazioni e le conseguenti misure necessarie per ridurre la superficie di attacco fornite da Akamai Guardicore Segmentation, hanno prodotto una combinazione vincente per questi clienti.

Background

Un cliente aziendale aveva subito un pesante attacco ransomware con l'interruzione delle sue attività fondamentali, che non sapeva come affrontare. I criminali avevano assunto il controllo dell'intero data center dell'azienda, costituito da migliaia di server, e la violazione doveva essere isolata immediatamente in modo sicuro. Affidandosi a Deloitte, il cliente aveva chiamato per chiedere consigli su come procedere. Con il team di Deloitte già pronto per offrire e implementare la soluzione Akamai Guardicore Segmentation, il cliente è riuscito ad ottenere rapidamente visibilità sulla portata dell'attacco, a comprendere le risorse e le applicazioni coinvolte e a individuare tutte le dipendenze delle applicazioni correlate.

Soluzione

Associando l'intero ambiente del cliente fino al livello dei singoli processi, la soluzione Akamai Guardicore Segmentation è riuscita a rivelare tutti i potenziali percorsi seguiti dal malware nell'infrastruttura violata, consentendo al team di Deloitte di focalizzarsi su parti specifiche della rete per condurre un'ulteriore analisi approfondita. In tal modo, il cliente ha potuto ripristinare le sue attività aziendali e accedere al suo data center con la certezza di aver rimosso qualsiasi dispositivo compromesso.

I risultati

Una volta risolto l'attacco ransomware, ritornato il data center online e ripristinate le attività aziendali, sono state intraprese le misure necessarie per evitare che un simile attacco possa ripetersi nuovamente. Come molte aziende, questo cliente utilizza un approccio alla sicurezza multilivello con l'implementazione di diverse soluzioni per la protezione di dispositivi, applicazioni, utenti, ecc. Tuttavia, poiché il gateway per un criminale può essere semplice come inviare un'e-mail di phishing, queste soluzioni da sole non sono sufficienti per fermare l'attacco. Con una visibilità completa, che include rete, dipendenze delle applicazioni e utenti che accedono al data center, il cliente è riuscito ad implementare accurati controlli di microsegmentazione in grado di ridurre notevolmente i percorsi che un futuro attacco ransomware potrebbe seguire.

Una volta provato il valore della soluzione, la fiducia del cliente nei confronti delle competenze di Deloitte è aumentata, il che l'ha portato a decidere di mantenere la soluzione per fornire la segmentazione Zero Trust, richiedendo a Deloitte di gestire quotidianamente la tecnologia per conto suo.

Riepilogo

Le profonde competenze tecniche e l'esperienza di Deloitte nell'esecuzione di progetti Zero Trust l'ha resa un partner ideale per l'implementazione e la gestione della soluzione Akamai Guardicore Segmentation per i clienti. I clienti possono affidarsi a Deloitte per utilizzare questa tecnologia in qualsiasi progetto di sicurezza, incluse operazioni di riduzione della superficie di attacco, controlli dello spostamento laterale, misure di contenimento delle applicazioni o mitigazione dei ransomware.

Informazioni su Deloitte

Deloitte fornisce innovativi servizi di controllo, consulenza, fisco e supporto a molti dei più famosi brand al mondo, tra cui quasi il 90% delle aziende Fortune 500® e a più di 7.000 società private. I nostri dipendenti collaborano per il bene dell'azienda e operano nei settori industriali che favoriscono e plasmano il mercato odierno, fornendo risultati tangibili e duraturi in grado di aiutare a rafforzare la pubblica fiducia nei nostri mercati dei capitali, ispirare i clienti a considerare le sfide come opportunità per trasformare e far prosperare le cose e guidare i processi volti a realizzare un'economia più solida e una società più sana. Deloitte è orgogliosa di far parte della rete di servizi professionali più grande al mondo con clienti che operano nei mercati più importanti per l'azienda. Con oltre 175 anni di attività, la nostra rete di aziende associate si espande in più di 150 paesi e territori in tutto il mondo. Scoprite come collaborano i 415.000 dipendenti di Deloitte a livello mondiale su deloitte.com.

Contatti

Ola Sergatchov
Responsabile del reparto Global Strategic Alliances di Akamai
osergatc@akamai.com

 | Supporto | Data di pubblicazione: 3/24