La microsegmentazione è l'ago della bilancia del modello Zero Trust nel settore del commercio

Le organizzazioni commerciali che operano nei settori del retail, dei viaggi e del turismo rappresentano obiettivi allettanti per criminali informatici, gang di ransomware e truffatori intenzionati a trarre profitto da dati aziendali o finanziari sensibili. Secondo il rapporto RH-ISAC di Industry Insights, i tipi più comuni di informazioni oggetto di furto includono i dati delle carte di credito e pagamento, le informazioni di identificazione personale (PII) ricavate dai programmi premi e fedeltà e la proprietà intellettuale.

Già prese di mira dai criminali, queste organizzazioni (e i loro team addetti alla sicurezza) devono fare i conti con molti punti da cui i criminali possono accedere alle loro reti per lanciare attacchi ransomware e altri tipi di malware. Tutte le organizzazioni si trovano ad affrontare le conseguenze di e-mail di phishing, credenziali VPN rubate ed exploit zero-day, ma molte società commerciali devono gestire gli ulteriori rischi introdotti da chioschi, dispositivi IoT, tablet presenti nei negozi, terminali POS, Wi-Fi guest e molto altro! A complicare la situazione, ogni punto vendita, che deve essere aperto al pubblico per poter svolgere le proprie attività commerciali, espone un'azienda a una superficie di attacco fisica e a un'intera gamma di altre minacce.

La redditività dei dati e i numerosi vettori di attacco aumentano la posta in gioco per gli addetti alla sicurezza che devono porre rimedio alla principale causa degli incidenti, ovvero all'errore umano, che causa l'82% dei problemi di sicurezza. Un maggiore controllo normativo da parte del settore delle carte di pagamento (PCI) o delle normative governative (GDPR, SEC, ecc.) aggiunge pressione e consuma ulteriormente le risorse e i budget destinati alla sicurezza IT, di per sé già limitati.

Anche se eliminare tutti i rischi è impossibile, le società commerciali di oggi devono adottare un atteggiamento mentale volto a "presupporre una violazione" per rilevare e fermare rapidamente la diffusione di un'inevitabile infezione o raggiro delle difese perimetrali. Le soluzioni di segmentazione Zero Trust di Akamai rendono più semplice e veloce per le società commerciali proteggere applicazioni, server e ambienti di rete, prevenendo, al contempo, la crittografia e l'esfiltrazione di dati sensibili.

La microsegmentazione, una funzionalità potenziata al meglio da un approccio definito dal software, fornisce un fondamento essenziale per i sistemi di sicurezza Zero Trust offrendo tre funzionalità chiave per le organizzazioni commerciali. Innanzitutto, la microsegmentazione limita naturalmente le potenziali conseguenze negative derivanti da un'infezione ransomware bloccando il movimento laterale. In secondo luogo, la microsegmentazione può contribuire a ridurre i costi necessari per raggiungere e mantenere la conformità allo standard PCI. Infine, la microsegmentazione offre i livelli di visibilità granulare e copertura necessari per proteggere gli ecosistemi moderni, ma più complessi, degli ambienti ibridi, multicloud e dei microservizi, nonché delle infrastrutture tradizionali.

Limitazione delle potenziali conseguenze negative dei ransomware

La selezione di un collegamento di phishing contenuto in un'e-mail, l'errata configurazione delle impostazioni di sicurezza oppure la presenza di porte RDP aperte o di credenziali violate offrono regolarmente ai criminali la possibilità di accedere ad una rete per cercare le preziose risorse di un'organizzazione in vista di un attacco ransomware. Le società che rimangono vittime di un evento di crittografia di massa (e di una possibile doppia estorsione tramite l'esfiltrazione di dati) subiscono molteplici livelli di perdite finanziarie e danni alle attività aziendali.

Le perdite commerciali dirette potrebbero verificarsi immediatamente quando gli ordini online e le operazioni del negozio si rallentano o si bloccano, impedendo ai clienti di acquistare articoli oppure di effettuare prenotazioni di hotel o voli. Le operazioni di e-commerce potrebbero non essere in grado di elaborare, evadere o spedire gli ordini esistenti, poiché i sistemi e i server critici diventano inaccessibili o vengono disconnessi nel tentativo di limitare la diffusione di un attacco.

Le perdite commerciali indirette comportano l'imbarazzo pubblico e i danni alla reputazione del brand in caso di violazione dei dati sensibili dell'azienda o dei clienti. Come tattica preferita, le gang di ransomware pubblicizzano gli attacchi ed esfiltrano i dati come prova su siti "name and shame" per aumentare ulteriormente la pressione sulle vittime a scopo di estorsione. I recenti requisiti della SEC obbligano, inoltre, le organizzazioni ad inviare una notifica all'agenzia entro quattro giorni relativamente ad eventuali impatti materiali subiti, il che fa notizia, oltre a provocare danni alla reputazione.

I costi di ripristino per le spese legali, la risposta agli incidenti, l'analisi forense dei dati e la risoluzione delle violazioni direttamente correlate al ripristino dopo un attacco ransomware sono elevati perché implicano un notevole lavoro da parte di consulenti e team IT per recuperare i dati, ripristinare le copie di backup e riportare online i sistemi. Tuttavia, anche queste spese possono essere superate dai costi dei contenziosi o dalle multe e dalle sanzioni normative causate dalla violazione di informazioni sensibili. I premi assicurativi informatici potrebbero aumentare notevolmente, i pagamenti delle richieste di risarcimento causate dai ransomware potrebbero essere negati o la copertura potrebbe essere eliminata del tutto.

La posta in gioco è molto alta e non sorprende che gli attacchi ransomware siano stati citati come la principale preoccupazione per il 2024 dai CISO che operano nel settore alberghiero e nel retail e che i responsabili della sicurezza siano pronti a investire in controlli in grado di aiutare a ridurre i rischi una volta che i criminali hanno preso piede nei sistemi presi di mira. Tuttavia, per diffondere il ransomware, i criminali devono essere in grado di attivare il movimento laterale una volta ottenuto l'accesso iniziale per ottenere il massimo impatto. Il rapporto sulla difesa digitale di Microsoft per il 2022 rileva come il 93% degli incidenti ransomware sia il risultato di controlli inadeguati del movimento laterale che hanno consentito ai criminali di bloccare applicazioni e infrastrutture critiche e che il tempo medio impiegato da un criminale per attivare il movimento laterale da un endpoint all'interno della rete aziendale sia solo di un'ora e 42 minuti.

I recenti dati sullo stato della segmentazione di Akamai hanno rivelato come il numero più alto di attacchi ransomware negli ultimi 12 mesi sia stato segnalato dalle società di e-commerce rispetto alle aziende di altri settori industriali. Ecco perché CISO ed esperti di sicurezza stanno adottando strumenti di sicurezza basati sul modello Zero Trust, come la microsegmentazione, per ridurre il rischio di un'infezione da ransomware, ridurre al minimo le superfici di attacco e "rompere" la kill chain dei ransomware.

Rilevando e bloccando la possibilità di attivare il movimento laterale, i criminali avranno difficoltà ad accedere alle risorse IT necessarie per l'escalation dei privilegi, ad individuare informazioni sensibili e a propagare gli attacchi ransomware su larga scala. Applicando i principi dell'accesso basato sul privilegio minimo ai carichi di lavoro critici nell'intera infrastruttura commerciale, la soluzione di microsegmentazione di Akamai, apprezzata dagli analisti, offre una visibilità approfondita sui flussi di dati est-ovest di applicazioni e carichi di lavoro, nonché una protezione granulare tramite policy definite da software per limitare il movimento laterale e fermare i criminali nel loro cammino.

Anche le principali compagnie di assicurazioni informatiche si rendono conto del valore della microsegmentazione. Poiché i ransomware favoriscono sia gli acquisti che l'aumento dei sinistri, molti assicuratori sono stati costretti ad aumentare i requisiti e i controlli di sicurezza, ad incrementare i premi assicurativi (a volte fino al 96% all'anno) e a ridurre i limiti di copertura del pagamento delle richieste di risarcimento per contenere le notevoli perdite. Alcune aziende vengono addirittura escluse dal mercato delle assicurazioni informatiche o viene loro negata del tutto la copertura. Sebbene l'assicurazione informatica da sola non sia in grado di prevenire un'intrusione devastante e le conseguenti ricadute finanziarie, esistono controlli di sicurezza (come la microsegmentazione), che consentono alle organizzazioni di soddisfare più facilmente i più recenti requisiti sottoscritti.

"Con un singolo agente su un computer, abbiamo risolto definitivamente il problema di un attacco all'endpoint tramite il movimento laterale."

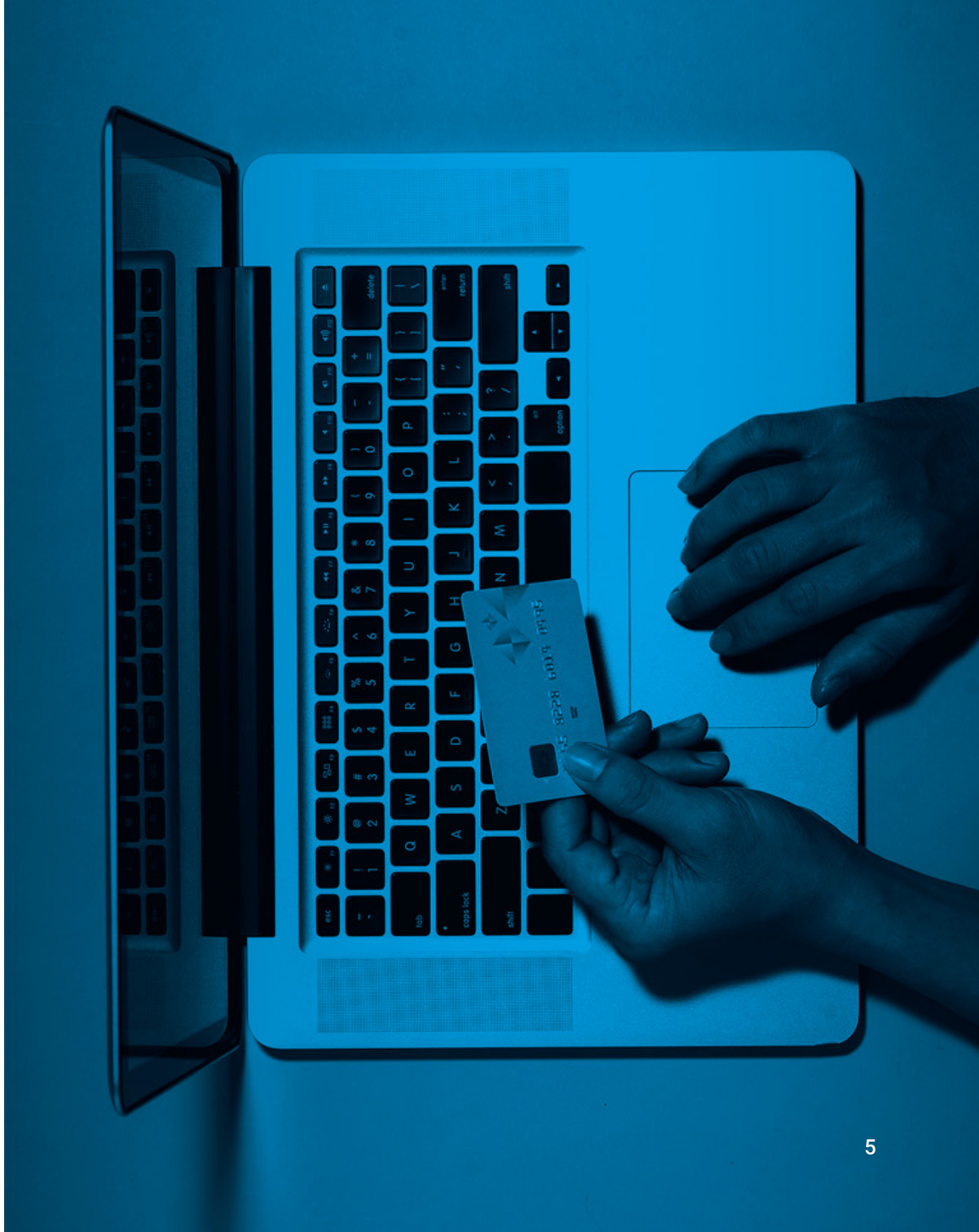
Infrastructure Architect
in un'azienda globale di retail e beni di consumo

Riduzione dell'ambito degli audit di conformità al PCI

Come le società di e-commerce ben sanno, raggiungere e mantenere la conformità al PCI rappresenta una parte considerevole dei budget annuali destinati alle questioni di governance, rischio e conformità, che può implicare un onere significativo per FTE e risorse di sicurezza. Lo standard PCI Data Security (PCI DSS) richiede audit continui delle policy e dei controlli di sicurezza adottati per proteggere l'ambiente dei dati dei titolari di carte di credito (CDE). L'ambito del PCI, che si riferisce all'identificazione di persone, processi e tecnologie che interagiscono o potrebbero altrimenti avere un impatto sulla sicurezza dei dati dei titolari di carta (CHD), può anche aumentare notevolmente i costi associati alla conduzione di un audit richiesto dal PCI.

Sebbene la segmentazione della rete non sia un requisito ufficiale del PCI DSS, le organizzazioni commerciali utilizzano da anni metodi tradizionali di segmentazione della rete, come vLAN, ACL e firewall interni, per contribuire a ridurre la portata, i costi, le difficoltà e i rischi correlati nell'intento di mantenere la conformità. Tuttavia, poiché gli ambienti IT dei retailer moderni sono diventati più dinamici grazie alla presenza di architetture ibride, multicloud e di microservizi, le tecnologie e le tecniche di segmentazione tradizionali non riescono a tenere il passo con queste innovazioni, causando costi operativi, complessità e tempi di downtime delle applicazioni, nonché falle nella sicurezza.

Questi problemi si verificano perché i metodi di segmentazione tradizionali sono complicati da gestire e mantenere, in quanto consumano risorse per garantire che sistemi, reti e applicazioni all'interno dei confini del CDE siano adeguatamente protetti e controllati. Poiché le organizzazioni operano dal data center e dal cloud fino alle risorse basate sui container, molte di esse non hanno una visibilità completa sui flussi di comunicazione di applicazioni e sistemi e hanno difficoltà a mantenere gli standard di configurazione del firewall richiesti dal PCI.



Di conseguenza, adottano pratiche di segmentazione inadeguate che possono creare falle nella sicurezza, portando ad un mancato superamento degli audit richiesti dal PCI. Ecco perché le organizzazioni commerciali stanno adottando la segmentazione definita dal software per separare più facilmente il CDE dai sistemi che non rientrano nell'ambito delle infrastrutture, ridurre la portata di un audit richiesto dal PCI e accelerare la conformità consentendo la segmentazione e l'applicazione fino al livello 7, che va ben oltre ciò che gli strumenti tradizionali possono supportare. L'agile agente di Akamai non richiede di utilizzare firewall, apportare modifiche alla rete o riavviare i server e funziona indipendentemente dall'infrastruttura sottostante, il che elimina eventuali tempi di downtime delle applicazioni e finestre di manutenzione o controllo delle modifiche.

Poiché la segmentazione definita dal software scollega il sistema di sicurezza dall'infrastruttura e dai sistemi operativi sottostanti, è possibile eseguirla in modo indipendente, senza influire su reti o applicazioni. Adottando questo approccio, le organizzazioni commerciali possono ottenere una visibilità granulare sulla rete e sulle risorse in tutti gli ambienti, con una soluzione che funge da firewall stateful inspection distribuito, per ottenere una copertura completa. Inoltre, grazie alla minore quantità di risorse e sforzi necessari per l'implementazione e la gestione, insieme ad un miglioramento del 95% circa nella produttività del team SecOps, le organizzazioni possono raggiungere un maggior livello di sicurezza, evitando, al contempo, i numerosi grattacapi causati dalle operazioni di conformità al PCI. Come ulteriore vantaggio, la nostra soluzione consente alle organizzazioni commerciali di sfruttare le viste cronologiche e in tempo reale della rete per convalidare la conformità durante gli audit.

> "La segmentazione definita dal software ci ha consentito di creare e applicare policy di segmentazione a livello di processi, migliorando notevolmente la nostra strategia di sicurezza e la nostra capacità di soddisfare i requisiti tecnici dello standard PCI-DSS."
>
> Sr. Infrastructure Engineer, Honey Baked Ham

Visibilità e copertura sull'IoT fino all'infrastruttura tradizionale

Dall'arresto della diffusione dei ransomware alla gestione dei controlli di sicurezza per garantire la conformità al PCI, le organizzazioni commerciali devono affrontare anche l'ulteriore difficoltà di proteggere luoghi fisici come punti vendita, impianti di produzione e magazzini di distribuzione. Per le compagnie aeree, i sensori e i dispositivi IoT possono consentire il monitoraggio in tempo reale e la manutenzione predittiva dei sistemi aeronautici per migliorare le performance e la sicurezza. Le organizzazioni del settore alberghiero utilizzano dispositivi basati sull'IoT per connettere le camere d'albergo intelligenti progettate per favorire le customer experience e l'efficienza operativa.

È chiaro che molti di questi luoghi e ambienti contengono una miriade di risorse dell'IoT (Internet of Things) o della tecnologia operativa (OT) che non possono eseguire agenti di sicurezza basati su host, il che li rende ancora più soggetti alle vulnerabilità di hardware e software. La ricerca sullo stato della sicurezza dell'IoT pubblicata da Forrester nel 2023 ha rivelato che il 33% dei responsabili della sicurezza a livello globale ha citato i dispositivi IoT come l'obiettivo privilegiato dagli attacchi informatici provenienti dall'esterno. Pertanto, le organizzazioni devono implementare una soluzione di segmentazione con funzionalità senza agenti in grado di proteggere gli ambienti IoT e OT, riducendo, nello stesso tempo, al minimo il rischio che un criminale riesca a sfruttare la vulnerabilità di un dispositivo per ottenere l'accesso alla più ampia infrastruttura IT.

Questo tipo di soluzione deve essere in grado di monitorare continuamente i nuovi dispositivi connessi e impedire automaticamente ai dispositivi non autorizzati di comunicare con la rete. Tramite la funzione integrata di fingerprinting dei dispositivi, la soluzione di Akamai rileva e classifica automaticamente i dispositivi connessi in gruppi logici che costituiscono la base per formare policy di sicurezza astratte e scalabili. È possibile creare policy di segmentazione per i dispositivi IoT e OT tramite un'interfaccia unificata, che, come altre policy, seguono il dispositivo a cui è stato assegnato un ID digitale indipendentemente dalla posizione in cui si trova (anche se il dispositivo si sposta verso nuove posizioni di rete) o dal numero di dispositivi presenti nell'ambiente.

Le policy basate sul modello Zero Trust vengono applicate tramite ACL dello switch di rete senza la necessità di un agente, il che elimina eventuali lacune che possono creare rischi nelle implementazioni di dispositivi IoT e OT. Stabilire questi confini sicuri consente comunque di effettuare le connessioni necessarie ai sistemi di gestione IT, ai server di aggiornamento dedicati e ai server di registrazione per ridurre i problemi di sicurezza. La nostra soluzione consente di scoprire, visualizzare e mappare tutti i sistemi IoT e OT insieme all'infrastruttura IT per ottenere un'unica vista delle proprie risorse aziendali.

Oltre a proteggere le risorse IoT/OT e altri endpoint isolati, molti retailer si affidano notoriamente a sistemi, applicazioni e server eseguiti su sistemi operativi e infrastrutture meno recenti o non più supportati a cui, pertanto, non è possibile applicare patch, il che crea notevoli rischi. Molti di questi server tradizionali non possono essere rimossi perché risultano ancora redditizi per l'organizzazione o sono fondamentali per l'azienda, in particolare per le società di e-commerce che non sono nate nel cloud. Con i massimi livelli di copertura e compatibilità leader del settore, gli agenti di Akamai vengono eseguiti su sistemi operativi moderni e tradizionali, fornendo piena visibilità sui flussi di rete a livello di processi e servizi per i sistemi operativi Windows e Linux, insieme alla copertura degli endpoint MacOS.

Altre soluzioni forniscono solo una visibilità parziale per i sistemi operativi tradizionali, senza alcuna visibilità sui sistemi Microsoft Windows precedenti alla versione Windows Server 2008 R2. Ciò è dovuto al fatto che l'agente delle soluzioni di microsegmentazione tradizionali si basa su un firewall Windows in grado di applicare le policy, che era disponibile solo nei sistemi successivi alla versione 2002. Gli agenti per i sistemi Linux supportano solo la visibilità di livello 4, senza regole a livello di processo L7 per gli ambienti Linux, e dipendono da iptables per applicare le policy. La funzionalità Akamai Guardicore Segmentation è supportata su quasi tutti i sistemi operativi Windows e Linux, nuovi e tradizionali, poiché il funzionamento di questa soluzione non dipende dall'infrastruttura sottostante.

Semplice, veloce, intuitiva e più sicura

Dalla sede centrale al negozio retail, dal data center al cloud e non solo, la microsegmentazione è fondamentale per l'adozione del modello Zero Trust nell'intento di salvaguardare e proteggere le risorse IT critiche.

La semplicità di Akamai Guardicore Segmentation riduce notevolmente il tempo e il livello di impegno necessari per l'implementazione e l'applicazione delle policy, il monitoraggio e la risposta agli incidenti rispetto ai metodi di segmentazione della rete tradizionali, che sono più lenti. È possibile implementare rapidamente eventuali cambiamenti alle policy senza apportare complesse modifiche alla rete, il che può assumere un ruolo cruciale durante i periodi di picco delle vendite, le promozioni, il lancio di prodotti o altri eventi importanti.

Conclusione: proprio come non chiedereste mai ai vostri clienti, ospiti o passeggeri di scegliere tra qualità e sicurezza, una buona soluzione di microsegmentazione non vi chiederà mai di scegliere tra sicurezza e agilità. È ora di smettere di segmentare nel modo tradizionale.

Volete saperne di più?

Scoprite come ridurre la superficie di attacco, proteggere le applicazioni critiche e semplificare la conformità con Akamai Guardicore Segmentation, parte della gamma di prodotti Akamai Zero Trust.

Ulteriori informazioni

TechnologyAdvice | Akamai

Akamai protegge l'experience dei vostri clienti, dipendenti, sistemi e dati aiutandovi ad integrare la sicurezza in tutti i vostri prodotti, ovunque vengano creati e distribuiti. La visibilità della nostra piattaforma sulle minacce globali ci aiuta ad adattare e a migliorare la vostra strategia di sicurezza (per favorire l'adozione del modello Zero Trust, bloccare i ransomware, proteggere app e API o contrastare gli attacchi DDoS), offrendovi la sicurezza necessaria per concentrarvi sull'innovazione, sull'espansione e sulla trasformazione dell'azienda in modo continuativo. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito akamai.com o akamai.com/blog, e seguite follow Akamai Technologies su X (in precedenza Twitter) e LinkedIn.