Akamai

EBOOK

Stato della segmentazione

Agevolare l'implementazione è un processo risolutivo

Settore dell'e-commerce

Sommario

Introduzione

I team addetti alla sicurezza IT (specialmente quelli che difendono le società di e-commerce) non hanno mai avuto vita facile. Da sempre budget ridotti e risorse di sicurezza limitate impongono agli addetti alla sicurezza aziendale di dover fare di più con meno. Oggi però, criminali sempre più sofisticati e altamente motivati, insieme alla gestione di un'infrastruttura sempre più complessa, mettono i team addetti alla sicurezza sotto una nuova pressione. Le società di e-commerce operano basandosi su una presenza online performante, pertanto una violazione riuscita, come un attacco ransomware, può causare danni ingenti, se non irreparabili, alla reputazione del brand e al fatturato. Immaginate l'impatto devastante che potrebbe avere un'interruzione delle operazioni online, dei processi di evasione degli ordini o delle linee di produzione in seguito alla mancata disponibilità di server e sistemi di importanza critica a causa di un evento di crittografia di massa ed, eventualmente, ad un tentativo di doppia estorsione tramite l'esfiltrazione dei dati.

Come dimostrano i risultati di questo rapporto sullo stato della segmentazione nel settore dell'e-commerce, gli attacchi stanno avendo un impatto perfino maggiore, aumentando la pressione sui responsabili affinché scelgano le soluzioni e gli strumenti giusti per mantenere protetti i dati critici, senza sacrificare le performance o aumentare i costi operativi. Secondo il rapporto, l'e-commerce è il settore maggiormente preso di mira per tutti gli intervistati, il che evidenzia l'urgenza di prevenire, rilevare e rispondere il più rapidamente possibile ad un attacco ransomware per contenerne le conseguenze.

Gli intervistati che operano in società di e-commerce (in tutte le aree geografiche, inclusi Stati Uniti, America Latina, EMEA e APAC) concordano in modo schiacciante sull'efficacia della segmentazione nel mantenere le risorse IT protette, ma i loro progressi complessivi nell'implementazione in applicazioni, server e sistemi aziendali di importanza critica sono stati inferiori alle aspettative. Gli ostacoli principali per le società di e-commerce sono stati rappresentati da una mancanza di competenze idonee a implementare la segmentazione in modo efficace e l'onere di ottemperare ai requisiti di conformità dei dati. Non solo quindi i team faticano ad assumere o mantenere i necessari talenti nel loro settore, ma impiegano tempo prezioso a cercare di garantire la conformità normativa, consumando ulteriormente le risorse già sottoposte a notevoli pressioni.

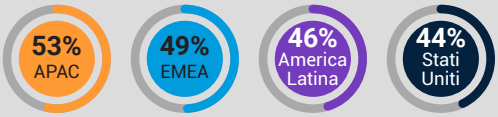
La buona notizia? Perseverare e scegliere la soluzione più adatta dà i suoi frutti. Per coloro che hanno segmentato la maggior parte delle risorse critiche in sei importanti aree aziendali, la segmentazione ha dimostrato di avere un effetto trasformativo sulle funzionalità di difesa, consentendo di mitigare e contenere i ransomware 11 ore più velocemente rispetto a coloro che avevano segmentato solo una risorsa. Immaginate la differenza che possono fare quelle 11 ore non solo per i vostri addetti alla sicurezza, ma anche per i vostri clienti e per la reputazione del vostro brand.

La segmentazione mostra nel complesso lenti progressi, ma coloro che hanno perseverato hanno ridotto enormemente il rischio

La segmentazione va bene. La microsegmentazione è ancora meglio.

La segmentazione è un approccio architetturale che divide una rete in segmenti più piccoli per migliorare la sicurezza e ridurre i rischi associati alle reti flat; inoltre, viene usata per contribuire a ridurre l'ambito, le complessità e i costi connessi al raggiungimento e al mantenimento della conformità al PCI da parte delle società basate sull'e-commerce.

La microsegmentazione è una tecnica di sicurezza definita dal software che divide in modo logico una rete in segmenti separati fino al livello dei singoli carichi di lavoro o processi (livello 7). È possibile quindi definire la delivery di servizi e controlli di sicurezza per ciascun segmento ad un livello più granulare rispetto ai metodi di segmentazione tradizionali come VLAN, ACL e firewall interni che offrono solo un controllo di livello 4. Ecco perché il 94% degli intervistati che operano nel settore dell'e-commerce preferisce le soluzioni di segmentazione basate sul software rispetto ai metodi tradizionali.



I responsabili decisionali della sicurezza nell'APAC sono più propensi ad affermare che la segmentazione della rete è estremamente importante per garantire la sicurezza delle loro organizzazioni rispetto a quelli nell'area EMEA, in America Latina o negli Stati Uniti. I responsabili decisionali della sicurezza in America Latina sono più propensi ad affermare che la microsegmentazione è la priorità assoluta (42%) rispetto alle controparti nell'APAC (35%), negli Stati Uniti (34%) e nell'area EMEA (26%).

L'e-commerce è il settore maggiormente preso di mira e gli attacchi ransomware continuano ad aumentare

Negli ultimi 12 mesi, sono stati sferrati contro le società di e-commerce, in media, 167 attacchi ransomware (riusciti o meno). Questo dato non solo posiziona l'e-commerce in cima all'elenco dei settori che hanno subito, in media, il maggior numero di attacchi ransomware, ma è circa il doppio di quello registrato dal settore più vicino (l'edilizia con una media di 89 attacchi).

I criminali informatici sono più propensi a prendere di mira le società di e-commerce negli Stati Uniti: il numero di attacchi ransomware è più alto negli Stati Uniti rispetto a tutte le altre aree geografiche, con una media di 312 attacchi negli ultimi 12 mesi, rispetto ai 119 attacchi nell'APAC, ai 91 attacchi nell'area EMEA e ai 68 attacchi in America Latina (1).

Numero medio di attacchi ransomware sferrati contro le società di e-commerce negli ultimi 12 mesi per area geografica

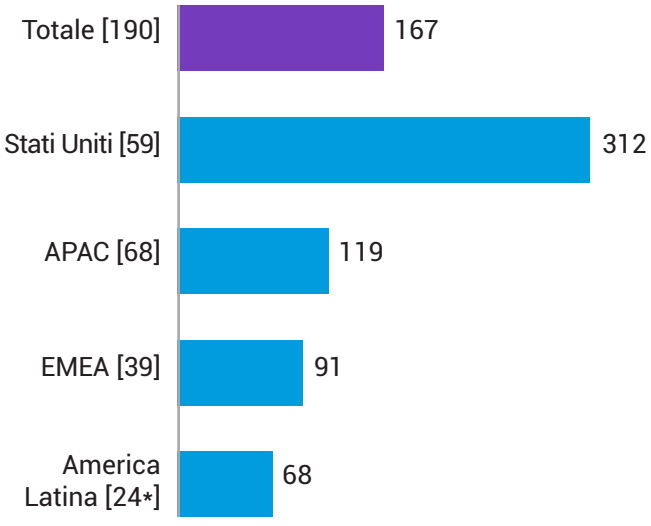


Figura 1. Quanti attacchi ransomware hanno colpito la vostra organizzazione negli ultimi 12 mesi (indipendentemente dal fatto che siano andati a buon fine)? Il grafico mostra il numero medio di attacchi negli ultimi 12 mesi, suddivisi per area geografica (dati relativi solo al settore dell'e-commerce).

* Attenzione: dimensioni di base inferiori a 30

Anche se i valori medi nelle varie aree geografiche al di fuori degli Stati Uniti non possono essere descritti come bassi, sono in grado di eclissare il numero di attacchi sferrati contro gli Stati Uniti. Gli Stati Uniti, la maggiore potenza economica al mondo, sono il pæse che ha subito il maggior numero di attacchi ransomware e i criminali hanno preso frequentemente di mira altri pæsi occidentali e di lingua inglese. Anche le motivazioni geopolitiche svolgono un ruolo fondamentale sui pæsi e sui settori maggiormente colpiti. Le società di e-commerce sono spesso nel mirino dei criminali perché, tradizionalmente, dispongono di un livello di sicurezza inferiore rispetto ad altri settori come i servizi finanziari, il che le rende, pertanto, un bersaglio più semplice. Oltre alla pressione esercitata, un attacco ransomware riuscito può risultare altamente pubblico, specialmente se le organizzazioni vengono colpite durante i periodi in cui raggiungono il massimo fatturato, come nelle vacanze natalizie, in occasione di festività, manifestazioni sportive, il rientro a scuola o altri eventi di picco degli acquisti, il che rende più probabile ricavare profitto (nella mente del criminale) in caso di interruzione delle attività aziendali.

Nonostante l'elevato numero di attacchi ransomware sferrati contro le società di e-commerce, la segmentazione è stata implementata ad un livello ancora inadeguato. Solo l'11% di queste società ha segmentato più di due aree aziendali, in modo ampiamente coerente in tutte le aree geografiche, a indicare che molte di queste società dispongono di risorse limitate rispetto a quanto richiesto per gestire i problemi e gli attacchi man mano che si verificano.

Gli attacchi ransomware sferrati contro il settore dell'e-commerce possono avere un impatto enorme e immediato sulle attività aziendali (Figura 2): i nostri intervistati affermano di aver subito perdite finanziarie e danni alla reputazione, che aumentano entrambi notevolmente la pressione esercitata sui team addetti alla sicurezza nelle società di e-commerce. Si è osservato anche un aumento nella percentuale degli intervistati che segnalano premi assicurativi più alti a dimostrare il livello di rischio in cui possono incorrere le società di e-commerce, che spesso conservano i dati personali sugli utenti e sulle loro abitudini di acquisto, oltre ai rischi legati a problemi logistici con le scorte o il warehousing.

L'impatto esercitato varia a seconda dell'area geografica: gli intervistati dell'area APAC sono particolarmente propensi a sottolineare il fatto di aver subito perdite finanziarie, aspetto segnalato da oltre la metà dei soggetti (51%) rispetto alla media complessiva del 42%. Gli intervistati negli Stati Uniti, invece, sono maggiormente propensi a segnalare problemi di downtime della rete, indicati da quasi la metà delle persone interrogate (49%) rispetto alla media complessiva del 39%. Gli intervistati dell'UE sono più propensi a segnalare come impatto la riduzione del morale nei dipendenti (41% rispetto alla media complessiva del 36%).

Vediamo l'effetto di questa pressione anche in termini di strategia: il numero di società di e-commerce che aggiornano continuamente le strategie o le policy di cybersicurezza è passato dal 3% nel 2021 al 13% nel 2023, in risposta non solo ai ransomware, ma anche ad una superficie di attacco in costante evoluzione. L'incremento della complessità dell'infrastruttura e la migrazione dei carichi di lavoro nel cloud sono solo alcuni dei fattori di rischio che influenzano quotidianamente le strategie e i team addetti alla sicurezza.

Impatto dei ransomware/attacchi informatici sulle società di e-commerce

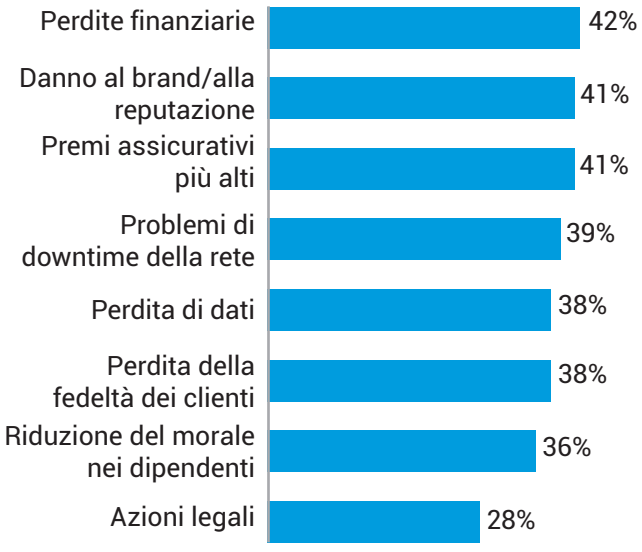
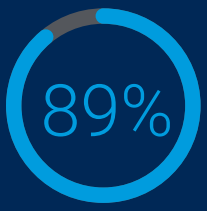


Figura 2. Quando è stato rilevato in precedenza un ransomware o un altro attacco informatico, quali dei seguenti impatti ha avuto sulla vostra organizzazione? Il grafico non mostra tutte le opzioni di risposta (dati relativi solo al settore dell'e-commerce).

La segmentazione è ampiamente riconosciuta come parte importante della strategia Zero Trust

I nostri intervistati concordano sull'importanza della segmentazione nel garantire la sicurezza delle loro organizzazioni e, in particolare, nell'affrontare i malware.



Quasi la metà degli intervistati (48%) afferma che la segmentazione è estremamente importante e l'89% di essi ritiene che sia fondamentale per contribuire a contrastare gli attacchi più devastanti.

La segmentazione è anche riconosciuta come una pietra miliare nel sistema di sicurezza Zero Trust e la buona notizia per le società di e-commerce consiste nel fatto che sono stati già compiuti progressi in questo ambito. Tutti gli intervistati stanno implementando o hanno già implementato un sistema di sicurezza Zero Trust (100%), anche se solo poco più di due intervistati su cinque (42%) segnalano che il loro sistema Zero Trust è pienamente completo e definito e può essere considerato ad un livello avanzato. Si tratta, quindi, di un'area in cui la segmentazione può aiutare le società di e-commerce a progredire nel loro percorso verso il modello Zero Trust. Sulla base dei dati, le organizzazioni negli Stati Uniti sono molto più avanti nel processo di implementazione del sistema di sicurezza Zero Trust e sono più propense a dichiarare che la loro implementazione del modello Zero Trust è pienamente realizzata e definita (63%) rispetto alle società di e-commerce dell'America Latina (46%), dell'APAC (32%) o dell'area EMEA (23%).

I motivi che spingono ad avviare un progetto di segmentazione della rete variano in modo significativo da un'area geografica all'altra, con un'attenzione alla cybersicurezza da parte delle organizzazioni governative, salendo al vertice con il 41%. L'America Latina e i pæsi dell'UE hanno entrambi indicato le vulnerabilità zero-day di alto profilo come i principali fattori che spingono ad avviare un progetto di segmentazione (rispettivamente, 44% e 42%). Tuttavia, gli intervistati dell'UE sono molto più propensi a segnalare anche che questi progetti sono stati avviati come parte delle loro best practice (41% rispetto alla media complessiva del 22%). Gli intervistati negli Stati Uniti e nell'area APJ, tuttavia, sono più propensi ad affermare di aver avviato un progetto di questo tipo per un'attenzione alla cybersicurezza da parte delle organizzazioni governative (rispettivamente, 41% e 39% rispetto alla media complessiva del 35%). Gli intervistati dell'area APJ sono, inoltre, più propensi ad affermare di aver avviato un progetto di questo tipo in seguito allo spostamento delle applicazioni di importanza critica nel cloud (39% rispetto alla media complessiva del 32%).

La maggioranza degli intervistati che operano nelle società di e-commerce aspira a spingersi oltre e a implementare la microsegmentazione, che protegge i carichi di lavoro delle applicazioni a livello granulare: il 92% dichiara che la microsegmentazione è almeno una priorità elevata, mentre il 34% la indica come priorità assoluta. Inoltre, tutti i responsabili decisionali del settore IT e della sicurezza (100%) in questo settore riferiscono che la segmentazione è stata adottata almeno da una minoranza del loro settore, sottolineando che si tratta di una soluzione di cui almeno tutti hanno un'ampia consapevolezza, anche se i progressi fino ad oggi sono stati limitati.

Gli intervistati sottolineano, inoltre, la necessità di ottenere una maggiore visibilità sull'ambiente IT delle loro organizzazioni. Gli intervistati in America Latina affermano di aver bisogno di molta più visibilità (63%) sulle comunicazioni di rete, sull'ubicazione delle risorse, ecc., per ridurre i rischi, seguiti dagli intervistati nell'APAC (56%), negli Stati Uniti (46%) e nell'area EMEA (44%).

Le implementazioni sono lente, ma perseverare produce risultati trasformativi

La dura realtà è che, nonostante in larga parte concordino sul fatto che la segmentazione sia la chiave per fermare gli attacchi mediante la protezione delle risorse IT, l'implementazione della segmentazione è stata lenta, forse più di quanto ci si aspettasse.

Solo l'11% delle società di e-commerce ha segmentato più di due delle aree aziendali più importanti, mentre il 48% ha avviato l'ultimo progetto di segmentazione della propria rete almeno due anni fa, il che suggerisce uno stallo.

Aree mission-critical

- Applicazioni di importanza critica
- Applicazioni per interazioni pubbliche
- Controller di dominio
- Endpoint
- Server
- Risorse/dati aziendali importanti

La lentezza delle implementazioni è spiegata più chiaramente dai principali ostacoli incontrati dagli intervistati: mancanza di competenze/esperienza nella segmentazione (40%), requisiti di conformità (40%) e aumento dei colli di bottiglia delle performance (38%), il tutto associato ai tradizionali metodi di segmentazione. Vale la pena notare che, sebbene la mancanza di risorse o esperienza sia la prima causa del ritardo nei progetti di segmentazione, una carenza di talenti si avverte nell'intero settore della cybersicurezza e, con i cambiamenti che avvengono così rapidamente in questo settore, è normale rilevare lacune di competenze.

Le società di e-commerce, in tutte le aree geografiche, devono affrontare alcune sfide: il 100% di quelle negli Stati Uniti e in America Latina afferma di aver riscontrato problemi durante la segmentazione della propria rete. Una percentuale analoga ha affermato lo stesso nell'APAC (99%) e nell'area EMEA (97%).

Tuttavia, se suddivisi per area geografica (Figura 3), gli ostacoli che con maggiore probabilità si incontreranno sono diversi tra loro a dimostrare che alcuni problemi (ad esempio, mancanza di competenze, conformità) possono essere favoriti tanto quanto o più da questioni locali anziché globali.

Sia nell'area EMEA che in America Latina, la mancanza di competenze/esperienza (in entrambi i casi, 54%) rappresenta il principale ostacolo alla segmentazione. Per gli Stati Uniti, la sfida maggiore è rappresentata dall'aumento dei colli di bottiglia delle performance (44%), mentre nell'APAC il problema più probabile è rappresentato dai requisiti di conformità (43%).

	Problema riscontrato con maggiore probabilità	Secondo/terzo problema riscontrato con maggiore probabilità	
Stati Uniti [59]	Aumento dei colli di bottiglia delle performance (44%)	Requisiti di conformità/Disponibilità limitata di strumenti adeguati (in entrambi i casi, 41%)	
America Latina [24*]	Mancanza di competenze/esperienza nella segmentazione (54%)	Elevata complessità (46%)	Alcune o tutte le apparecchiature utilizzate sono proprietarie/Alcune o tutte le apparecchiature utilizzate sono preesistenti (in entrambi i casi, 38%)
EMEA [39]	Mancanza di competenze/esperienza nella segmentazione (54%)	Disponibilità limitata di strumenti adeguati (41%)	Requisiti di conformità/Alcune o tutte le apparecchiature utilizzate sono preesistenti/Costo elevato (in tutti i casi, 36%)
APAC [67]	Requisiti di conformità (43%)	Disponibilità limitata di strumenti adeguati/Alcune o tutte le apparecchiature utilizzate sono proprietarie/Aumento dei colli di bottiglia delle performance (in tutti i casi, 37%)	

Figura 3. Quali eventuali problemi la vostra organizzazione ha incontrato/prevede di incontrare durante la segmentazione della rete? Il grafico mostra coloro che a un certo punto hanno segmentato la rete, con le prime tre risposte selezionate per area geografica (dati relativi solo al settore dell'e-commerce).

* Attenzione: dimensioni di base inferiori a 30

Concetti chiave: coloro che hanno segmentato sei aree aziendali critiche hanno ridotto notevolmente il rischio

La protezione e la segmentazione di un maggior numero di risorse nell'ambiente dell'e-commerce rendono immediatamente più sicure le organizzazioni. Con la soluzione giusta, i team addetti alla sicurezza sono in grado di identificare gli attacchi più rapidamente, migliorando così il tempo medio di rilevamento (MTTD) e il tempo medio di risposta (MTTR) a un incidente. Tuttavia, la sottosegmentazione delle risorse, che, in genere, deriva dall'utilizzo di tecnologie di segmentazione preesistenti, può creare falle nella sicurezza e punti ciechi, lasciando l'organizzazione in una posizione più vulnerabile o reattiva. Al contrario, se eseguita correttamente, la segmentazione tramite un approccio definito dal software può aiutare le organizzazioni a gestire meglio le proprie superfici di attacco per proteggere le risorse critiche in modo più efficiente ed economico.

I nostri risultati mostrano che, dopo una violazione, il recupero avviene 11 ore più velocemente con la segmentazione. Facciamo due calcoli: per le società di e-commerce che hanno implementato la segmentazione in sei aree mission-critical, sono necessarie, in media, tre ore per bloccare completamente un attacco ransomware. Per coloro che hanno implementato la segmentazione su una sola risorsa, sono necessarie 14 ore.

Allo stesso modo, la segmentazione consente di risparmiare 11 ore di contenimento del movimento laterale. Per coloro che hanno implementato la segmentazione in tutte e sei le aree mission-critical, sono necessarie in media tre ore per limitare in modo significativo gli spostamenti laterali di un attacco ransomware. Per coloro che hanno implementato la segmentazione su una sola risorsa, sono necessarie in media 14 ore.

Considerate la differenza per il vostro team, i danni al brand e i costi sostenuti durante queste 11 ore in entrambi i casi.

Per contrastare un attacco

3 ore

Il tempo necessario, in media, per bloccare completamente un attacco ransomware, per coloro che hanno segmentato tutte e sei le risorse aziendali. Per coloro che hanno segmentato una sola risorsa: **14 ore**

Per limitare il movimento

3 ore

Il tempo necessario, in media, per limitare in modo significativo il movimento laterale di un attacco ransomware, per coloro che hanno segmentato tutte e sei le risorse aziendali. Per coloro che hanno segmentato una sola risorsa: **14 ore**

In che modo una soluzione di microsegmentazione basata su software aiuta a risolvere le sfide

La microsegmentazione non solo consente un tipo di segmentazione più avanzato e granulare, ma ne semplifica anche l'implementazione.

Le soluzioni basate su software, come Akamai Guardicore Segmentation, possono essere implementate rapidamente, senza dover apportare modifiche fisiche alla rete. Non è necessario eseguire il re-IP dei nuovi segmenti o preoccuparsi della posizione fisica dei server e dei dispositivi. Ciò rende la soluzione molto più rapida e semplice da implementare rispetto agli approcci basati sull'infrastruttura, come i firewall e le VLAN. Inoltre, poiché la soluzione non si basa sul sistema operativo sottostante per l'applicazione delle policy, funziona in modo eccellente su tutti i computer e i sistemi operativi: dai server bare-metal alle implementazioni multicloud, dalle tecnologie legacy come Windows Server 2003 e Windows XP ai più recenti sistemi POS e dispositivi IoT/OT fino alla tecnologia containerizzata. Ciò significa che dovete gestire un'unica soluzione con un'unica interfaccia per visualizzare e controllare le connessioni effettuate da diversi sistemi operativi e dispositivi nell'intero ambiente, indipendentemente dalla loro posizione fisica.

Come facilita la distribuzione

Akamai Guardicore Segmentation genera, innanzitutto, una visualizzazione interattiva di tutte le connessioni che vengono effettuate nell'ambiente, un elemento fondamentale per superare i principali ostacoli all'implementazione. Inoltre, noi di Akamai abbiamo integrato nella nostra soluzione dei modi attivi per affrontare i colli di bottiglia delle performance e i requisiti di conformità.

I colli di bottiglia delle performance non derivano necessariamente da uno sforzo tecnico del sistema causato da una soluzione di segmentazione, ma da colli di bottiglia della forza lavoro causati dalla necessità di segmentare manualmente le aree aziendali e di risolvere manualmente i problemi che interessano tali aree quando si verificano. Akamai si adopera per ovviare alla situazione (e arginare l'ostacolo numero uno all'implementazione, ossia la mancanza di competenze) riducendo il tempo necessario per eseguire manualmente la segmentazione e offrendo un supporto tecnico e servizi professionali di alto livello. I nostri esperti di segmentazione collaborano con voi durante l'intero processo di implementazione per garantire il raggiungimento degli obiettivi di segmentazione nel vostro ambiente IT esclusivo.

Il supporto all'implementazione deriva anche dalla soluzione stessa: le raccomandazioni di etichettatura e policy basate sull'intelligenza artificiale e i modelli di policy già pronti per i casi d'uso più comuni fanno risparmiare tempo e operazioni, semplificano il flusso di lavoro, riducono il tempo complessivo di implementazione delle policy e prevengono le configurazioni errate dovute a errori umani. Per uno dei nostri clienti, siamo stati in grado di realizzare un progetto di segmentazione granulare che avrebbe richiesto due anni e oltre un milione di dollari di costi totali in sole sei settimane con un solo tecnico, riducendo il costo complessivo del progetto dell'85%, dimostrando che la segmentazione granulare può essere implementata in modo rapido e semplice, senza subire colli di bottiglia.

Come la segmentazione facilita la conformità

Molti dei nostri clienti utilizzano la nostra soluzione per garantire e attestare la conformità a una serie di mandati di conformità nazionali e internazionali, come PCI-DSS, SWIFT, Sarbanes-Oxley, HIPAA, GDPR e molti altri. Questi mandati di conformità, di solito, richiedono che i dati in questione, come i dati dei titolari di carte di credito (CDE) per il PCI DSS, siano separati e protetti dagli altri sistemi dell'ambiente.

Sebbene ciò possa essere proibitivo utilizzando firewall e VLAN, la nostra soluzione basata su software consente di creare segmenti specifici per i dati in questione e di applicare regole di comunicazione su chi può o non può accedere a tali dati. Utilizzando la nostra mappa visiva con visualizzazioni quasi in tempo reale e storiche, potete attestare la vostra conformità a questi mandati dimostrando fisicamente che i dati in questione non sono accessibili a utenti, sistemi e computer non autorizzati.

Perseverare con la soluzione e il supporto giusti per trasformare la strategia di sicurezza

La segmentazione può essere eccessivamente difficile da implementare. Tuttavia, come dimostra questo rapporto, chi riesce a implementarla in modo efficace vede ridursi in modo massiccio il proprio rischio informatico. Una segmentazione adeguata limita il movimento laterale e consente agli addetti alla sicurezza di reagire più rapidamente durante un attacco attivo. E dopo una violazione, le operazioni di ripristino sono più sicure e richiedono meno tempo.

Scegliere una soluzione definita dal software, che è stata progettata per superare le sfide comuni associate ad un'implementazione tradizionale della segmentazione, e collaborare con esperti del settore durante il percorso, vi mette nella migliore posizione possibile per trasformare la vostra strategia di sicurezza. Inoltre, più aree aziendali segmentate, più fate progredire la vostra architettura Zero Trust, riducendo il rischio attuale.

Il nostro gruppo di sondaggio

Per gli scopi di questo rapporto, abbiamo analizzato 190 intervistati che operano nel settore dell'e-commerce (59 negli Stati Uniti, 39 nell'area EMEA, 68 nell'APAC e 24 in America Latina).

Per lo studio di ricerca completo, abbiamo intervistato 1.200 responsabili decisionali del settore IT e della sicurezza in 10 pæsi allo scopo di misurare i progressi compiuti dalle organizzazioni in termini di protezione dei loro ambienti, focalizzandoci sul ruolo della segmentazione.

Agli intervistati sono state poste domande sui loro sistemi di sicurezza IT e sulle strategie di segmentazione adottate, nonché sulle minacce che le loro organizzazioni si sono trovate ad affrontare nel 2023. Dai dati e dai risultati emersi, possiamo comprendere come le strategie di sicurezza siano cambiate a partire dal 2021 e individuare le aree che ancora necessitano di miglioramenti.

Hanno partecipato al sondaggio intervistati che lavorano in tutto il mondo, inclusi Stati Uniti, India, Messico, Brasile, Regno Unito, Francia, Germania, Cina, Giappone e Australia, all'interno di aziende che impiegano oltre 1.000 dipendenti e operano in vari settori e industrie.

Nota: questo campione è leggermente diverso da quello del 2021. Dimensioni del campione: 2023: 1.200 risposte; 2021: 1.000 risposte. Nel 2023 sono stati intervistati anche responsabili provenienti da Australia, Giappone e Cina. I settori sono leggermente diversi rispetto al 2021. Nel 2023, ci siamo concentrati specificamente sul commercio digitale come settore a sé stante.

Scoprite ulteriori informazioni su Akamai Guardicore Segmentation

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 Akamai Technologies su X (in precedenza Twitter) e LinkedIn. Data di pubblicazione: 05/24.

Vanson Bourne è un'azienda indipendente specializzata in ricerche di mercato per il settore tecnologico. La sua reputazione di azienda in grado di offrire analisi solide e credibili si basa su principi di ricerca rigorosi e sulla capacità di raccogliere le opinioni di responsabili decisionali senior in tutti i ruoli tecnici e commerciali, in tutti i settori e in tutti i principali mercati. Per altre informazioni, visitate www.vansonbourne.com.