EBOOK

Superare i problemi di implementazione per proteggere i sistemi dei settori energia e petrolio/gas

Rapporto sullo stato della segmentazione globale

Sommario

Introduzione

I reparti della sicurezza IT e OT affrontano da sempre sfide significative, ma nei settori dell'energia, del petrolio/gas e dei servizi pubblici in generale, la pressione diventa ancora maggiore a causa delle criticità legate all'offerta di servizi pubblici alle popolazioni. Spesso, i conflitti locali, le pressioni politiche e le controversie ideologiche aggravano le difficoltà e aumentano i pericoli affrontati da questo settore. Tuttavia, poiché i criminali diventano più sofisticati e combinano varie tecniche per sferrare minacce più vaste e più frequenti, i team addetti alla sicurezza delle società energetiche si trovano ora ad affrontare una pressione senza precedenti. Senza sistemi connessi online o alle proprie reti OT private, per una società energetica è impossibile operare e una singola violazione riuscita può comportare danni significativi alla sua reputazione e alle sue performance finanziarie.

I risultati di questo rapporto indicano che le ripercussioni di questi attacchi si stanno intensificando, aumentando così l'onere per i responsabili della sicurezza di scegliere soluzioni tali da garantire la sicurezza dell'intero ambiente senza sacrificare le performance.

Per contro, le agenzie di regolamentazione e i governi di tutto il mondo attualmente stanno formulando linee guida e regolamenti sulla sicurezza in risposta al sostanziale aumento delle minacce alla cybersicurezza in questo settore e alla natura critica dei servizi forniti. Le società energetiche sono obbligate ad aderire agli standard normativi e a garantire la manutenzione e la sicurezza dei loro servizi.

Gli intervistati che operano in società energetiche (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 protette, ma i loro progressi complessivi nell'implementazione in applicazioni e risorse aziendali di importanza critica sono inferiori alle aspettative.

L'ostacolo numero uno per le società energetiche è stato rappresentato dall'aumento dei colli di bottiglia delle performance, il che suggerisce che i team potrebbero esitare a imbarcarsi in un progetto che potrebbe interrompere le performance senza un'adeguata garanzia che questa situazione non si verificherà. È fondamentale tenere presente che, data la natura vitale dei servizi forniti al pubblico da queste società, eventuali interruzioni nella funzionalità delle soluzioni possono causare danni ai clienti o mettere a repentaglio la sicurezza del personale addetto alla manutenzione.

Al contrario, si prevede che il settore dell'energia enfatizzerà di più la segmentazione rispetto alla maggior parte degli altri settori, il che indica che il suo valore è indubbiamente riconosciuto.

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 le performance e la sicurezza.

La microsegmentazione è una tecnica di sicurezza che vi consente di dividere in modo logico una rete in segmenti separati fino al livello dei singoli carichi di lavoro. È possibile quindi definire i controlli di sicurezza e la delivery di servizi per ogni singolo segmento. Questo approccio granulare alla sicurezza offre un controllo più preciso sull'accesso e sulla protezione dei dati sensibili. Implementando la microsegmentazione, le organizzazioni possono limitare l'impatto di una violazione della sicurezza e proteggere meglio la propria rete da avanzate minacce informatiche. Nel complesso, la combinazione di segmentazione e microsegmentazione fornisce una strategia di sicurezza completa, essenziale per salvaguardare le risorse critiche nel panorama delle minacce complesso e dinamico di oggi.

Gli attacchi ransomware continuano ad aumentare, così come il loro impatto

Il numero di attacchi ransomware (riusciti o meno) sferrati contro le società energetiche è aumentato notevolmente negli ultimi due anni, passando da una media di 37 nel 2021 a 62 nel 2023, e non c'è motivo di sospettare che questa crescita non continuerà nel breve termine. L'impatto di questi attacchi può avere effetti dannosi sulla popolazione e sulle economie, tra cui problemi di blackout o danni alle infrastrutture che portano alla perdita di credibilità dell'azienda, al furto di informazioni aziendali e dati personali o addirittura al rischio per la vita delle persone. Mentre gli attacchi ransomware diventano sempre più devastanti e frequenti, è fondamentale per le società energetiche proteggere i propri sistemi e i propri dati. In caso contrario, non solo si mette a rischio l'organizzazione, ma si mette a repentaglio anche la sicurezza delle persone e delle comunità che fanno affidamento su questi servizi. Poiché gli attacchi ransomware diventano sempre più sofisticati, è fondamentale per le organizzazioni rimanere vigili e proattive nelle loro strategie di difesa per mitigare i potenziali danni e i disagi causati da queste minacce.

Numero medio di attacchi ransomware negli ultimi 12 mesi per settore

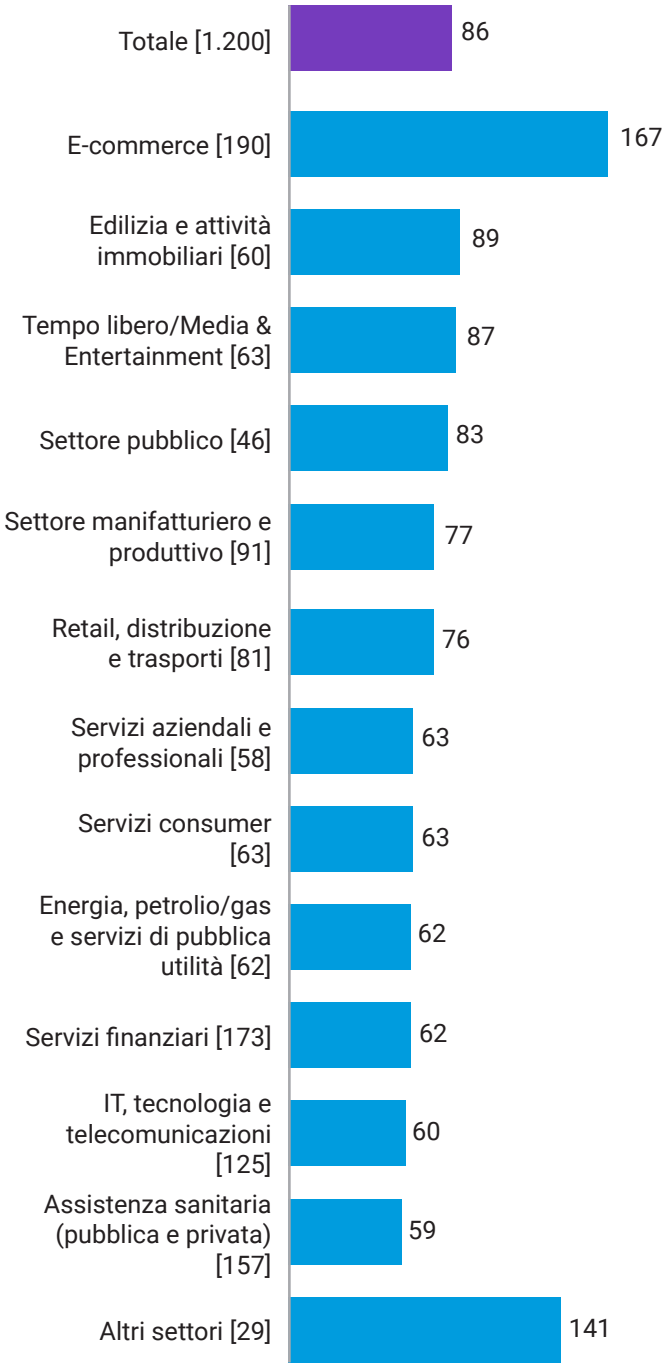

Figura 1. Quanti attacchi ransomware hanno colpito la vostra organizzazione negli ultimi 12 mesi (indipendentemente dal fatto che siano andati o meno a buon fine)? Il grafico mostra il numero medio di attacchi negli ultimi 12 mesi, numeri di base suddivisi per settore.

Uno dei motivi di questo numero relativamente basso di attacchi è che la risorsa principale di una società energetica tende ad essere fisica (petrolio, gas, ecc.) piuttosto che digitale (denaro o dati dei clienti). Inoltre, le società energetiche non sono note per essere obiettivi facili da colpire, come altre organizzazioni disciplinate da poche normative, ad esempio il settore dei media o il retail. Pertanto, è più probabile che gli attacchi siano guidati da obiettivi politici anziché finanziari. Questo dato è potenzialmente supportato dal fatto che, mentre solo il 5% degli intervistati in tutti i settori ha affermato complessivamente che la propria organizzazione non ha mai rilevato un attacco informatico, questa percentuale sale al 24% degli intervistati nel settore dell'energia.

Gli attacchi ransomware contro il settore dell'energia sono stati più frequenti nel 2023 rispetto al 2021, ma dalla gravità del loro impatto emergono dati più eterogenei (figura 2): i nostri intervistati indicano un notevole aumento della perdita di dati, ma una diminuzione di tutte le altre problematiche. Questa tendenza generale potrebbe essere guidata dalla crescente consapevolezza del valore dei dati (che sono quindi un obiettivo prioritario per gli hacker), ma potrebbe anche essere dovuta ad un miglior approccio adottato nel settore dell'energia. Il numero di società energetiche che aggiornano le strategie o le policy di cybersicurezza almeno una volta alla settimana è passato dal 2% nel 2021 al 23% nel 2023. Poiché gli eventi globali (principalmente legati ai conflitti o ai cambiamenti climatici) spingono i paesi a considerare più attentamente la propria sicurezza energetica, non sorprende vedere che le società energetiche si siano focalizzate maggiormente sulle loro strategie di cybersicurezza.

Impatto dei ransomware/attacchi informatici sul settore dell'energia

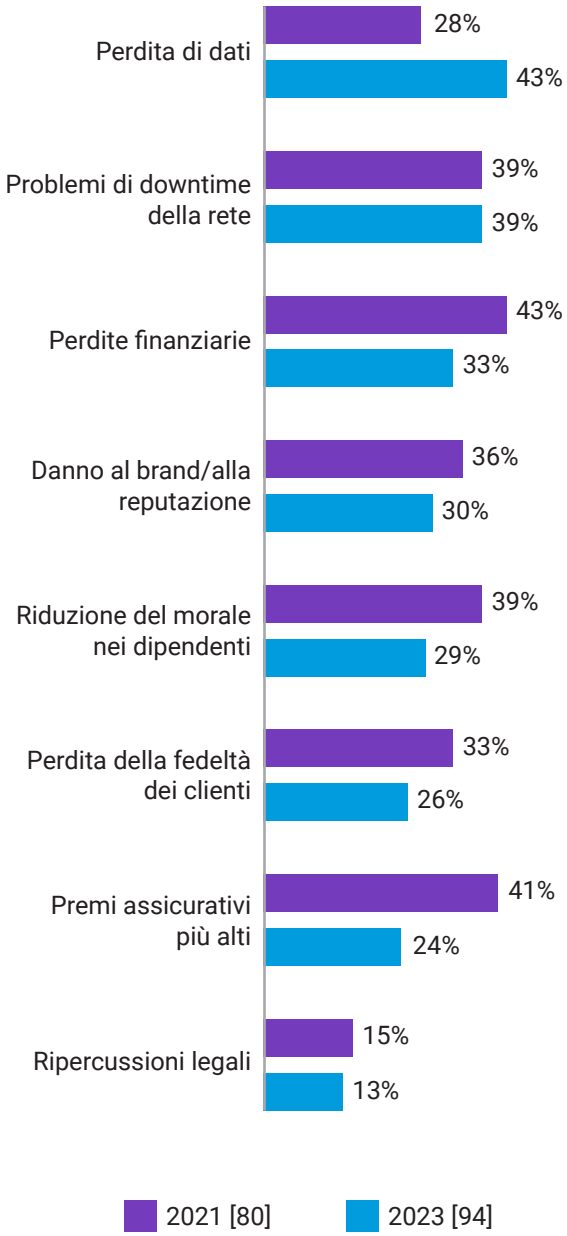

Figura 2. Quando è stato rilevato in precedenza un ransomware o un altro attacco informatico, quali dei seguenti impatti ha avuto sulla vostra organizzazione? Il grafico mostra le dimensioni di base per anno, senza mostrare tutte le opzioni di risposta, suddivise per dati storici (dati relativi solo al settore dell'energia).

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

I nostri intervistati che operano nel settore dell'energia concordano sull'importanza della segmentazione nel garantire la sicurezza delle loro organizzazioni e, in particolare, nell'affrontare i malware. Il 66% degli intervistati (una delle percentuali più alte di tutti i settori) afferma che la segmentazione sia estremamente importante e il 95% di essi ritiene che sia fondamentale per contrastare gli attacchi più devastanti.

La segmentazione contribuisce anche notevolmente all'adozione di un sistema Zero Trust e la buona notizia per le società energetiche consiste nel fatto che sono stati già compiuti progressi in questo ambito. Tutti gli intervistati (100%) stanno implementando o hanno già implementato un sistema di sicurezza Zero Trust, anche se meno della metà di essi (46%) riferisce che il proprio sistema Zero Trust sia finalizzato e definito e, pertanto, possa essere considerato ad un livello avanzato. Si tratta, quindi, di un'area in cui la segmentazione può aiutare le società energetiche nel loro percorso verso il modello Zero Trust. Questo è il risultato dell'indagine per gli ambienti IT delle organizzazioni, sebbene l'ambiente OT possa essere diverso per le tecnologie utilizzate.

La maggioranza degli intervistati che operano nelle società energetiche aspira a spingersi oltre e a implementare la microsegmentazione, che protegge i carichi di lavoro delle applicazioni a livello granulare: l'88% dichiara che la microsegmentazione è almeno una priorità elevata, mentre il 47% la indica come priorità assoluta. In tutti i settori esaminati, solo il 34% degli intervistati segnala la microsegmentazione come priorità assoluta a indicare che le società energetiche sono più propense, in media, a spingere affinché venga implementata il prima possibile. Inoltre, quasi tutti (98%) i responsabili decisionali IT e della sicurezza in questo settore riferiscono che la microsegmentazione sia stata adottata almeno da una minoranza del loro settore, sottolineando che si tratta di una soluzione di cui quasi tutti hanno un'ampia consapevolezza.

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, l'implementazione della segmentazione è stata più lenta di quanto ci si aspettasse. Solo il 38% delle società energetiche ha segmentato più di due delle aree aziendali più importanti nel 2023 (rispetto al 30% nel 2021), mentre il 33% ha avviato l'ultimo progetto di segmentazione della propria rete almeno due anni fa, il che suggerisce uno stallo.

La lentezza delle implementazioni è spiegata più chiaramente dai principali ostacoli incontrati dagli intervistati: aumento dei colli di bottiglia delle performance (49%), requisiti di conformità (43%) e apparecchiature proprietarie (41%, Figura 3).

Ostacoli incontrati durante la segmentazione della rete nel settore dell'energia

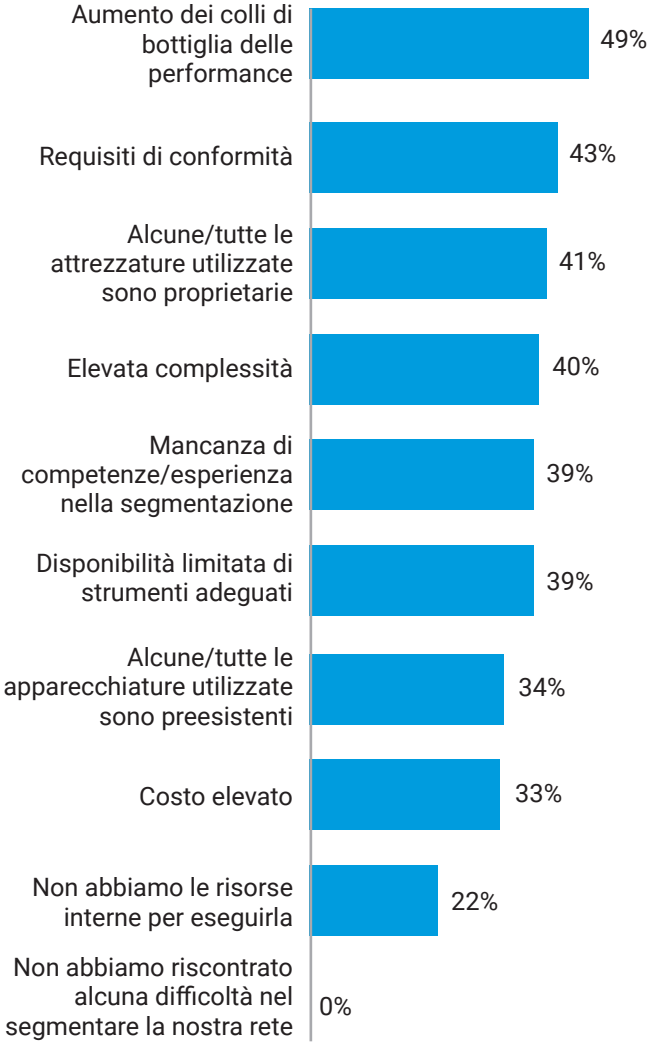

Figura 3. Quali eventuali problemi la vostra organizzazione ha incontrato/prevede di incontrare durante la segmentazione della rete? Il grafico mostra una dimensione di base di 94, riportando solo coloro che a un certo punto hanno segmentato la rete, senza mostrare tutte le opzioni di risposta (dati relativi solo al settore dell'energia).

Un dato incoraggiante per il settore dell'energia, tuttavia, è che il 42% degli intervistati riferisce che il proprio progetto di segmentazione della rete sia iniziato a seguito di un suggerimento da parte della direzione/del consiglio di amministrazione. Questa percentuale è la più alta di tutti i settori (la media complessiva è del 28%) e dimostra che la segmentazione sia chiaramente riconosciuta come importante in questo settore.

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 utilizza un driver proprietario 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 ai più recenti dispositivi IoT/OT e alla tecnologia containerizzata. Ciò implica la gestione di un'unica soluzione con una singola interfaccia per visualizzare e gestire le connessioni effettuate da diversi sistemi operativi e dispositivi nell'intero ambiente, indipendentemente dalla loro posizione fisica.

È importante notare come sia possibile utilizzare la soluzione Akamai Guardicore Segmentation anche in ambienti OT, consentendo l'applicazione della microsegmentazione a reti di controllo private, sistemi operativi tradizionali e dispositivi IoT senza agenti.

Come facilita la distribuzione

La microsegmentazione 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 determinati dalla necessità di segmentare manualmente le aree aziendali e di risolvere manualmente i problemi di tali aree in caso di interruzioni. Akamai si adopera per risolvere questo problema (e l'ostacolo numero uno all'implementazione, ossia la mancanza di competenze) riducendo la necessità di eseguire la segmentazione manualmente 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 specifico ambiente OT o IT.

Il supporto all'implementazione deriva anche dalla soluzione stessa: le raccomandazioni di policy basate sull'intelligenza artificiale e i modelli di policy già pronti per i casi d'uso più comuni fanno risparmiare tempo e clic, 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%, a indicare che sia possibile implementare la segmentazione granulare in modo rapido e semplice, senza causare colli di bottiglia.

Come la microsegmentazione 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, LGPD e molti altri. Questi mandati di conformità di solito richiedono che i dati in questione siano separati 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 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 delle minacce e consente di reagire più rapidamente durante una violazione attiva. Nel caso di una violazione, le operazioni di recupero sono più sicure e richiedono meno tempo per il loro completamento, poiché l'impatto dovrebbe essere limitato al solo segmento interessato.

Scegliere una soluzione progettata per superare le sfide comuni all'implementazione 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 e garantendo una difesa di prima linea contro i vettori di minaccia futuri.

Punti chiave

La segmentazione e la microsegmentazione sono considerate più importanti nel settore dell'energia che in molti altri settori: i responsabili decisionali del reparto IT/OT e della sicurezza IT nelle società energetiche (66%) sono più propensi ad affermare che la segmentazione della rete sia estremamente importante per garantire la sicurezza delle loro organizzazioni rispetto a quelli nel settore dei servizi consumer (36%), ma meno propensi rispetto a quelli nei settori IT e tecnologia (73%).

Gli intervistati nel settore dell'energia sono molto più propensi ad affermare che la microsegmentazione sia la priorità assoluta (47%) rispetto alle controparti nel settore dei servizi consumer (12%) e solo leggermente meno propensi rispetto a quelli nel settore pubblico (48%).

Gli intervistati nel settore dell'energia sono tra i meno propensi ad affermare di non aver effettuato alcuna segmentazione: gli intervistati del settore dell'energia sono meno propensi ad affermare di non aver segmentato alcuna risorsa business-critical (4%), anche se sono comunque più propensi di quelli dei settori dell'edilizia, dei servizi consumer e dei media (tutti 0%), ma meno propensi di quelli nel settore pubblico (15%).

Gli intervistati nel settore dell'energia sono tra i più propensi ad affermare di aver compiuto i migliori progressi nella segmentazione: le società energetiche sono solo leggermente meno propense ad affermare di aver segmentato più di due risorse business-critical (38%) rispetto a quelle del settore del retail (43%) e molto più propense rispetto a quelle nel settore dei servizi consumer (3%).

Il nostro gruppo di sondaggio

Per lo studio di ricerca completo, abbiamo intervistato 1.200 responsabili decisionali del settore IT e della sicurezza in 10 paesi 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.

Per gli scopi di questo rapporto, abbiamo analizzato 94 intervistati (2023) e 80 intervistati (2021) che lavorano nel settore dell'energia.

Scoprite ulteriori informazioni su Akamai Guardicore Segmentation

A sostegno e protezione della vita online c'è sempre Akamai. Le principali aziende al mondo scelgono Akamai per creare, offrire e proteggere le loro experience digitali, aiutando miliardi di persone a vivere, lavorare e giocare ogni giorno. 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 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 il sito www.vansonbourne.com.