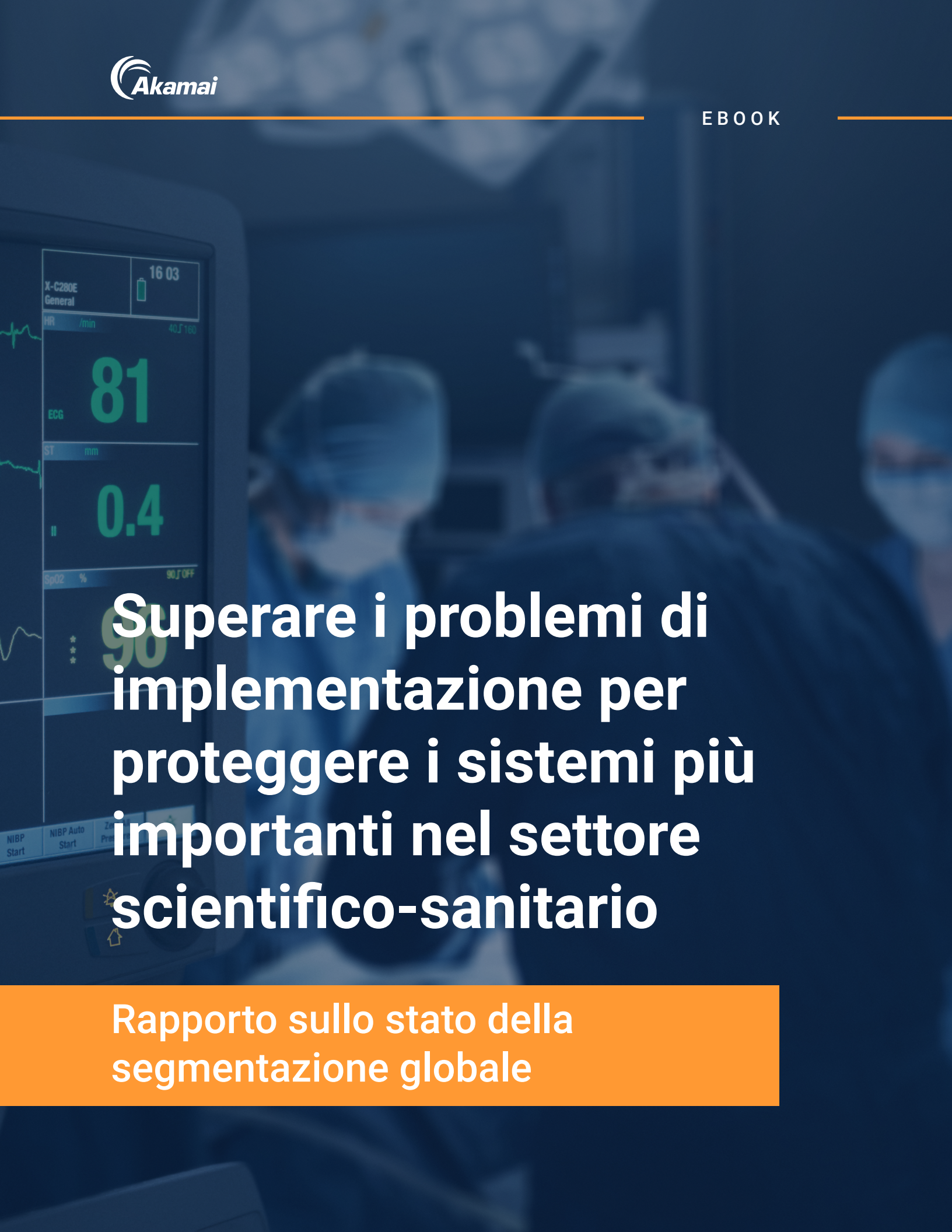
Akamai

EBOOK



Superare i problemi di implementazione per proteggere i sistemi più importanti nel settore scientifico-sanitario

Rapporto sullo stato della segmentazione globale

Sommario

Introduzione

Ora più che mai, il sistema IT nel settore sanitario riguarda uffici, sale riunioni e studi medici. Le violazioni di dati di alto profilo aumentano in termini di gravità e frequenza con un enorme impatto sulle attività e sulla reputazione delle aziende sanitarie. Poiché i criminali utilizzano tattiche sempre più sofisticate e, in molti casi, uniscono le loro forze, i pericoli che affliggono l'ecosistema sanitario sono più frequenti e più gravi. Considerando l'ampio utilizzo di strumenti tecnologici preesistenti, il valore finanziario dei dati dei pazienti e le sfide legate alla rapida digitalizzazione e all'espansione dell'IoMT (Internet of Medical Things), questo ambiente dinamico deve proteggere le proprie infrastrutture, organizzazioni, app e API come nessuno avrebbe immaginato neanche cinque anni fa.

Come dimostrano i risultati di questo rapporto, gli attacchi informatici stanno aumentando la pressione sui responsabili della sicurezza affinché scelgano le soluzioni più appropriate in un settore in cui la continuità del tempo di attività è una questione di vita o di morte.

Gli intervistati delle organizzazioni del settore scientifico-sanitario negli Stati Uniti, in America Latina, Europa, Medio Oriente, Africa e nell'area Asia-Pacifico concordano in modo schiacciante sull'efficacia della segmentazione per mantenere le risorse protette, riferendo, tuttavia, anche che i loro progressi nell'implementazione della segmentazione nelle applicazioni e nelle risorse aziendali critiche sono inferiori alle aspettative. Gli intervistati (inclusi provider di servizi sanitari e specialisti di tecnologie sanitarie, tra le altre organizzazioni specializzate in servizi o prodotti sanitari) affermano che l'ostacolo principale per le aziende del settore scientifico-sanitario è stato rappresentato dalla mancanza delle competenze necessarie per implementare la segmentazione. La complessità storica dell'implementazione dei metodi di segmentazione tradizionali, che non coprono i dispositivi medici, è aggravata dal fatto che i team sono ancora alle prese con il personale richiesto prima della pandemia di COVID-19.

Da un sondaggio condotto dall'HIMSS (Healthcare Information and Management Systems Society), un'organizzazione statunitense senza scopo di lucro, è emerso che l'84% degli esperti IT sanitari degli Stati Uniti fatica ad attrarre personale e il 67% di essi riferisce che trattenerlo è un problema. Inoltre, come ha rilevato l'HIMSS, la maggior parte del personale non dispone di una formazione aggiornata sulle minacce prevalenti ed emergenti.

E questa formazione aggiornata cosa dovrebbe includere? La segmentazione ha dimostrato di avere un effetto trasformativo sulla difesa per coloro che hanno segmentato la maggior parte delle risorse critiche, consentendo loro di mitigare e contenere i ransomware 11 ore più velocemente rispetto a coloro che avevano segmentato solo una risorsa. Immaginate la differenza che fanno quelle 11 ore per il vostro team, i vostri pazienti e la vostra reputazione.

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.

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

I dati del 2021 rispetto al 2023 mostrano che il numero di attacchi ransomware (riusciti o meno) sferrati contro le aziende sanitarie in un arco di 12 mesi è aumentato del 162%. Gli effetti di questi attacchi possono variare da problemi di downtime operativi, come interventi chirurgici cancellati o riprogrammati, a problemi con le interazioni farmacologiche dovuti alla mancanza di accesso alle cartelle cliniche e alle deviazioni delle ambulanze verso altre strutture sanitarie.

Percentuale di aumento del numero di attacchi ransomware negli ultimi 12 mesi per settore (dati del 2021 rispetto ai dati del 2023)

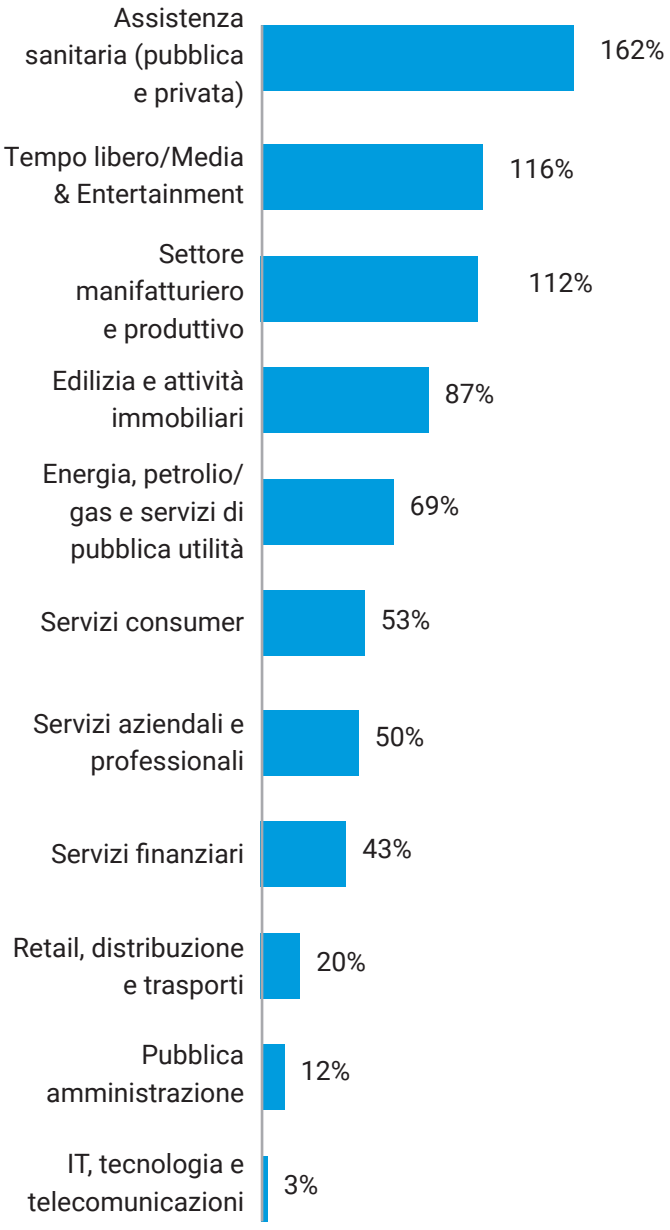


Figura 1. Quanti attacchi ransomware hanno colpito la vostra organizzazione negli ultimi 12 mesi (indipendentemente dal fatto che siano andati o meno a buon fine)? Il grafico riflette le dimensioni di base dei 1.200 intervistati, mostrando solo la percentuale media di aumento del numero di attacchi, suddivisi per settore, negli ultimi 12 mesi.

In media, la velocità di aumento nel settore sanitario è la più alta rispetto a tutti i settori a indicare che le aziende sanitarie, compresi gli ospedali pediatrici, che subiscono anch'essi un numero sempre maggiore di attacchi, potrebbero essere considerate con minore probabilità dagli hacker come "off limits".

Gli attacchi ransomware contro le aziende sanitarie non solo sono più frequenti nel 2023 rispetto al 2021, ma hanno anche un impatto più devastante (Figura 2): gli intervistati indicano un incremento dei danni alla reputazione, della perdita della fedeltà dei clienti (pazienti) e dei problemi di downtime della rete, tutti fattori che alzano notevolmente la posta in gioco per i team addetti alla sicurezza.

Questa pressione ha influenzato anche l'adozione di una strategia agile. Il numero di aziende sanitarie che aggiornano le strategie o le policy di cybersicurezza almeno una volta alla settimana è passato dal 17% nel 2021 al 25% nel 2023, in risposta non solo ai ransomware, ma anche ad una superficie di attacco in costante evoluzione.

Esaminando ulteriormente questo aspetto, le aziende sanitarie sono le più soggette a subire perdite finanziarie a seguito di un attacco alla cybersicurezza rispetto a quelle di altri settori (43% rispetto alla media complessiva del 36%). Le aziende sanitarie sono anche più soggette a subire la perdita della fedeltà dei membri/pazienti in seguito ad un attacco alla cybersicurezza (48% rispetto alla media complessiva del 33%), il che dimostra che, sotto molti aspetti, le aziende sanitarie corrono rischi maggiori rispetto ad altri tipi di organizzazioni.

Impatto dei ransomware/ attacchi informatici sul settore scientifico-sanitario

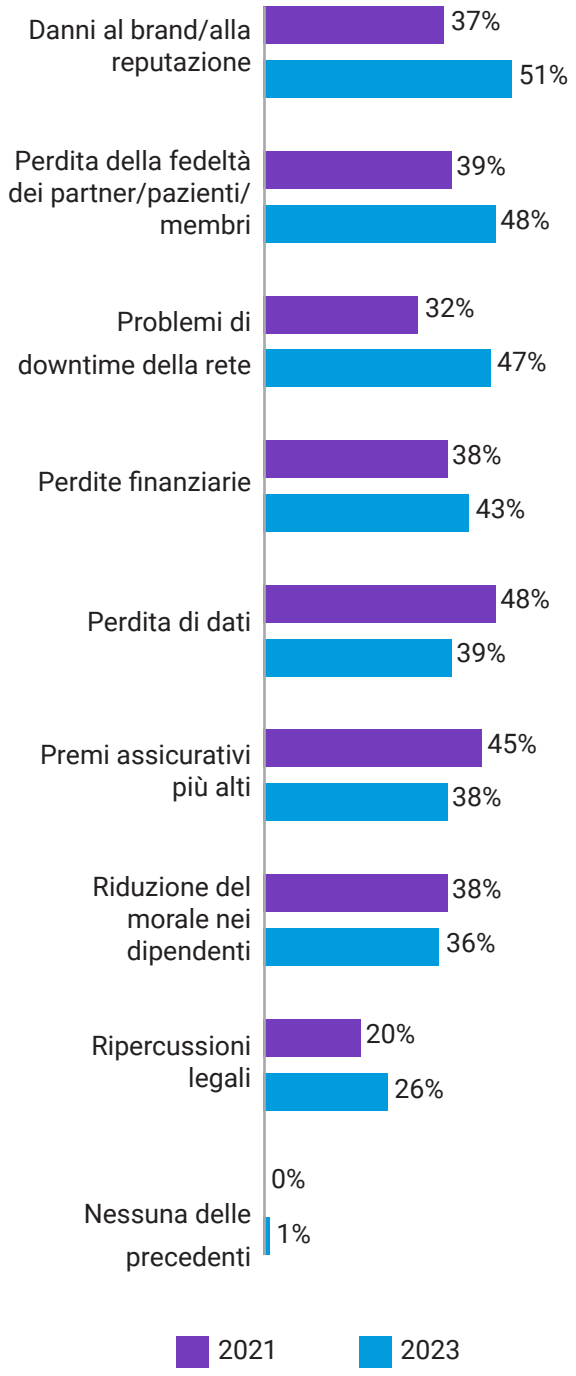


Figura 2. Quando è stato rilevato in precedenza un ransomware o un altro attacco informatico, quali dei seguenti impatti ha avuto sulla vostra organizzazione? Il grafico mostra le dimensioni di base per anno, senza mostrare tutte le opzioni di risposta, suddivise per dati storici (2021=112, 2023=157) (dati relativi solo al settore sanitario).

La segmentazione riconosciuta come la pietra miliare del modello Zero Trust

Gli intervistati che operano nel settore scientifico-sanitario concordano sull'importanza della segmentazione nel garantire la sicurezza delle loro organizzazioni e, in particolare, nell'affrontare i malware.

Il modello Zero Trust è una strategia di protezione della rete basata sul concetto secondo cui l'accesso ai carichi di lavoro o sistemi IT di un'azienda da parte di persone o dispositivi, interni o esterni alla rete aziendale, deve essere consentito solo se ritenuto espressamente necessario. In sintesi, non si basa su una fiducia implicita.

Il 64% degli intervistati afferma che la segmentazione sia estremamente importante e il 94% di essi ritiene che sia fondamentale per contrastare gli attacchi più devastanti.

L'adozione del modello Zero Trust è spesso favorita da circostanze che esulano dal controllo dei responsabili IT sanitari. Quando si è citato il motivo per cui un'organizzazione ha avviato un progetto di segmentazione, un terzo degli intervistati del settore sanitario (33%) ha affermato che ciò è dovuto ad un'attenzione del loro governo alla cybersicurezza e un numero quasi uguale di intervistati (29%) afferma che ciò è dovuto al fatto di essere già stati vittime di un attacco ransomware.

Tuttavia, solo circa un intervistato del settore sanitario su tre (34%) riferisce che il proprio sistema Zero Trust sia finalizzato e definito e, pertanto, possa essere considerato ad un livello avanzato. Questa percentuale è tra le più basse di tutti i settori, con alcuni settori (come l'edilizia e i servizi finanziari) che sono notoriamente più propensi ad aver implementato un sistema Zero Trust avanzato (rispettivamente, 53% e 47%). Le aziende sanitarie negli Stati Uniti (di cui il 50% afferma di avere un sistema fina e definito) mostreranno con maggiore probabilità un livello avanzato del sistema Zero Trust rispetto alle altre aree geografiche (solo il 23% di altri paesi e aree geografiche afferma di avere un sistema Zero Trust finalizzato e definito).
Ciò riflette la tendenza generale, secondo cui le aziende statunitensi di tutti i settori riferiscono di aver subito attacchi informatici rispetto ad altre aree geografiche (115 attacchi negli ultimi 12 mesi rispetto alla media complessiva di 86 attacchi).

Le aziende sanitarie si trovano quindi ad affrontare delle sfide quando si tratta del modello Zero Trust. Gli intervistati del settore sanitario sono più propensi ad affermare di aver riscontrato problemi relativi alle tecnologie proprietarie durante la segmentazione della rete (41% rispetto alla media complessiva del 32%) e di aver affrontato sfide di budget durante l'implementazione del sistema Zero Trust (47% rispetto ad una media del 37% in tutti i settori). Il supporto fornito da un partner esperto può aiutare a superare alcune sfide: tra gli aspetti più difficili da implementare per le aziende sanitarie in un sistema Zero Trust, figura il carico di lavoro delle applicazioni (68% rispetto alla media complessiva del 60%); un partner può colmare le lacune di competenze segnalate dal 45% delle aziende sanitarie.

La maggioranza degli intervistati che operano nelle aziende sanitarie aspira a spingersi oltre e a implementare la microsegmentazione, che protegge i carichi di lavoro delle applicazioni a livello granulare:

Il 92% degli intervistati del settore sanitario dichiara che la microsegmentazione sia almeno una priorità elevata, mentre il 43% la indica come priorità assoluta. In tutti i settori esaminati, solo il 34% segnala la microsegmentazione come priorità assoluta a indicare che le organizzazioni del settore sanitario sono più propense, in media, a valorizzare e sostenere i sistemi Zero Trust

Le implementazioni sono lente, ma perseverare produce risultati trasformativi

Benché la segmentazione sia ampiamente considerata come fondamentale per prevenire gli attacchi informatici, la sua implementazione è lenta.

Solo il 36% delle organizzazioni del settore sanitario ha segmentato più di due delle aree aziendali critiche nel 2023, mentre il 43% 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 può essere attribuita a molti dei principali ostacoli incontrati dagli intervistati nel settore sanitario: mancanza di competenze/esperienza nella segmentazione (45%), aumento dei colli di bottiglia delle performance (come quelli causati dalla necessità di risolvere manualmente i problemi, 44%) e l'utilizzo di tecnologie proprietarie (41%, Figura 3). Nello specifico, la mancanza di competenze/esperienza è un problema per le aziende sanitarie più che per le organizzazioni di qualsiasi altro settore (tutte inferiori al 45% del settore sanitario, con una media trasversale dei segmenti verticali pari al 39%). Questi risultati sono allineati con quanto rilevato recentemente dal Ponemon Institute, una delle principali organizzazioni di ricerca sulla sicurezza IT, relativamente alle minacce prevalenti per il settore sanitario, che includono principalmente attacchi ransomware e schemi BEC (Business Email Compromise). Se da un lato la retribuzione competitiva per i professionisti IT del settore sanitario rappresenta una sfida, dall'altro il crescente volume di complesse esigenze normative costituisce un'altra sfida.

Le aziende sanitarie di tutto il mondo continuano a risentire delle conseguenze della pandemia di COVID-19 e della pressione che ha posto sul capitale umano e fiduciario, il che aggrava tali sfide.

Ostacoli incontrati durante la segmentazione della rete nel settore scientifico-sanitario

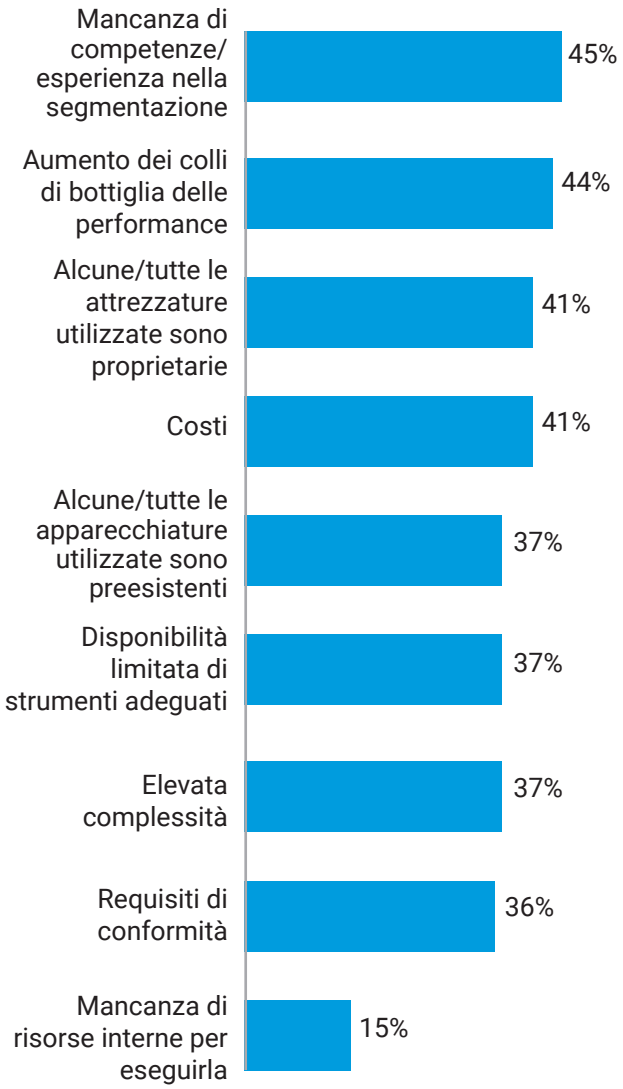


Figura 3. Quali eventuali problemi la vostra organizzazione ha incontrato/prevede di incontrare durante la segmentazione della rete? Il grafico mostra le dimensioni di base del 2023 pari a 157, senza mostrare tutte le opzioni di risposta.
Questa domanda è stata mostrata solo agli intervistati delle organizzazioni che a un certo punto hanno segmentato la rete (dati relativi solo al settore sanitario).

Nonostante i lenti progressi, i tassi di segmentazione stanno gradualmente aumentando in tutti i settori. All'interno del settore sanitario, la percentuale di organizzazioni con applicazioni/dati business-critical segmentati è aumentata del 20% e quella dei server segmentati del 18% dal 2021 al 2023. Tuttavia, mentre questi aumenti superano gli incrementi medi complessivi che sono stati osservati in tutti i settori (rispettivamente, 12% e 8%), le principali vulnerabilità implicano che i tassi di segmentazione devono accelerare. Gli intervistati del settore sanitario sono i più propensi ad affermare di aver avuto un dipendente/utente in ufficio come motivo/fonte che ha consentito al criminale di accedere alla rete (47% rispetto alla media complessiva del 26%), un dato che rappresenta più del doppio di altri settori critici dal punto di vista della conformità come i servizi finanziari e il settore dell'energia (entrambi 19%). L'impatto di tali attacchi può essere ridotto al minimo con la segmentazione e, considerando la delicatezza di molti sistemi all'interno delle aziende sanitarie (in cui è in gioco la vita di molte persone), il valore apportato da una tempestiva segmentazione risulta evidente.

Le lezioni apprese dalla segmentazione di sei aree aziendali critiche

Migliorare la visibilità riduce il rischio, il che è fondamentale in un settore avverso al rischio. Proteggere e segmentare più risorse rende le aziende sanitarie più sicure, consentendo ai team addetti alla sicurezza di identificare più rapidamente le minacce e rispondere in modo molto più efficace.

I risultati di Vanson Bourne mostrano che, dopo una violazione, il recupero avviene 11 ore più velocemente con la segmentazione. Facciamo due calcoli: per le aziende sanitarie che hanno implementato la segmentazione in tutte e sei le 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 offre un tipo di segmentazione non solo più avanzato e granulare, ma anche più semplice.

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 ai più recenti dispositivi IoMT (Internet of Medical Things) 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 un cliente, Akamai ha realizzato 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 microsegmentazione facilita la conformità

Molte organizzazioni del settore scientifico-sanitario hanno implementato la soluzione Akamai Guardicore Segmentation per garantire la conformità a una serie di mandati di conformità nazionali e internazionali, come HIPAA, GDPR, PCI DSS e molti altri. Questi mandati normativi, 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. E dopo una violazione, le operazioni di ripristino sono più sicure e richiedono meno tempo.

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

I criminali informatici prendono di mira le organizzazioni del settore sanitario a un ritmo crescente: gli attacchi ransomware sferrati contro le aziende sanitarie sono cresciuti del 162% dal 2021 al 2023. In confronto, il settore energetico è cresciuto del 69% nello stesso periodo di tempo, mentre i servizi finanziari sono cresciuti del 43%.

Gli intervistati del settore sanitario sono propensi ad affermare che la loro organizzazione ha subito perdite finanziarie a seguito di un attacco alla cybersicurezza, come riferito dal 43% di essi rispetto al 36% degli intervistati di tutti i settori.

La segmentazione e la microsegmentazione sono considerate più importanti nel settore sanitario che in molti altri settori: i responsabili decisionali della sicurezza IT nelle aziende sanitarie (64%) sono più propensi ad affermare che la segmentazione della rete sia estremamente importante per garantire la sicurezza delle loro organizzazioni rispetto a quelli in molti altri settori, come l'edilizia (58%), il settore manifatturiero (53%) e l'e-commerce (48%).
Le opinioni dei responsabili decisionali della sicurezza IT nel settore sanitario sono in linea con i dati degli intervistati nei settori dei servizi finanziari e dell'energia (entrambi 66%).

Le aziende sanitarie sono meno avanti nel processo di implementazione del sistema di sicurezza Zero Trust: gli intervistati nel settore sanitario sono meno propensi ad affermare che l'implementazione del loro sistema Zero Trust sia pienamente completa e definita (34%) rispetto a quelli del settore dei servizi finanziari (47%), dell'energia (46%) e dell'e-commerce (42%).

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 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 sottosegmenti verticali.

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.

Per gli scopi di questo rapporto sul settore scientifico-sanitario, abbiamo analizzato 157 intervistati (2023) e 112 intervistati (2021) che lavorano in questo settore negli stessi paesi degli intervistati per il rapporto principale (Stati Uniti, India, Messico, Brasile, Regno Unito, Francia, Germania, Cina, Giappone e Australia).

Lo studio di ricerca completo ha incluso gli altri seguenti settori: e-commerce (190), servizi finanziari (173), IT, tecnologia e telecomunicazioni (125), energia, petrolio/gas e servizi di pubblica utilità (94), settore manifatturiero e produttivo (91), retail, distribuzione e trasporti (81), tempo libero/Media & Entertainment (63), edilizia e attività immobiliari (60), servizi aziendali e professionali (58), settore pubblico (46), servizi consumer (33), altri settori (29).

Per 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 Akamai per il settore scientifico-sanitario, visitate il sito akamai.com/healthcare 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.