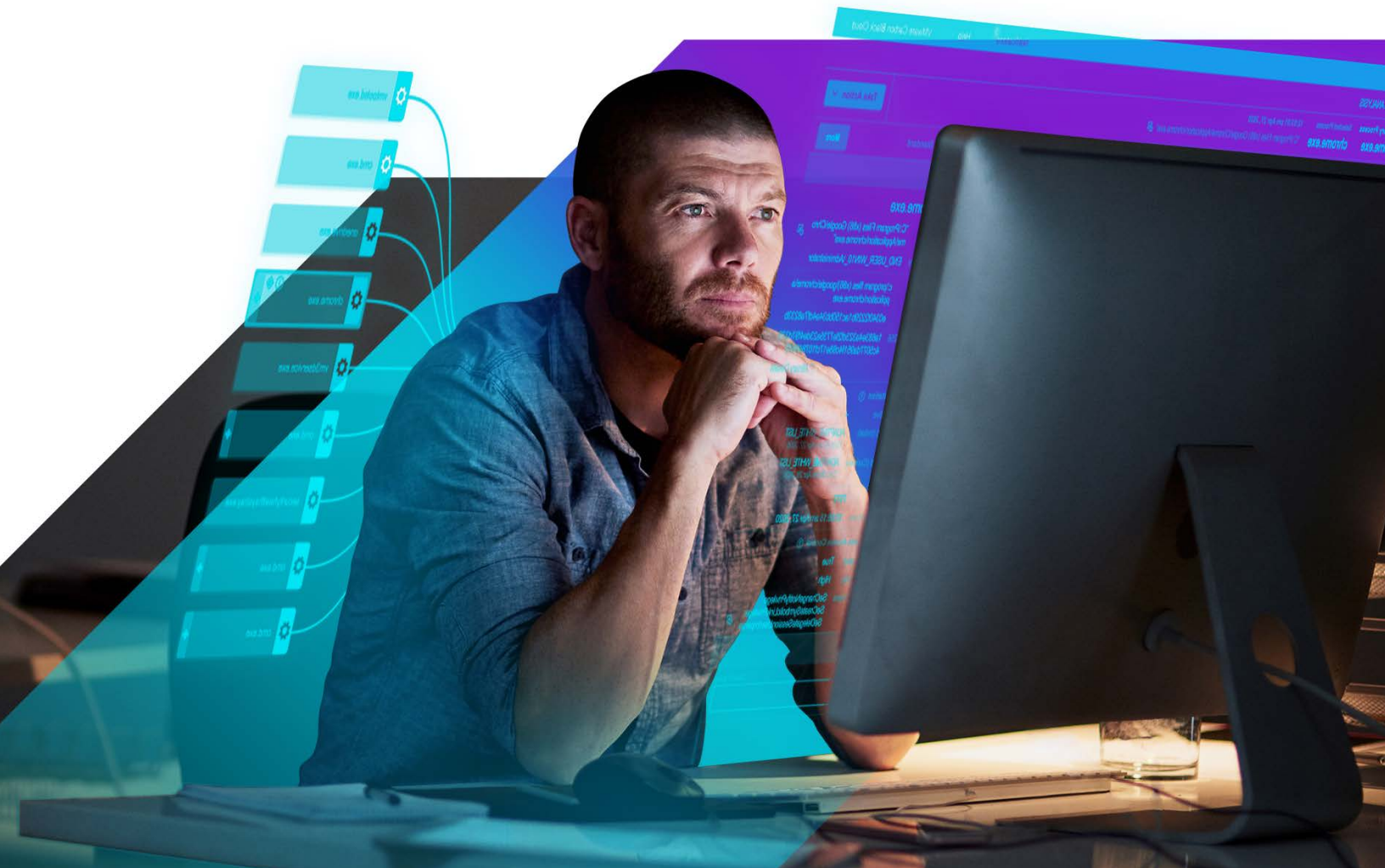
vmware®

Italia

Report Security Insights di VMware per l'Italia

2021



Introduzione

Questa ricerca è stata condotta per comprendere le sfide e le problematiche che le imprese in Italia si trovano a dover affrontare di fronte all'intensificazione degli attacchi informatici. La ricerca individua le tendenze della pirateria informatica, gli attacchi con codici dannosi e l'impatto che eventuali violazioni hanno avuto, in termini finanziari e di reputazione in quello che è stato un anno assolutamente senza precedenti. Prende in esame i piani delle aziende per la messa in sicurezza delle nuove tecnologie, per l'adozione di una strategia in materia di sicurezza informatica di tipo cloud-first e la complessità dell'attuale ambiente di gestione della cybersicurezza.

Leggete questo report per scoprire come i CISO stanno pianificando di adattarsi alle sfide di sicurezza legate a un luogo di lavoro distribuito e di far evolvere le difese per rendere la sicurezza intrinseca a infrastrutture e attività operative.

Riepilogo per la dirigenza:

Prefazione

ANALISI DEL PANORAMA DELLA SICUREZZA INFORMATICA IN ITALIA

Di Rick McElroy, Principal Cybersecurity Strategist, Security BU di VMware

Tutto è diverso… eppure uguale.

I professionisti della cybersecurity che hanno contribuito alla seconda edizione del nostro report Security Insights per l'Italia sono in una posizione molto diversa rispetto a quando hanno risposto al sondaggio del 2020. Dopo un anno che ha visto la più vasta e veloce trasformazione dei modelli di lavoro nella storia, i team di sicurezza ora presiedono un ecosistema che è più distribuito ed eterogeneo che mai.

I programmi di digital transformation sono avanzati rapidamente mentre la superficie degli attacchi informatici si espandeva fino a includere salotti, cucine, reti domestiche e dispositivi personali. La forza lavoro remota si comporta in modo molto diverso dalla forza lavoro in ufficio, accedendo alla rete in orari imprevedibili mentre si sforza di rimanere produttiva e al contempo si prende cura della propria famiglia e segue le restrizioni governative. Di conseguenza, il traffico di rete ha subito cambiamenti che lo rendono irriconoscibile. I defender devono adattare i sistemi di monitoraggio e i punti trigger o rischiano di consentire agli autori delle minacce di usare modelli atipici per mascherare i tentativi di infiltrazione.

In questo contesto in rapido cambiamento, alcune cose rimangono le stesse: un settore che non è stato sconvolto dal COVID-19 è il crimine informatico.

La frequenza degli attacchi è alta, la loro raffinatezza continua ad evolversi e le violazioni sono l'inevitabile risultato.

Tre quarti (74%) dei 251 intervistati nell'ambito della nostra indagine hanno dichiarato che il numero di attacchi che si sono trovati a dover affrontare è aumentato nell'ultimo anno e di questi, il 71% ha affermato che gli attacchi sono aumentati come risultato del maggior numero di dipendenti che lavorano da casa. Il 66% ha dichiarato che gli attacchi sono diventati più sofisticati e, tra questi, il 14% ha affermato che erano significativamente più sofisticati – un aumento rispetto al 5% che aveva affermato lo stesso nel report di giugno del 2020.

I CISO non riescono a vedere negli angoli

I volumi dei cyberattacchi sono cresciuti, ma il rapido passaggio al lavoro da remoto significa che le aziende non stanno ancora vedendo il quadro completo. Il comportamento discontinuo dei dipendenti, l'uso dei dispositivi personali e della rete domestica riducono la visibilità, creando punti ciechi e angoli bui dove gli attacchi non vengono rilevati. Di conseguenza:

Il 71%

ha dichiarato che gli attacchi sono aumentati a causa del lavoro da casa

2,4

violazioni, in media, per azienda, all'anno

L'86%

ha dichiarato di aver subito una violazione sostanziale

Il risultato? Il numero di violazioni è aumentato, con gli intervistati che hanno subito un attacco informatico che riportano 2,4 violazioni in media all'anno. Non si è trattato di incidenti minori; in otto casi su dieci, la violazione era costituita da un incidente sostanziale che ha richiesto la segnalazione alle autorità di regolamentazione o il coinvolgimento di un team di IncidentResponse.

Chiaramente, i team responsabili della sicurezza sono sotto pressione e c'è poco compiacimento:

Il 41% dei CISO teme una violazione sostanziale nel prossimo anno.

Debolezza dei processi, tecnologia di sicurezza obsoleta e ransomware rappresentano le principali cause delle violazioni

Quando abbiamo chiesto cosa stesse causando le violazioni, i tre principali vettori costruiscono un quadro di minacce esterne e debolezze interne. La debolezza dei processi è stata la causa più comune, alla base del 14% delle violazioni, seguita da vicino da una tecnologia di sicurezza non aggiornata e poi dal ransomware.

Il rapido spostamento verso il lavoro da qualsiasi luogo ha esposto le aziende carenti in termini di igiene della sicurezza e che non avevano implementato l'autenticazione multifattoriale. Tali aziende hanno pagato un caro prezzo per tecnologie e processi obsoleti.

Il ritorno del ransomware

Il ransomware ritorna come una delle principali cause di violazione, mentre gli aggressori lanciano campagne in più fasi sofisticate e redditizie.

Il 10% **di tutte le violazioni è stato causato dal ransomware.**

Oltre a queste minacce, la rapida escalation del ransomware ha aggiunto ulteriori sgradite tensioni. Le campagne multifase che prevedono penetrazione, persistenza, furto di dati ed estorsione stanno aumentando la pressione, mentre gli aggressori sfruttano le interruzioni affrontate dai lavoratori remoti. Nella maggior parte degli attacchi legati al ransomware, la posta elettronica continua a essere utilizzata come il vettore di attacco più frequente per acquisire l'accesso iniziale.

Lo sviluppo di app e il relativo consumo costituiscono motivo di apprensione

Anche le app di terze parti sono una causa frequente di violazioni secondo i CISO da noi intervistati, quindi non sorprende che i team di sicurezza si stiano concentrando sull'affinare il loro approccio al consumo e sviluppo di dette app.

Quasi metà degli intervistati è d'accordo sul fatto che[1] hanno bisogno di una migliore visibilità sui dati e sulle app per prevenire gli attacchi e un numero simile concorda sulla necessità di una migliore sicurezza contestuale per tracciare la sicurezza dei dati attraverso il ciclo di vita delle applicazioni. L'impatto della pandemia di COVID-19 è riconosciuto: il 47% degli intervistati concorda sul fatto che sia necessario considerare la sicurezza in modo diverso rispetto al passato a causa dell'espansione della superficie soggetta agli attacchi.

Le app sono inoltre in cima alla lista come il punto più vulnerabile nel percorso dei dati, ma non sono affatto l'unica area di preoccupazione.

I carichi di lavoro stanno aumentando significativamente di importanza come fonte di vulnerabilità percepita.

[1] D'accordo" corrisponde alle opzioni "Decisamente d'accordo" e "Abbastanza d'accordo" combinate fra loro.

Il 17% degli intervistati ha dichiarato che i carichi di lavoro sono il punto di violazione più vulnerabile nel percorso dei dati all'interno della loro azienda, notando che 12 mesi fa le cose non stavano così.

Un ulteriore 4% ha dichiarato che i carichi di lavoro hanno costituito il punto di maggiore vulnerabilità per più di 12 mesi. I team stanno riconoscendo che gli antivirus tradizionali non riescono a proteggere i carichi di lavoro dei server e le configurazioni errate rappresentano un rischio significativo di violazione. Questo spesso si verifica a causa di un divario di conoscenze tra i team di sicurezza e quelli dell'infrastruttura: i team di sicurezza non sanno come i carichi di lavoro di produzione dovrebbero comportarsi e i team dell'infrastruttura non sono esperti nel riconoscere il comportamento degli aggressori. Quest'anno prevediamo che le aziende cercheranno di affrontare queste lacune e rafforzare le difese per i carichi di lavoro nel cloud.

Per quanto riguarda quest'ultimo, la nostra ricerca rileva che il passaggio al cloud è effettivamente in corso. Quasi tutti i CISO che abbiamo intervistato o seguono già una strategia di sicurezza incentrata sul cloud, o prevedono di farlo molto presto. Si tratta di un cambiamento considerevole e mostra che le aziende stanno accelerando la loro tabella di marcia nell'ambito della sicurezza del cloud in risposta alle sfide legate alla pandemia di COVID-19. Potrebbe trattarsi di una strada che stavano già percorrendo, ma stanno spingendo sull'acceleratore riconoscendo l'imperativo di una sicurezza di tipo cloud-first, per un mondo "cloud-first".

Ci auguriamo che possiate trovare il nostro secondo **report VMware dedicato alle Security Insights per l'Italia** ricco di analisi e informazioni.

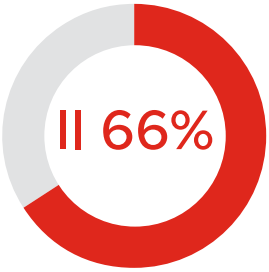
Risultati principali

La frequenza degli attacchi e il rischio di violazioni si mantengono alti

La frequenza degli attacchi è alta, la loro raffinatezza continua ad evolversi e le violazioni sono l'inevitabile risultato.

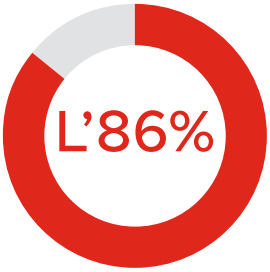
Il 74% ha dichiarato che i volumi degli attacchi sono aumentati negli ultimi 12 mesi, con una media del 62% nelle aziende colpite.

Il 71% di quanti hanno subito un attacco informatico ha dichiarato che l'aumento degli attacchi è dovuto al maggior numero di persone che lavorano da casa.

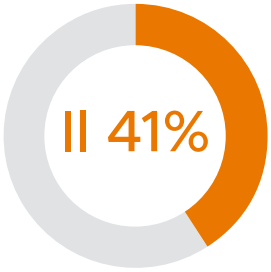


di quanti hanno subito un attacco informatico ha dichiarato che gli attacchi sono diventati più sofisticati.

ha subito una violazione negli ultimi dodici mesi; le aziende colpite hanno subito una media di 2,4 violazioni durante tale arco temporale.



ha dichiarato che le violazioni subite erano di tipo sostanziale.



teme una violazione sostanziale nei prossimi dodici mesi.

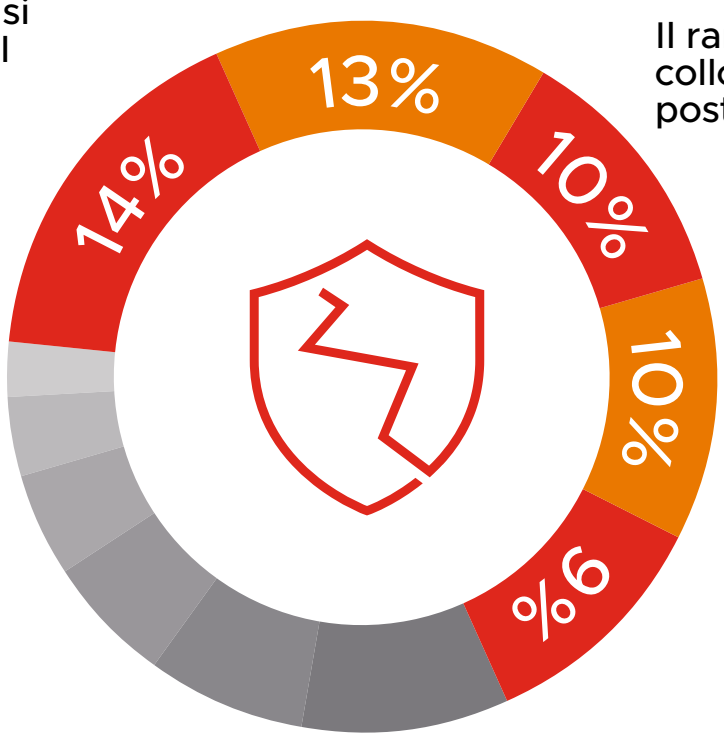
Tecnologia obsoleta, debolezza dei processi e ransomware sono in cima alle preoccupazioni dei CISO

I tre vettori principali che causano violazioni danno vita a un quadro costituito da minacce esterne e debolezze interne.

Ecco le principali cause di violazioni per chi aveva subito un attacco informatico:

La debolezza dei processi si è collocata al primo posto con il 14%.

Una tecnologia di sicurezza obsoleta si è collocata al secondo posto con il 13%.



Il ransomware si è collocato al terzo posto con il 10%.

A completare le prime cinque posizioni troviamo poi la vulnerabilità del sistema operativo (10%) e le applicazioni di terze parti (9%).

App e carichi di lavoro sono inoltre in cima alla lista come il punto più vulnerabile nel percorso dei dati, ma non sono affatto l'unica area di preoccupazione.

L’espansione delle superfici soggette agli attacchi ha spinto i leader a ripensare il tradizionale approccio alla sicurezza

La buona notizia è che c’è il riconoscimento di un cambiamento fondamentale nella sicurezza per un’era digitale altamente connessa, che supporta il lavoro a distanza.

Il 47% è d’accordo sul fatto di avere bisogno di concepire la sicurezza in modo diverso da come è stato fatto in precedenza, dato che la superficie di attacco si è ampliata.

Il 52% concorda sul fatto di avere bisogno di una migliore sicurezza contestuale per essere in grado di tracciare i dati attraverso il ciclo di vita.

Il 48% è d’accordo sul fatto di avere bisogno di una migliore visibilità su dati e app per prevenire gli attacchi.

Nei piani per il 2021 troviamo: semplificazione, consolidamento e il passaggio a una strategia di tipo cloud-first

I CISO intervistati sembrano seguire un percorso di consolidamento tecnologico e l'adozione di un approccio più intrinseco alla sicurezza, mentre il 31,5% afferma di stare aumentando il budget per la sicurezza al fine di raggiungere questi obiettivi.

Il 51% sta integrando maggiore sicurezza nell'infrastruttura e nelle app, nonché riducendo il numero di soluzioni mirate.

Il 31,5% ha adattato la propria sicurezza per mitigare il rischio.

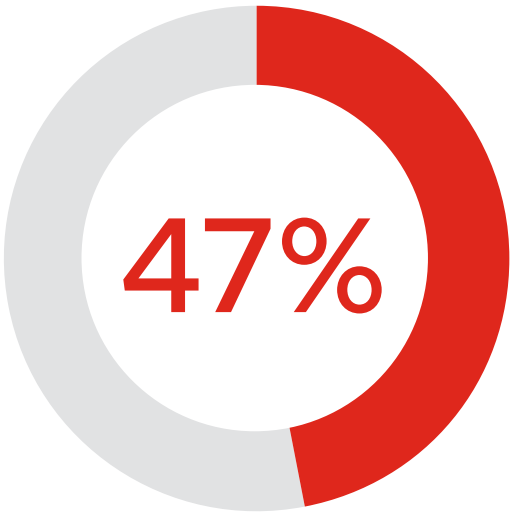
Il 37,5% ha aggiornato la propria tecnologia di sicurezza per mitigare il rischio.

Il 40% ha aggiornato la propria policy di sicurezza e il proprio approccio per mitigare il rischio.

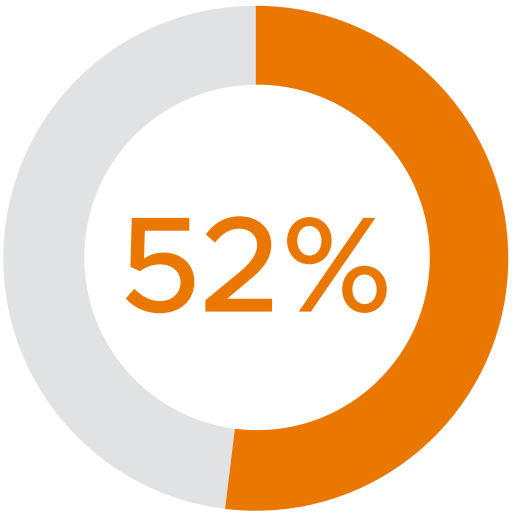
Il 95% è passato, o ha in programma di passare, a una strategia di sicurezza di tipo cloud-first.

L'IA è la prossima frontiera per l'innovazione aziendale – ma i problemi di sicurezza stanno soffocando il progresso?

La prossima frontiera per l'innovazione aziendale è l'intelligenza artificiale, dato che le aziende cercano un vantaggio per promuovere servizi ai clienti ed esperienze digitali più competitivi.

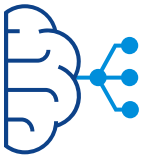


Eppure, quasi la metà degli intervistati (47%) concorda sul fatto che i problemi di sicurezza stanno impedendo loro di abbracciare le app basate su intelligenza artificiale/apprendimento automatico per migliorare tali servizi.



E il 52% degli intervistati concorda sul fatto che la capacità di innovare dipende dalla capacità di costruire e far arrivare app nelle mani di dipendenti e clienti in modo più sicuro.

L'IA è la prossima frontiera per l'innovazione aziendale – ma i problemi di sicurezza stanno soffocando il progresso?



Molti intervistati temono di non essere in grado di sfruttare l'opportunità digitale.

Il 43% è d'accordo sul fatto che c'è troppa complessità nel mercato delle soluzioni di sicurezza per fargli cambiare la propria policy in materia di sicurezza, anche se sa che la sicurezza IT odierna non sta funzionando.

Il 48% è d'accordo sul fatto che il proprio consiglio di amministrazione/team di alti dirigenti è sempre più preoccupato quando si introducono nuove app/nuovi servizi sul mercato, a causa della crescente minaccia e del danno che le violazioni/gli attacchi riguardanti i dati comportano.

Il 44% è d'accordo sul fatto di voler utilizzare in misura maggiore l'intelligenza artificiale/l'apprendimento automatico nelle proprie applicazioni per migliorare sicurezza e servizi.

Il 48% è d'accordo sul fatto di avere bisogno di una migliore visibilità su dati e app per prevenire gli attacchi.

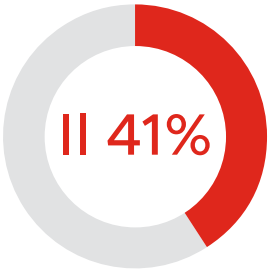
Proteggere il brand e la reputazione: questo impone una maggiore urgenza di cambiamento?

Il brand e la reputazione rimangono il Santo Graal per le imprese ed è facile che vadano persi. Tuttavia, l'impatto che le violazioni della sicurezza hanno sulla reputazione supera quello finanziario.

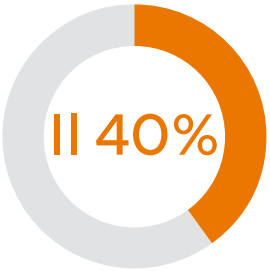
Il 66% di coloro che hanno subito un cyberattacco afferma che ci sia stato in qualche misura un impatto negativo sulla reputazione.

L'86% degli intervistati che hanno subito una violazione ha dovuto effettuare una segnalazione alle autorità di regolamentazione o ingaggiare una società di IncidentResponse per superare i problemi di reputazione causati da violazioni sostanziali.

Tra gli intervistati, la percezione della gravità di queste violazioni non è uniforme e si riscontra una mancanza di urgenza di cambiamento, nonostante il crescente panorama di minacce.



teme di subire una violazione sostanziale nell'anno a venire.



ha aggiornato la propria policy di sicurezza e il proprio approccio per mitigare il rischio.

I risultati completi dell'indagine

Ha riscontrato un aumento degli attacchi informatici nei confronti della sua azienda negli ultimi 12 mesi? Se sì, può quantificare?

Il 74% dei CISO interpellati ha dichiarato di aver riscontrato un aumento del numero di attacchi informatici nei confronti della propria azienda negli ultimi 12 mesi. L'aumento medio dei volumi di attacchi riportato è pari al 62%, ossia un calo rispetto all'aumento del 78% dei volumi medi degli attacchi riportati nel giugno 2020.

La media ha premiato il settore sanitario, con il 62% degli intervistati che ha riportato un aumento del volume degli attacchi. Nel settore retail, tuttavia, il 95% degli intervistati ha riferito un aumento.

Le piccole aziende sono sotto pressione, con il 16% dei CISO di aziende con meno di 50 dipendenti che affermano che i volumi di attacchi sono aumentati in misura superiore al 100%.

Il numero di attacchi informatici globali tipici rivolti contro il vostro sistema è cambiato a causa del maggior numero di dipendenti che lavorano da casa per via della pandemia di COVID-19?

Il 71% degli intervistati che aveva sperimentato attacchi informatici ha dichiarato di aver notato un aumento della frequenza dovuto al fatto che un maggior numero di dipendenti lavora da casa.

Gli intervistati del settore della pubblica amministrazione hanno riscontrato un aumento superiore alla media degli attacchi, a causa del lavoro da casa dei dipendenti; l'80% ha riferito un aumento.

I team IT con 31-40 membri hanno segnalato aumenti degli attacchi superiori alla media; l'81,5% ha riscontrato un aumento della frequenza.

Gli attacchi informatici nei confronti della sua azienda sono diventati più o meno sofisticati negli ultimi 12 mesi?

In termini di raffinatezza degli attacchi, il 66% dei CISO interpellati che avevano subito un attacco informatico ha riscontrato un aumento della raffinatezza.

Il 66% dei CISO interpellati ha riscontrato che gli attacchi sono diventati più sofisticati.

Il 27% degli intervistati che avevano subito attacchi ha detto che questi sono diventati moderatamente più sofisticati e per il 14% lo sono diventati in modo significativo, un aumento rispetto al 5% che lo aveva dichiarato nel report di giugno 2020.

La raffinatezza degli attacchi è cresciuta in maniera superiore alla media nel settore dei servizi finanziari, dove il 27% degli intervistati ha dichiarato che gli attacchi che si trovavano a dover affrontare erano significativamente più raffinati.

Qual è stato il tipo di attacco informatico più prolifico (vale a dire, più frequente) che la sua azienda ha subito negli ultimi 12 mesi?

In Italia, il contesto degli attacchi è diversificato, con pochi intervistati che riscontrano lo stesso mix di tipologie e nessun tipo di attacco risulta dominante. Questo mette in evidenza le sfide che i CISO italiani si trovano a dover affrontare: hanno infatti bisogno di costruire risposte strategiche e tattiche a un mix incredibilmente diversificato di vettori e tecniche di attacco.

Il malware di tipo "commodity" (reperibile attraverso canali non legali, N.d.T.) è in cima alla classifica, con il 9% degli intervistati che ha subito un attacco informatico di questo tipo con maggiore frequenza. Tuttavia, il ransomware e il formjacking (una tipologia di attacchi indirizzata ai form di siti di e-commerce e/o portali in cui è richiesto l'inserimento dei dati di una carta di credito, N.d.T.) si collocano subito dopo come tipo di attacco principale per l'8% degli intervistati in ciascun caso.

Gli attacchi fileless e il malware personalizzato rappresentano ciascuno il 7% degli attacchi affrontati.

Qual è stata la frequenza delle violazioni dovute ad attacchi informatici subite dalla sua azienda negli ultimi 12 mesi?

L'85% delle aziende interpellate ha subito una violazione alla sicurezza nell'ultimo anno.

L'85% dei CISO che hanno partecipato alla nostra ricerca ha dichiarato che la loro azienda aveva subito una violazione a causa di un attacco informatico nell'ultimo anno. Si tratta di un dato è in calo, rispetto al 99% che aveva dichiarato di essere stato vittima di violazioni nel giugno 2020.

Il numero medio di violazioni subite da ciascuna azienda è aumentato leggermente, passando da 2,2 (dato del giugno 2020) a 2,4 (dato di questo report). Il 16,5% degli intervistati ha affermato che la propria azienda aveva subito cinque o più violazioni.

Il settore sanitario ha subito un numero di violazioni superiore alla media: 3,4.

Qual è stata la causa principale di queste violazioni?

Il 14% dei CISO intervistati che avevano subito un attacco informatico si è trovato a dover affrontare una sgradita scoperta: la causa delle violazioni andava ricercata nella debolezza dei processi. Ad aggravare questo problema c'era una tecnologia di sicurezza dei dati non aggiornata, che è stata la causa delle violazioni per il 13%. La tensione esercitata dall'improvviso passaggio al lavoro a distanza ha messo chiaramente in evidenza quelle aree in cui policy e tecnologia non sono riuscite a tenere il passo con l'ambiente in evoluzione.

Tuttavia, la responsabilità non era interamente da attribuire all'azienda: il 10% delle violazioni è il risultato di un ransomware. Il 10% delle violazioni sono state attribuite alla vulnerabilità del sistema operativo e il 9% ad applicazioni di terze parti. Ancora una volta, questa diversità di cause di violazione evidenzia i molti fronti su cui i CISO italiani devono difendere la propria azienda.

La debolezza dei processi è stata un problema particolare nelle aziende sanitarie, causando più di un quinto (21%) delle violazioni. Per il settore della pubblica amministrazione, una tecnologia di sicurezza dei dati non aggiornata è stata responsabile del 19,5% degli incidenti di violazione.

Quale percentuale delle violazioni dovute a un attacco informatico negli ultimi 12 mesi ritiene sia stata una violazione sostanziale, vale a dire che ha dovuto segnalarla alle autorità di regolamentazione/chiamare un team di IncidentResponse per effettuare il ripristino, ecc.?

Quando avviene una violazione, si tratta di una faccenda seria. La maggior parte degli intervistati (86%) ha dovuto effettuare una segnalazione alle autorità di regolamentazione o ingaggiare una società di IncidentResponse per superare i problemi causati da violazioni negli ultimi 12 mesi.

L'86% delle aziende ha subito una violazione sostanziale.

Il 48% degli intervistati che ha subito un cyberattacco ha dichiarato che il 21-30% delle violazioni era sostanziale e un ulteriore 29% ha affermato che il 31-40% delle violazioni era sostanziale.

Il 56% degli interpellati operanti nel settore dei servizi finanziari e il 54% di quelli operanti nel settore della pubblica amministrazione hanno affermato che il 21-30% delle violazioni era sostanziale.

Quali sono state le conseguenze di tali violazioni per la sua azienda, dal punto di vista finanziario e della reputazione?

Solo il 9% degli intervistati che aveva subito un cyberattacco ha dichiarato di aver avuto un impatto finanziario negativo dovuto a una violazione dei dati subita dalla propria azienda. Si tratta di un dato notevolmente inferiore a quello della media globale, che si attesta al 24%. Secondo il 31,5% degli intervistati, non c'era stato alcun impatto finanziario; tuttavia, il 43% ha dichiarato di non sapere quale impatto finanziario avevano causato le violazioni subite.

Nel complesso, l'effetto sulla reputazione del brand è stato più consistente. Il 66% degli intervistati che hanno subito un attacco informatico ha dichiarato che il loro brand era stato influenzato negativamente da una violazione dei dati.

Solo il 20% ha affermato di non aver subito alcuna perdita, in termini di reputazione, a seguito di una violazione.

Gli intervistati del settore dei servizi finanziari sono stati molto più propensi a segnalare un impatto finanziario negativo – con il 19% che ha dichiarato di aver subito danni economici.

In che misura teme le violazioni sostanziali da cui, a suo avviso, sarà colpita la sua azienda nei prossimi 12 mesi?

Esiste decisamente un fattore "paura" associato all'eventualità di violazioni sostanziali nel prossimo anno. Due quinti (41%) sono molto timorosi, o in una certa misura timorosi, che una violazione possa colpire la propria azienda; di questi, il 10% è molto timoroso.

Il settore dei servizi finanziari mostra una suddivisione in termini di preoccupazione, con il 48% degli intervistati che dice di temere una violazione, mentre il 10% non crede che ci sarà una violazione nel prossimo anno. Il 45% degli intervistati operanti nel settore della pubblica amministrazione teme una violazione.

Come state affrontando questo aspetto (la probabilità di violazioni), se lo state affrontando?

Alla domanda in merito ai piani per mitigare il rischio di violazioni, gli intervistati hanno dato la priorità alla semplificazione e al consolidamento delle soluzioni di sicurezza, unitamente alla capacità di rendere la sicurezza un aspetto intrinseco. Sono state ritenute importanti anche l'adattamento della tecnologia e della policy e la capacità di destinare un budget alla questione.

Il 51% degli intervistati ha dichiarato che prevede di **incorporare più sicurezza nell'infrastruttura e nelle app e di ridurre il numero di soluzioni dedicate a un unico scopo**. Questo dato sale al 53% per il settore della pubblica amministrazione.

Il 31,5% ha dichiarato di aver **adattato la propria sicurezza per mitigare il rischio**. In questo caso è il settore dei servizi finanziari quello maggiormente propenso ad adottare tale approccio (40%).

> Il 51% ha in programma di incorporare più sicurezza nella propria infrastruttura e nelle app e di ridurre il numero di soluzioni dedicate a un unico scopo.

Il 31,5% ha **aumentato il budget destinato alla sicurezza**.

Il 37,5% ha detto di **aver aggiornato la propria tecnologia di sicurezza per mitigare il rischio** – un investimento importante, visti i significativi cambiamenti avvenuti nel panorama della sicurezza nell'ultimo anno. Il 46% delle aziende operanti nel settore sanitario ha adottato questo approccio.

Il 40% ha **aggiornato la propria policy di sicurezza e il proprio approccio per mitigare il rischio**. Gli intervistati del settore della pubblica amministrazione (47%) erano maggiormente propensi ad adottare questo approccio rispetto a quelli di altri settori.

In che misura è d'accordo, o in disaccordo, con le seguenti affermazioni relative allo sviluppo e al consumo di app nella sua azienda?

Alla domanda relativa al cambiamento del modo di considerare le sfide di sicurezza inerenti allo sviluppo e al consumo di app nella loro azienda, i nostri intervistati hanno offerto un'analisi dei problemi che stanno affrontando.

La visibilità rappresenta un motivo di preoccupazione. Il 48% è d'accordo sul fatto di avere **bisogno di una migliore visibilità su dati e app per prevenire gli attacchi**. Questo dato sale al 62% per il settore dei servizi finanziari.

> Il 48% ha bisogno di una maggiore visibilità su dati e app.

Il 47% degli intervistati italiani è d'accordo sul fatto che il cambiamento nel panorama degli attacchi provocato dalla pandemia di COVID-19 richiede un ripensamento della sicurezza, concordando sulla **necessità di concepire la sicurezza in modo diverso da quanto fatto in precedenza, dato che la superficie suscettibile agli attacchi si è ampliata**.

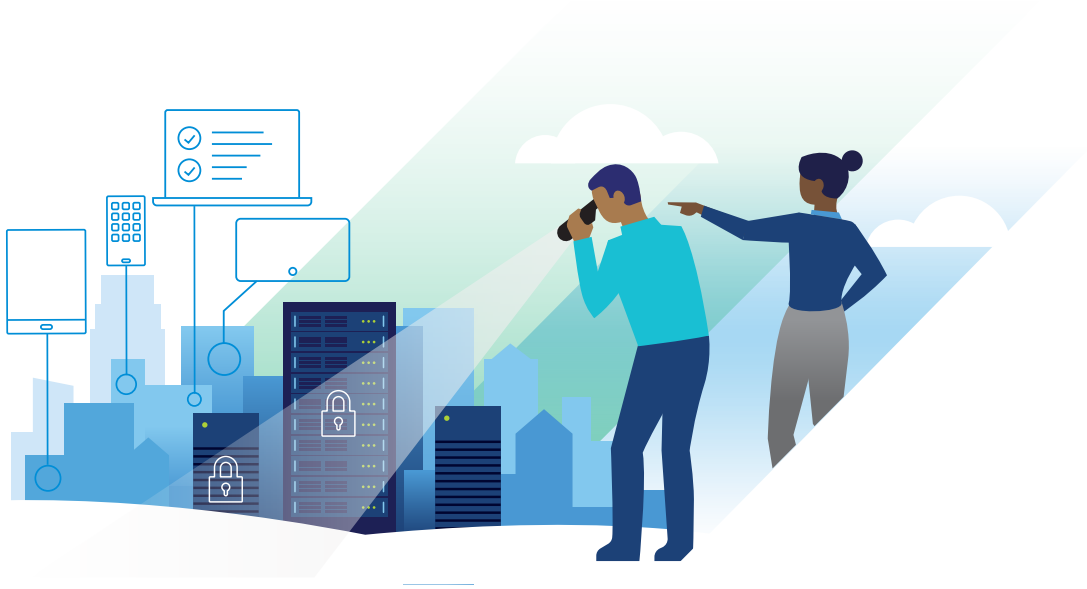
> Il 52% è d'accordo sul fatto di avere bisogno di una maggiore sicurezza contestuale per tracciare i dati/la sicurezza attraverso il ciclo di vita.

Oltre la metà (52%) afferma di **avere bisogno di una migliore sicurezza contestuale per essere in grado di tracciare i dati attraverso il ciclo di vita**. Questo sta a indicare un ambiente prevalente in cui la sicurezza tende ad essere incentrata sulle minacce e reattiva. I leader IT stanno riconoscendo che gli ambienti dinamici richiedono un approccio incentrato sul contesto.

Il 52% degli intervistati italiani ha convenuto che la loro **capacità di innovare come azienda dipende dalla capacità di costruire, gestire e distribuire app in modo più sicuro**.

Il 49% degli intervistati **si sente sicuro nell'introdurre nuove app/nuovi servizi sul mercato perché sa che saranno sicuri** – questo dato è inferiore alla media internazionale. La fiducia è più alta tra gli intervistati operanti nel settore dei servizi finanziari, dove il 58% è fiducioso all'idea di introdurre nuove app/nuovi servizi sul mercato.

Interrogati sulla loro visione dell'IA nello sviluppo di app sicure, gli intervistati hanno riportato opinioni discordanti. Il 47% è d'accordo sul fatto che **le preoccupazioni per la sicurezza ci impediscono di abbracciare app basate su intelligenza artificiale/apprendimento automatico per migliorare i servizi**, ma il 44% è d'accordo sul fatto che **per migliorare la sicurezza e i servizi, vorrebbe usare più IA e apprendimento automatico nelle app**.



Il 43% è d'accordo sul fatto che **c'è troppa complessità nel mercato delle soluzioni di sicurezza per far cambiare la relativa policy, pur ammettendo che la sicurezza IT di oggi non sta funzionando**. Questo dato sta a indicare che i vendor hanno del lavoro da fare per semplificare la loro proposta integrandola in un approccio unificato.

Da ultimo, il 48% è d'accordo sul fatto che la sicurezza delle app stia attirando l'attenzione a livello di consiglio di amministrazione e che il proprio **consiglio di amministrazione/ team di alti dirigenti è sempre più preoccupato quando si introducono nuove app/nuovi servizi sul mercato, a causa della crescente minaccia e del danno che le violazioni/ gli attacchi riguardanti i dati comportano**.

Il 48% afferma che il proprio consiglio di amministrazione è sempre più preoccupato dei rischi di sicurezza legati all'introduzione di nuove app sul mercato.

Quale ritiene sia il punto più suscettibile a una violazione nel percorso dei dati all'interno della vostra infrastruttura di sicurezza? E questa vulnerabilità è cambiata negli ultimi 12 mesi?

Le applicazioni sono state indicate come il punto più esposto alle violazioni nel percorso dei dati ed è chiaro che questo, da qualche tempo, costituisce una preoccupazione. Quello che è più interessante è che i carichi di lavoro stanno aumentando significativamente come fonte di vulnerabilità percepita. È probabile che l'anno prossimo le aziende si concentreranno maggiormente su questo rischio.

28%
App

Per il 13% lo sono oggi e lo erano 12 mesi fa, per il 15% lo sono oggi e non lo erano 12 mesi fa

21%
Carichi di lavoro

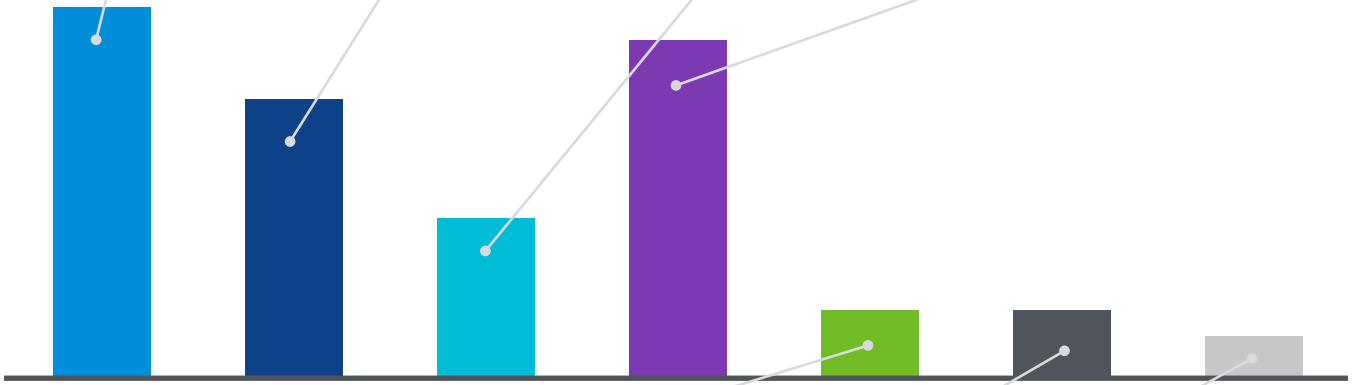
Per il 4% lo sono oggi e lo erano 12 mesi fa, per il 17% lo sono oggi e non lo erano 12 mesi fa

12%
Endpoint

Per il 8% lo sono oggi e lo erano 12 mesi fa, per il 4% lo sono oggi e non lo erano 12 mesi fa

25,5%
Reti

Per il 16% lo sono oggi e lo erano 12 mesi fa, per il 9,5% lo sono oggi e non lo erano 12 mesi fa



5%
Edge

Per il 3% lo è oggi e lo era 12 mesi fa, per il 2% lo è oggi e non lo era 12 mesi fa

5%
Cloud

Per il 3% lo è oggi e lo era 12 mesi fa, per il 2% lo è oggi e non lo era 12 mesi fa

3%
Container

Per l'1% lo sono oggi e lo erano 12 mesi fa, per il 2% lo sono oggi e non lo erano 12 mesi fa

Come hanno affrontato le aziende le sfide legate al passaggio al lavoro a distanza?

Abbiamo chiesto ai CISO intervistati di valutare il proprio successo nel far passare la forza lavoro alla modalità incentrata sul lavoro a distanza e se un approccio incentrato sulla sicurezza avrebbe contribuito a una transizione più efficace.

Il 40% concorda sul fatto di essere stato in grado di rendere operativa la loro forza lavoro da remoto e che la sicurezza non ha rappresentato un impedimento. Questo testimonia il lavoro dei team di sicurezza che sono stati al centro delle attività operative come mai in precedenza. Gli intervistati dei servizi finanziari se la sono cavati bene, con il 54% che concorda sul fatto di non aver incontrato impedimenti legati alla sicurezza nell'impostare il lavoro da casa. Per contro, i CISO del settore della pubblica amministrazione che abbiamo intervistato hanno riscontrato difficoltà, con il 27,5% che non è d'accordo sul fatto di essere stato in grado di rendere operativa la propria forza lavoro senza problemi.

Gli intervistati riconoscono che c'è sempre spazio per il miglioramento, con il 51% che concorda sul fatto che un approccio incentrato sulla sicurezza avrebbe aumentato la loro capacità di consentire ai dipendenti di lavorare da luoghi alternativi e rimanere produttivi. Questo dato è confermato anche da una precedente ricerca di VMware, che ha rilevato che l'incapacità di implementare l'autenticazione multifattore era il principale motivo di preoccupazione per i professionisti IT nella loro risposta al passaggio al lavoro da casa. Ora che il profilo della sicurezza è aumentato, dovrebbe essere più facile per i CISO assicurarsi il supporto del consiglio di amministrazione per un approccio incentrato sulla sicurezza.

Utilizza, o ha in programma di utilizzare, una strategia di sicurezza di tipo cloud-first?

Il 96% utilizza già, o ha in programma di adottare, un approccio incentrato sul cloud per proteggere l'azienda.

Gli intervistati hanno dichiarato quasi all'unanimità che stanno pianificando di passare a una strategia di sicurezza incentrata sul cloud – se non immediatamente, si tratta sicuramente di un obiettivo presente nella tabella di marcia nel 96% delle aziende degli intervistati.

In generale, il 35,5% afferma di aver adottato un approccio cloud-first da più di un anno, mentre il 28% sostiene di aver promosso un modello cloud-first da meno di 12 mesi. Un altro 13% prevede di implementare una tecnologia di tipo cloud-first nel prossimo anno, mentre per il 19% il passaggio avverrà più avanti nel tempo.

La maturità necessaria per adottare un approccio cloud-first è alta tra le aziende di servizi finanziari, dove il 38% e il 22% hanno optato per una strategia cloud-first rispettivamente da più di 12 mesi e da meno di 12 mesi. Il 58% degli intervistati nel settore sanitario sta già operando con una strategia di sicurezza incentrata sul cloud.

Analisi e azioni principali

Il nostro report Security Insights per l'Italia rileva che i professionisti senior della cybersecurity e le aziende che servono, continuano ad affrontare un alto volume di sofisticate minacce. Queste sono esacerbate dal passaggio a una forza lavoro altamente distribuita e, anche se la maggior parte delle aziende è riuscita a passare al lavoro da remoto, i CISO riconoscono che un approccio incentrato sulla sicurezza avrebbe reso la transizione più facile.

Indubbiamente, la pandemia di COVID-19 ha cambiato l'ambiente della sicurezza informatica in modo significativo e continuerà a influenzare la strategia in materia di sicurezza. Dal canto suo, l'industria della cybersecurity deve concentrarsi sulla fornitura di soluzioni in grado di ridurre la complessità operativa, proteggendo allo stesso tempo in modo robusto gli ambienti di lavoro distribuiti, che diventeranno lo scenario standard del futuro per la maggior parte delle aziende.

L'analisi delle risposte al sondaggio rivela aree importanti su cui concentrare l'attenzione alla sicurezza informatica nel prossimo anno:

Assegnare la priorità a migliorare la visibilità

Le aziende riscontrano un problema di visibilità dovuto al rapido passaggio al lavoro da casa. La vera gravità degli attacchi è difficile da comprendere, in quanto i defender non possono vedere negli angoli in cui i dispositivi mobili personali e le reti domestiche si sono innestati nell'ecosistema aziendale. Se aggiungiamo a questo le sfide derivanti dal monitoraggio di app di terze parti e vendor, il numero di punti ciechi aumenta in modo esponenziale.

Detto in parole semplici, i defender non sanno quello che non sanno e questo ha come conseguenza l'esposizione delle aziende. Questa visione contestuale limitata del rischio mette i defender in posizione di svantaggio quando devono proteggere una superficie soggetta ad attacchi estesa. Le aziende devono assegnare la priorità al miglioramento della visibilità di tutti gli endpoint e dei carichi di lavoro per proteggere l'ambiente di lavoro remoto. Un'intelligence situazionale solida, in grado di fornire il contesto delle minacce, aiuterà i defender ad assegnare le priorità e a porre rimedio al rischio in modo efficace.

Rispondere alla ricomparsa del ransomware

I cyberattacchi hanno continuato a diventare sempre più sofisticati e il ransomware non fa eccezione. Gli aggressori stanno ottenendo un accesso non rilevato alle reti, esfiltrando i dati e stabilendo backdoor, prima di lanciare richieste di riscatto e/o monetizzare direttamente i dati rubati. Per evitare di diventare vittime di attacchi ripetuti, le aziende hanno bisogno di combinare una protezione avanzata contro il ransomware con una robusta correzione post-attacco che rilevi l'ulteriore presenza di minacce nel loro ambiente.

Risolvere il problema di una tecnologia di sicurezza legacy ormai inefficace e della debolezza dei processi

Una sicurezza obsoleta e le debolezze dei processi continuano a rappresentare un rischio significativo per le aziende che, con il passaggio al lavoro da remoto, sono ancora più esposte. Mentre usciamo dalla fase di risposta immediata e cominciamo a vedere il futuro a lungo termine prendere forma, le aziende devono identificare i cambiamenti critici da apportare ai processi e alla tecnologia necessari per aiutare i lavoratori in modalità remota e ibrida a lavorare in modo sicuro riducendo i rischi.

Fornire sicurezza come servizio distribuito

C'è stata un'epoca in cui i team di sicurezza proteggevano i desktop di proprietà dell'azienda per i dipendenti che lavoravano in sede, collegandosi alle applicazioni aziendali in esecuzione su server situati in un data center aziendale. Il mondo è oggi un posto più complicato, con lavoratori remoti che si connettono ad applicazioni in esecuzione su infrastrutture che possono o meno essere gestite, possedute o controllate dall'azienda. Con così tante nuove superfici e tipi diversi di ambienti da difendere, la sicurezza non può essere fornita come una lista di prodotti dedicati a un unico scopo e strozzature della rete. I controlli di rete ed endpoint devono invece essere forniti come servizio distribuito. Questo significa fornire sicurezza che segue gli asset da proteggere, indipendentemente dal tipo di ambiente in oggetto.

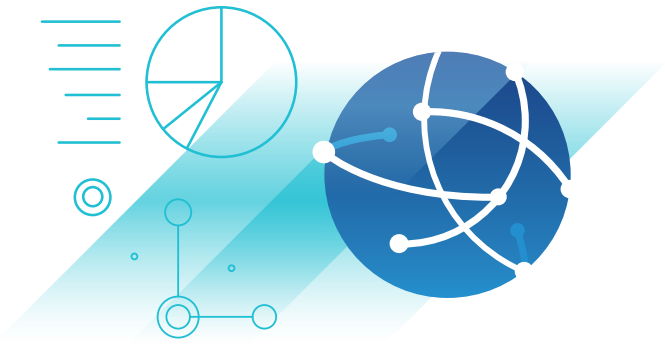
Adottare un approccio intrinseco alla sicurezza di tipo cloud-first

Il principale cambiamento messo in luce dalla nostra ricerca è il passaggio a una strategia di sicurezza incentrata sul cloud. È difficile sopravvalutare la portata del cambiamento che si è verificato in un così breve lasso di tempo; prima del 2020, pochissimi CISO avevano descritto la loro strategia di sicurezza come cloud-first. È la conseguenza del fatto che le aziende hanno dovuto rispondere alle improvvise pratiche di lavoro altamente distribuite a seguito della pandemia di COVID-19.

Ma passare al cloud non è una panacea per la sicurezza – non tutti i cloud sono uguali e i controlli devono essere approvati dalle organizzazioni di consumatori perché, se gli avversari vogliono attaccare su ampia scala, il cloud è il posto giusto per farlo. Via via che questo cambiamento prende slancio, l'investimento nella sicurezza del public cloud assumerà un'importanza fondamentale. Quando si passa a un public cloud, ci si muove su questioni molto complesse, dove la sicurezza dipende non solo dalle proprie azioni, ma anche da quelle di tutti gli altri soggetti. Se anche si è in grado di mettere al sicuro le proprie risorse, non si ha alcun controllo sugli utenti che condividono quello stesso ambiente. Le aziende devono dare la priorità alla protezione dei carichi di lavoro sul cloud in ogni punto del ciclo di vita della sicurezza, mentre il grande spostamento sul cloud continua.

In definitiva, il report Security Insights 2021 di VMware per l'Italia mostra un settore che è concentrato a costruire sui successi dell'anno scorso e a rispondere al cambiamento dell'ambiente delle minacce. I CISO hanno una chiara consapevolezza della direzione che devono percorrere e degli strumenti che devono sfruttare per restare un passo avanti rispetto agli aggressori.

Metodologia



Nel dicembre del 2020 VMware ha commissionato un'indagine a Opinion Matters, una società di ricerca indipendente. Sono stati intervistati **251 CIO, CTO e CISO** di aziende operanti in un'ampia gamma di settori come: servizi finanziari, sanità, pubblica amministrazione statale e locale, retail, produzione e progettazione industriale, alimenti e bevande, servizi di pubblica utilità, servizi professionali, media e intrattenimento. Si tratta del secondo report Security Insights per l'Italia di VMware, basato sulla precedente indagine svoltasi nel giugno del 2020, nell'ambito di un progetto di ricerca globale in **14 Paesi**, come: Australia, Canada, Arabia Saudita, Medio Oriente, Regno Unito, Francia, Germania, Spagna, Paesi Bassi, Paesi Nordici, Italia, Giappone, Singapore e Stati Uniti.

Informazioni su VMware

Il software di VMware è alla base della complessa infrastruttura digitale mondiale. Le soluzioni dell'azienda per cloud, modernizzazione delle app, networking, sicurezza e Digital Workspace aiutano i clienti a distribuire qualsiasi applicazione su qualsiasi cloud, indipendentemente dal dispositivo. VMware, la cui sede centrale è a Palo Alto, California, si impegna a essere un agente di cambiamento positivo sotto tutti gli aspetti, dalle rivoluzionarie innovazioni tecnologiche all'impatto globale. Per ulteriori informazioni, visitare vmware.com/it/company.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com