CSO

Microsoft Security

CONTENUTO SPONSORIZZATO

Sicurezza Zero Trust: **lezioni degli early adopter**

CSO Microsoft Security

Indice

CSO Microsoft Security

Introduzione

Gli ultimi due anni hanno sconvolto i modelli IT e di sicurezza tradizionali. Di conseguenza, la sicurezza Zero Trust è rapidamente passata dall'essere un concetto interessante a una solida base della moderna sicurezza aziendale.

La nuova ricerca di Foundry rivela che il 52% delle aziende sta sperimentando o ha distribuito l'architettura Zero Trust e un altro 15% sta studiando modelli Zero Trust. Le aziende che hanno adottato questa architettura segnalano numerosi vantaggi nelle proprie distribuzioni, tra cui una migliore protezione dei dati dei clienti, la riduzione della complessità e la distribuzione di un accesso sicuro e affidabile alle risorse aziendali.

Questo e-Book esplora i risultati della ricerca condotta da Foundry che evidenzia l'importanza di una strategia Zero Trust per aiutare i CISO a proteggere le proprie aziende da una moltitudine di rischi posti da numerosi vettori di attacco. Include inoltre indicazioni su come implementare Zero Trust per chi ha appena iniziato il percorso.

Informazioni sul sondaggio

A febbraio e marzo 2022, Foundry ha intervistato aziende statunitensi per esplorare lo stato attuale dell'adozione di Zero Trust. Gli intervistati dovevano ricoprire la posizione di responsabile IT o una posizione superiore presso un'azienda con più di 500 dipendenti e avere un ruolo nell'acquisto di prodotti e servizi di sicurezza informatica.

Gli intervistati sono stati in totale 250 per un sondaggio di 23 domande.

CSO Microsoft Security

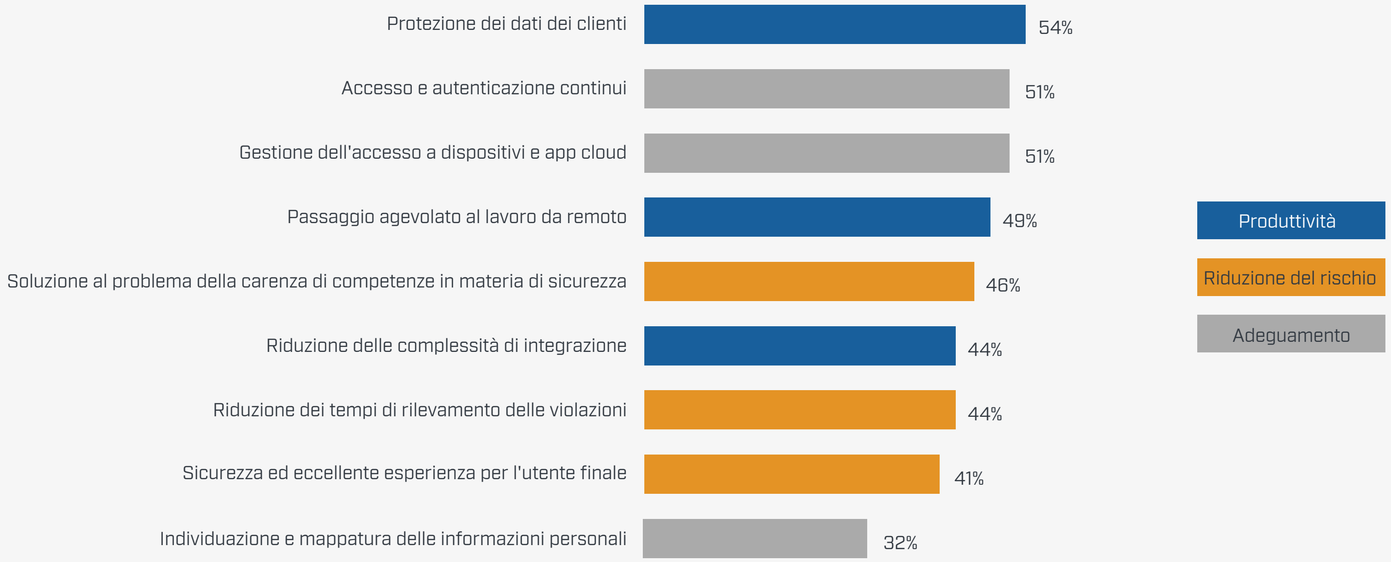
Zero Trust è ormai una realtà e offre valore

I risultati della ricerca, così come le interviste approfondite con dirigenti IT e della sicurezza, evidenziano quanto Zero Trust sia in cima alla lista delle priorità della maggior parte delle aziende. E quelle che hanno distribuito diverse componenti Zero Trust ne stanno già apprezzando i vantaggi.

La maggior parte degli intervistati che hanno implementato Zero Trust (87%) afferma che l'architettura soddisfa pienamente o supera gli obiettivi originari in termini di implementazione, adozione e integrazione.

"Per noi, il modello [Zero Trust] è diventato una procedura operativa standard. Non credo che torneremo mai indietro", afferma il direttore IT di un rivenditore globale. Agli intervistati è stato garantito l'anonimato, così da poter parlare liberamente dei propri piani di sicurezza.

Vantaggi ottenuti dalla implementazione di Zero Trust



Il 12% degli intervistati ha affermato di ottenere *tutti* questi vantaggi

Fonte: Zero Trust Adoption Survey, marzo 2022, Foundry. Base: 250

CSO Microsoft Security

Circa il 44% degli intervistati ha inoltre affermato che Zero Trust ha ridotto le complessità associate all'implementazione di un'architettura di sicurezza integrata. "Quando si gestisce e si lavora con un framework, tutto diventa meno complicato", afferma il CISO di un'azienda di call center con 3.500 dipendenti.

Un VP e CISO di una società di servizi finanziari con 17.000 dipendenti afferma che l'autenticazione a più fattori implementata dall'azienda nell'ambito della strategia Zero Trust ha riscosso un enorme successo tra i dipendenti. "Ha davvero aumentato la soddisfazione dei dipendenti, i quali ora non devono più passare al dispositivo fornito dall'azienda e usare un client VPN, ma possono accedere alle risorse ovunque si trovino", afferma.

Il concetto di accesso con privilegi minimi ha, a sua volta, determinato dei vantaggi, commenta il CISO. "Grazie all'implementazione di quel sistema di accesso con privilegi, abbiamo riscontrato un minor numero di errori disastrosi da parte degli amministratori di sistema", afferma. "Questi ottengono infatti i privilegi per attività e periodi di tempo specifici, limitando così le probabilità di fare errori".

Con la maggiore diffusione di attacchi di phishing e altri attacchi informatici, il direttore IT dell'azienda retail riassume i vantaggi di Zero Trust in questo modo: "Se non avessimo questi tipi di strumenti, probabilmente ora ci troveremmo in una brutta situazione, obbligati a pagare qualcuno in bitcoin".

CSO Microsoft Security

Fattori chiave della distribuzione Zero Trust

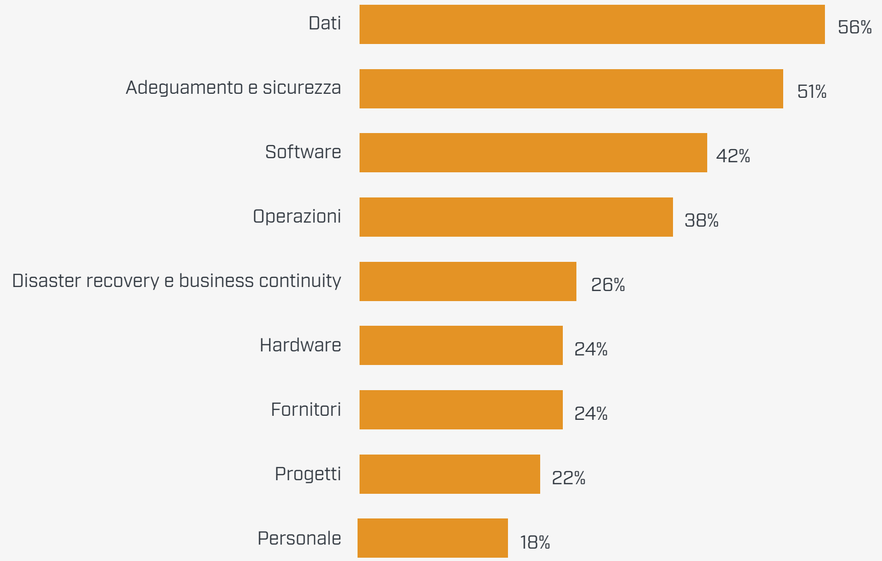
Una convergenza di eventi sta portando le aziende a prendere almeno in considerazione un'architettura Zero Trust. Al primo posto c'è l'esigenza di gestire i rischi per una moltitudine di risorse proteggendole da numerose minacce. Gli intervistati hanno attribuito un anno di incidenti della sicurezza a diverse cause e principalmente a vulnerabilità della sicurezza di persone o aziende di terze parti. Altre cause includono:

- Rischi aziendali imprevisti
- Configurazione errata di servizi o sistemi
- Attacchi interni intenzionali dannosi
- Errori di utenti non malintenzionati, tra cui le vittime di phishing
- Identità compromesse
- Software senza patch
- Credenziali rubate

Questi incidenti determinano una varietà di rischi, principalmente per i dati.

Per molte aziende, l'improvviso passaggio al lavoro da remoto richiesto dalla pandemia ha accelerato i piani di adozione di Zero Trust, mentre i modelli di sicurezza basati sul perimetro diventavano obsoleti. Molte aziende andavano già verso quella direzione, con il trasferimento di altre applicazioni e dell'infrastruttura IT al cloud, ma la pandemia ha fornito una scossa supplementare.

Principali categorie a rischio in tema di minacce alla sicurezza informatica



Fonte: Zero Trust Adoption Survey, marzo 2022, Foundry. Base: 250

CSO Microsoft Security

Ad esempio, il CISO di un'azienda di tecnologie medicali con 1.700 dipendenti afferma che il cloud e la pandemia sono stati fattori chiave per la sua adozione di Zero Trust, che ora offre una base sicura per qualsiasi modello di ambiente di lavoro riservi il futuro.

"I fattori chiave aziendali sono stati la nostra identità di azienda basata sul cloud e l'esigenza di proteggere il nostro ambiente", afferma. "Dovevamo inoltre fornire una forza lavoro da remoto efficiente durante la pandemia. [Zero Trust] ci ha consentito di ridurre drasticamente il nostro impatto immobiliare e probabilmente rimarremo almeno al 60% un'azienda virtuale remota".

CSO Microsoft Security

Le minacce non mancano

Le esigenze di adeguamento hanno anche prodotto una spinta verso modelli di sicurezza più solidi. "Gli enti di controllo ci osservano e si aspettano miglioramenti continui del nostro framework di sicurezza", afferma il vicepresidente senior della sicurezza informatica globale di una società di servizi finanziari con 290.000 dipendenti.

Alcune aziende hanno intrapreso azioni proattive verso il modello Zero Trust per evitare violazioni di alto profilo che le avrebbero poste al centro dell'attenzione per i motivi sbagliati. "Volevamo essere proattivi e cercare di non finire in prima pagina", afferma il CIO di un istituto di istruzione superiore con 3.500 dipendenti. "Ci sono orribili storie di altri istituti locali delle nostre dimensioni che hanno dovuto fermarsi per un lungo periodo".

Altri hanno già subito un grave incidente di sicurezza informatica che li ha indotti a rivedere velocemente la propria strategia di sicurezza. Dopo che una compagnia di assicurazioni con 6.000 dipendenti ha subito un attacco ransomware che ha determinato la chiusura delle rete aziendale per due settimane, l'ordine di adottare Zero Trust è arrivato direttamente dal CEO. "Abbiamo fortemente velocizzato l'implementazione", afferma il vicepresidente dello sviluppo IT dell'azienda. "All'inizio si trattava solo di procedure consigliate, ma dopo l'attacco ransomware tutto è stato decisamente accelerato".

Un catalizzatore basato sul cloud

Il VP e CISO di un'importante società di servizi finanziari afferma che il suo team ha ammesso la necessità di una nuova architettura di sicurezza diversi anni fa, quando l'azienda ha iniziato ad adottare un maggior numero di risorse basate sul cloud e gli utenti sono diventati più mobili.

"Ci siamo resi conto che la nostra architettura di sicurezza tradizionale era obsoleta e non ci avrebbe protetto dagli attacchi in futuro", afferma.

Questa realtà è diventata più che evidente all'inizio del 2020, quando la società ha scoperto che, nel corso dell'anno precedente, un utente malintenzionato aveva penetrato il suo perimetro e si era spostato lateralmente all'interno dell'ambiente senza essere rilevato. "Avevamo bisogno di una nuova architettura con cui proteggere e autenticare l'uso di quelle risorse ovunque risiedano e Zero Trust è un'architettura progettata a questo scopo".

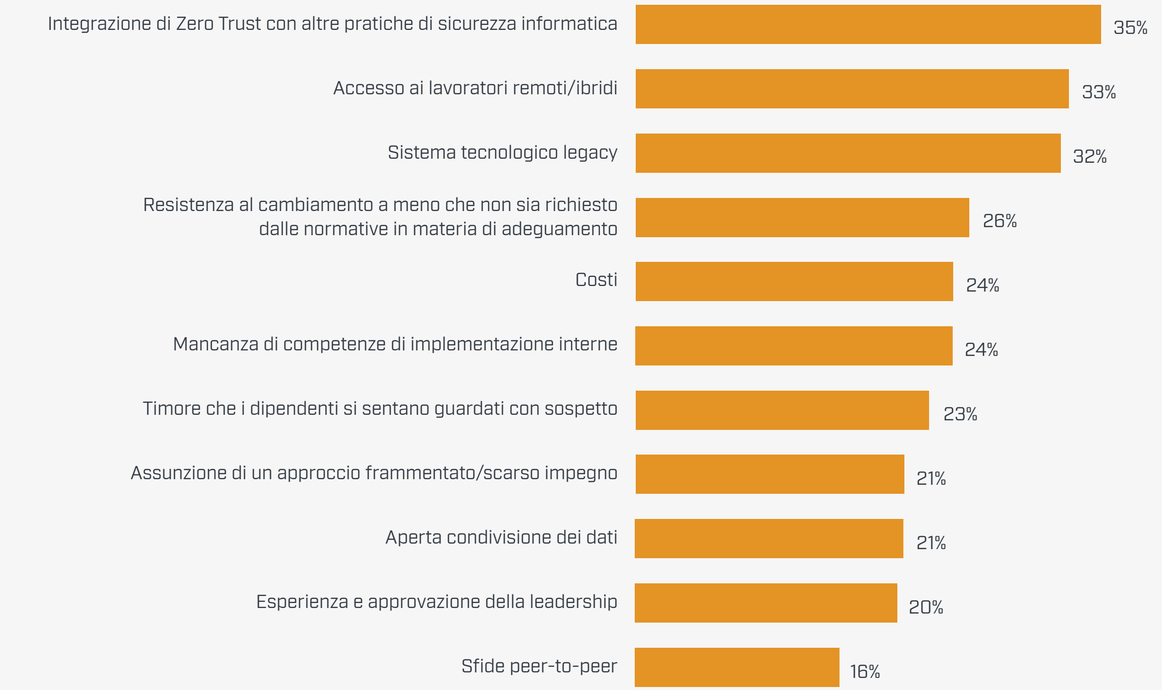
CSO Microsoft Security

Ostacoli all'adozione di Zero Trust

Per molte aziende, il modello Zero Trust rappresenta una svolta fondamentale nella struttura, nei processi e nella mentalità associati alla sicurezza e questo spiega alcuni degli ostacoli che è necessario superare prima di adottarlo.

"All'interno dell'azienda abbiamo dovuto affrontare molti comparti isolati diversi", afferma il CISO del call center, spiegando che i team dei server, della rete e dei database avevano il proprio contingente di strumenti e server Web. "Questo ci ha creato seri problemi perché ognuno aveva un'idea diversa sulle scelte da fare e su come procedere".

Cosa ostacola l'adozione di Zero Trust?



Fonte: Zero Trust Adoption Survey, marzo 2022, Foundry. Base: 250

CSO Microsoft Security

Portare alla luce questi problemi può in realtà essere un effetto collaterale positivo di Zero Trust, secondo Anthony Mocny, Senior Product Marketing Manager per Zero Trust in Microsoft. "Come architettura, Zero Trust è progettata per eliminare l'isolamento dei team di sicurezza presenti all'interno dei pilastri tecnologici e aiutare i team a collaborare in sinergia", afferma. "Questo può comportare anche un cambiamento culturale, in termini di modalità di collaborazione dei team".

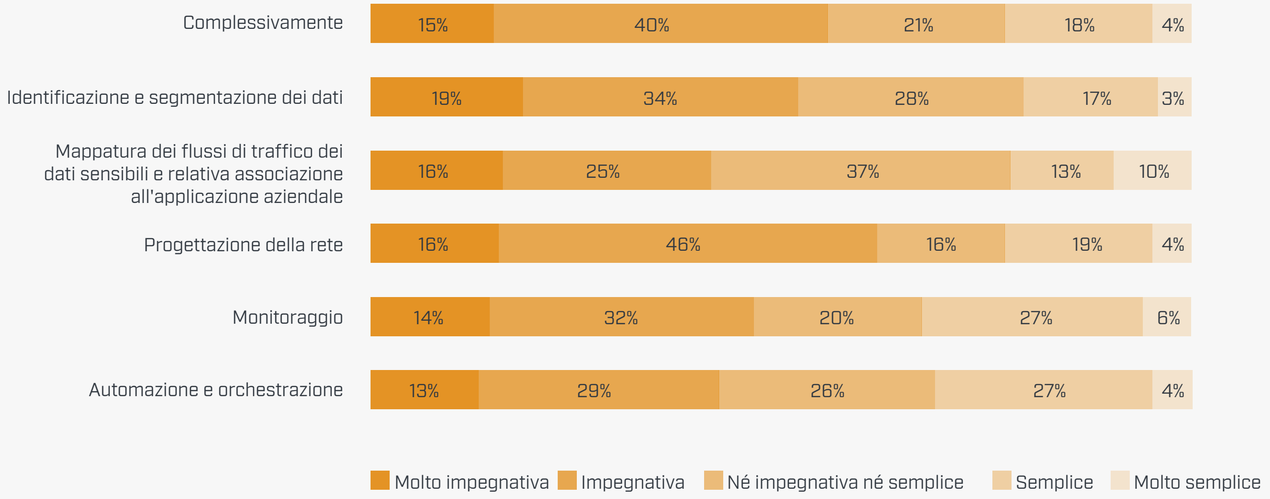
Per il VP/CISO dei servizi finanziari, le applicazioni legacy erano un ostacolo da superare nel percorso verso Zero Trust. "Devono essere aggiornate con tecnologia di autenticazione moderna", afferma. "E questa non è un'operazione molto facile da fare, dipende da quanto sono vecchie".

CSO Microsoft Security

Sfide di distribuzione

Una volta intrapreso un percorso Zero Trust, è possibile che emerga una varietà di sfide di implementazione. Oltre la metà degli intervistati (56%) ha ammesso che l'implementazione di Zero Trust è stata impegnativa o molto impegnativa. In particolare:

Quanto è impegnativa l'implementazione di Zero Trust?



Fonte: Zero Trust Adoption Survey, marzo 2022, Foundry. Base: 168

CSO Microsoft Security

Difficoltà relative alla segmentazione e alla microsegmentazione sono emerse spesso nelle interviste approfondite.

"La rete viene segmentata fino al singolo host", afferma il VP/CISO dei servizi finanziari. "È come predisporre un piccolo firewall tra ogni singolo host sulla rete interna, in modo da poter vedere tutto il traffico e controllarlo fino al singolo computer. Questo comporta enormi vantaggi in termini di sicurezza, ma è difficilissimo da implementare perché ci si troverà essenzialmente a gestire decine di migliaia di firewall".

La mappatura dei flussi di traffico può essere un altro processo della durata di diversi mesi. Il CTO di una casa editrice multimediale con 5.000 dipendenti afferma che, dopo aver definito i servizi di dati, applicazioni e rete critici da proteggere, "l'azienda ha mappato i flussi di transazioni lungo la rete e ha cercato di considerarli come gruppi di informazioni.

"[Abbiamo poi] segmentato porzioni di queste informazioni e come queste attraversano la rete, anche fino ai singoli pacchetti di informazioni". A quel punto, l'azienda ha applicato i criteri Zero Trust a ciascun tipo di flusso di traffico. "Ci siamo inoltre basati su nuove funzionalità per monitorare e gestire la nostra rete".

Nonostante le difficoltà, molti intervistati ritengono che Zero Trust in fin dei conti semplifichi le operazioni quotidiane. Con le tecnologie tradizionali, "apportare modifiche richiede giorni: è necessario inviarle a tutti i componenti hardware e software e noi usiamo molte risorse per farlo", afferma il vicepresidente senior dei servizi finanziari per la sicurezza informatica globale. "Analizzando Zero Trust, invece, ci rendiamo conto che riduce veramente al minimo la complessità architetturale nel lungo periodo, nonché il numero di dipendenti che servono per fare lo stesso tipo di attività".

CSO Microsoft Security

Procedure consigliate per l'implementazione di Zero Trust

Le aziende che implementano un'architettura Zero Trust sono sempre più numerose e stanno sviluppando roadmap e procedure consigliate utili per altre aziende. Ecco cinque considerazioni utili in fase di pianificazione di una distribuzione.

Inizia con un passo alla volta

La mappatura di una strategia Zero Trust può intimorire se la si vede solo nell'ampio contesto di dover rivedere criteri e protezioni di reti, dati, applicazioni, identità, endpoint e infrastruttura. "All'inizio guardavamo a questa enorme montagna da scalare e ci chiedevamo se davvero l'avremmo fatto", afferma il CIO dell'istituto di istruzione superiore. "Occorre fare un passo alla volta".

Il CIO e il suo team hanno infine adottato un approccio basato sull'aspetto finanziario, dando la priorità alla segmentazione delle applicazioni finanziarie e per buste paga e stipendi su una rete separata.

Identificare le risorse più critiche da proteggere è un buon approccio, secondo Mocny. "Prima di tutto, presta attenzione al motivo per cui stai implementando Zero Trust", afferma.

Nel dubbio, inizia con l'autenticazione a più fattori

Quando definiscono le priorità dello stack di sicurezza, molti CISO e fornitori di servizi di sicurezza consigliano di concentrarsi inizialmente sull'autenticazione e su altre protezioni basate sull'identità. "Se non hai in mente un punto di partenza, l'autenticazione a più fattori è un'ottima scelta", afferma Mocny.

Microsoft stima che l'autenticazione a più fattori può evitare più del 90% degli attacchi basati sull'identità.

Il VP/CISO dei servizi finanziari concorda. "L'autenticazione è un elemento fondamentale dell'implementazione dell'architettura Zero Trust. Nessuno degli altri componenti funziona se non puoi convalidare l'identità dell'utente finale, quindi abbiamo iniziato da lì".

Poi, il VP/CISO dei servizi finanziari si è dedicato al componente di rete, ottenendo vantaggi immediati per il supporto del personale remoto. Il team ha lasciato la microsegmentazione alla parte finale del percorso, in quanto non immediatamente visibile all'azienda nel suo complesso. "Una volta completata, sei decisamente più protetto, ma nessuno percepisce la differenza", afferma.

CSO Microsoft Security

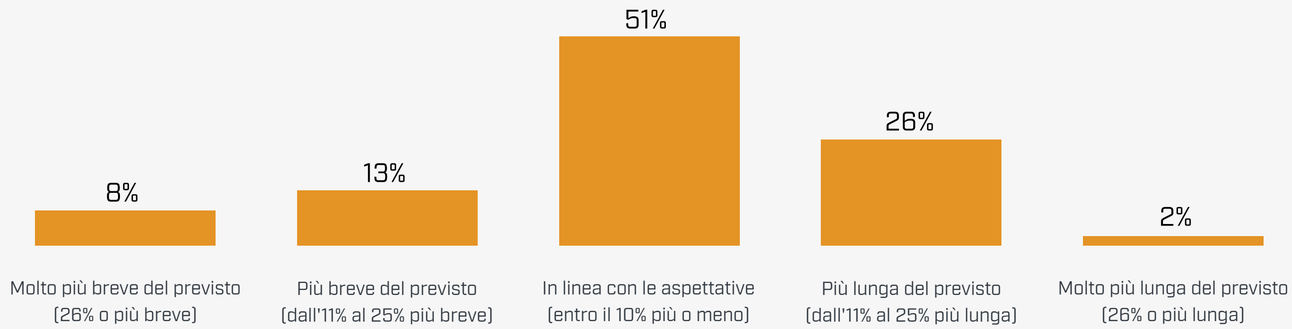
Sii realistico sui tempi

È importante che i CISO definiscano aspettative realistiche per le distribuzioni Zero Trust. "L'implementazione di un'architettura Zero Trust è un programma, non un progetto", afferma il VP/CISO dei servizi finanziari. "Questo è stato un enorme cambiamento. Un'implementazione corretta comporta numerosi progetti e probabilmente andrà avanti per anni. Un'implementazione facile e veloce dell'architettura Zero Trust non esiste".

Il suo collega, vicepresidente senior dei servizi finanziari, concorda. "Non credo che finiremo mai perché ci saranno sempre nuove tecnologie, nuovo malware e nuove minacce in arrivo", afferma.

La maggioranza degli intervistati (72%) afferma che i tempi delle distribuzioni hanno rispettato la tabella di marcia o erano in anticipo rispetto a quanto pianificato, con il resto degli intervistati che afferma che l'implementazione ha richiesto più del tempo previsto.

Zero Trust soddisfa i tuoi obiettivi temporali?



Fonte: Zero Trust Adoption Survey, marzo 2022, Foundry. Base: 168

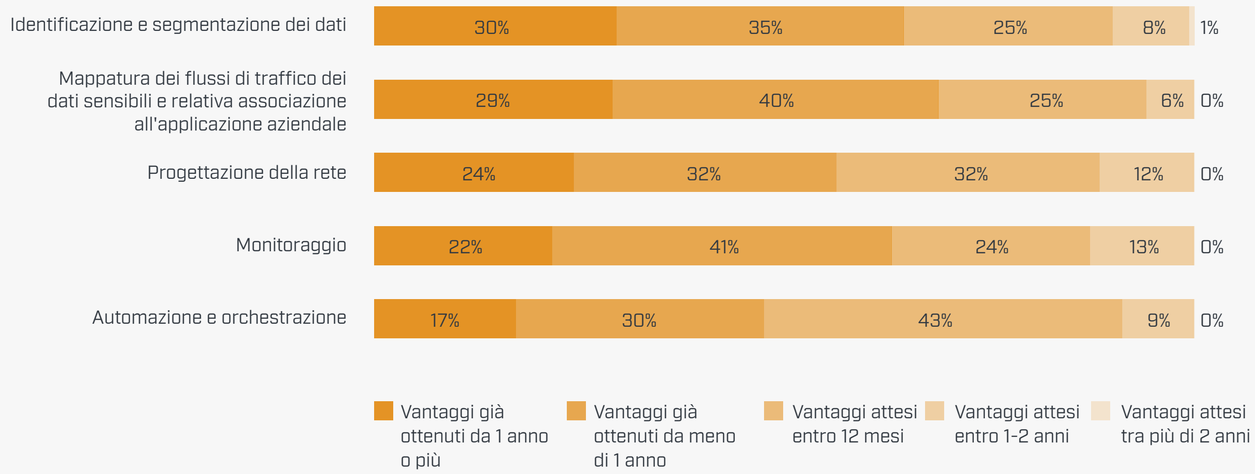
CSO Microsoft Security

Misura i progressi

Anche se una distribuzione Zero Trust è un'attività continua, i CISO possono e devono creare tappe intermedie lungo il percorso al fine di misurare i progressi. È un buon segno che circa i due terzi degli intervistati affermino di aver ottenuto vantaggi dalla maggior parte degli aspetti dei propri progetti entro un anno e che circa un quarto o più si aspetti di ottenerli entro 12 mesi in relazione ad attività importanti quali l'identificazione e la segmentazione dei dati, la mappatura dei flussi di traffico e la progettazione della rete.

"La necessità di una valutazione continua per difendersi dalla natura mutevole degli attacchi fa di Zero Trust un percorso", afferma Mocny. "Presta sempre attenzione e apporta miglioramenti."

Tempi per ottenere i vantaggi di Zero Trust



Fonte: Zero Trust Adoption Survey, marzo 2022, Foundry. Base: 103

CSO Microsoft Security

Concentrati sulle persone, non solo sulla tecnologia

Per la sua ampia portata, un modello di sicurezza Zero Trust interessa tutti i dipendenti, inclusi i team IT e di sicurezza che hanno il compito di distribuirlo. Ecco perché, come per qualsiasi grande progetto tecnologico, è importante assicurarsi che le distribuzioni siano in sincronia con i nuovi processi e le pratiche di gestione del cambiamento per garantire un'implementazione fluida e di successo.

"Oltre a un cambiamento tecnologico, c'è un cambiamento culturale", afferma Mocny. "Se ci sono più team che si occupano della sicurezza, composti da architetti di rete o esperti di identità, sarà necessario cambiare anche il modo in cui questi team collaborano. È necessario evitare l'isolamento tra i team per assicurarsi che tutto funzioni in sinergia".

L'eliminazione dell'isolamento implica il diretto coinvolgimento dei team di tutte queste discipline in progetti pilota e di modello di verifica. Un direttore dei sistemi IT di una società di telecomunicazioni con circa 2.000 dipendenti ha imparato questa lezione dopo aver combattuto con diversi singoli punti di errore durante la distribuzione, tra cui servizi che non consentivano l'autenticazione e risultavano improvvisamente "non attendibili", diventando non disponibili, così come alcuni sistemi.

"La distribuzione di un servizio può determinare un effetto domino e interromperne altri", afferma. In futuro, "saremo molto più attenti: più tempo per il modello di verifica, più revisioni e più verifiche dell'architettura con esperti in materia prima della distribuzione".

ROI di Zero Trust

Uno **studio commissionato Total Economic Impact™ di Forrester Consulting** del 2021 quantifica il risparmio sui costi e i vantaggi aziendali delle soluzioni Microsoft Zero Trust. In base alle cinque imprese intervistate da Forrester, un'azienda composita ha realizzato un ritorno sull'investimento del 92% in tre anni grazie all'implementazione di un'architettura Zero Trust con Microsoft.

Questa azienda composita ha inoltre risparmiato una media di 20 USD per dipendente al mese eliminando la necessità di strumenti di sicurezza diventati ridondanti nel modello Zero Trust, tra cui soluzioni di gestione degli endpoint, antivirus e antimalware.

CSO Microsoft Security

Dove ti trovi nel percorso verso il modello Zero Trust?

Come indica il sondaggio, i vantaggi di un modello di sicurezza Zero Trust superano chiaramente alcune delle sfide di distribuzione affrontate dai CISO e dai loro team di sicurezza. Affrontare queste sfide con un piano ben congegnato può aiutare la tua azienda a migliorare velocemente le protezioni, ridurre il rischio e iniziare a offrire valore all'intero business.

Per valutare il livello di maturità Zero Trust della tua azienda e scoprire altre pratiche risorse per la distribuzione, inizia la **valutazione del modello di maturità Zero Trust** di Microsoft.