Rubrik Zero Labs

LA CRISI DELLE IDENTITÀ

COMPRENDERE E SVILUPPARE LA RESILIENZA CONTRO LE MINACCE BASATE SULL'IDENTITÀ

INDICE

EXECUTIVE SUMMARY

Rubrik Zero Labs e Wakefield Research hanno di recente intervistato 1.625 responsabili IT e della sicurezza in tutto il mondo per valutare la loro capacità di difesa e di recupero dagli attacchi basati sull'identità. A questo vanno aggiunte oltre 2,2 milioni di snapshot che Rubrik analizza ogni giorno alla ricerca di minacce annidate nei dati di backup.

Con la scomparsa dei tradizionali confini di rete dovuta alla migrazione al cloud, all'adozione del lavoro da remoto e ora all'AI agentica, l'identità non rappresenta più solo un livello di controllo. È diventata la principale superficie d'attacco, sfruttata dagli attori delle minacce per accedere agli ambienti IT e "per agire dall'interno" durante l'attacco. La stragrande maggioranza delle violazioni odierne si basa sull'abuso della fiducia e di credenziali valide, più che sull'elusione delle difese di rete.

Considerato che quasi ogni attacco coinvolge un'identità, umana o non, sia per ottenere l'accesso iniziale che per l'escalation dei privilegi e per il movimento laterale, non sorprende che la grande maggioranza delle persone intervistate (90%) concordi sul fatto che gli attacchi basati sull'identità rappresentano la minaccia più grave per la propria organizzazione.

Questo report ha l'obiettivo di quantificare la capacità delle organizzazioni di resistere agli attacchi basati sull'identità, evidenziando le aree più critiche e le tempistiche previste per la risposta.

Infine, esplora gli elementi fondamentali per la resilienza dell'identità, tra cui:

- L'integrazione di visibilità, capacità di risposta e recovery in tempo reale su tutti i provider di identità, on-premise e cloud, per identità sia umane che non umane
- Lo sviluppo di una forte fiducia nella capacità dell'organizzazione di ripristinare rapidamente e con affidabilità l'infrastruttura di identità centrale a uno stato precedente all'infezione
- L'adozione di pratiche di rafforzamento dell'identità e costruzione della resilienza basate sui principi Zero Trust, per ridurre la superficie d'attacco e l'impatto di una compromissione
- L'integrazione della resilienza dell'identità nella pianificazione generale del ciclo di vita della cyber resilience

Un approccio realmente olistico è l'unico che consente alle organizzazioni di rafforzare l'infrastruttura di identità ed evitare potenziali interruzioni, perdite di fatturato o danni reputazionali.

Prima di iniziare, diamo uno sguardo all'andamento anno su anno emerso dal nostro sondaggio precedente.

2024 VS. 2025 TENDENZE DEL SONDAGGIO

(Wakefield)

90%
ha subito un attacco informatico nell'ultimo anno

La stessa percentuale che aveva dichiarato almeno un attacco anche nel 2024

89%
di chi ha subito un attacco ransomware ha pagato per recuperare i dati o fermare l'attacco

20%
ha riferito di aver subito più di 25 attacchi contro il 18% del 2024

L'11% ne ha subiti 100 o più, un leggero aumento rispetto all'8% del 2024

LA FIDUCIA NEI TEMPI DI RECOVERY È IN CALO

Nel 2025, solo il 28% ritiene di poter completare il recovery da un attacco informatico in 12 ore o meno, rispetto al 43% nel 2024

77%
ha dichiarato di gestire un ambiente cloud più ampio rispetto all'anno precedente

58%
ritiene che l'AI agentica sarà la causa della metà o più degli attacchi informatici nel prossimo anno

58%
ritiene che ci vorranno 2 giorni o più per ripristinare completamente i servizi dopo un attacco

VIOLAZIONE DELL'IDENTITÀ:

IL LASCIAPASSARE DEI CYBERCRIMINALI PER AGIRE DALL'INTERNO

La maggior parte degli incidenti informatici moderni include in qualche misura la compromissione dell'identità. Tuttavia, le identità vanno considerate come strumenti, più che obiettivi in sé. Oggi sono più spesso il mezzo attraverso cui un attore delle minacce persegue il suo obiettivo, come sorveglianza, furto di dati o estorsione, e non come il fine ultimo.

86%

degli attacchi a semplici applicazioni web oggi sfrutta credenziali rubate

(Verizon)[1]

79%

dei rilevamenti CrowdStrike erano “senza malware”, ovvero gli aggressori accedevano ai sistemi senza distribuire malware tradizionali

(Crowdstrike 2025)[2]

4,67

MILIONI (USD)

per violazione

È il costo medio quando gli aggressori sfruttano credenziali compromesse

(IBM)[3]

In quanto vettore d'attacco, la compromissione dell'identità consente agli attori delle minacce di:

"Agire dall'interno", eludendo il rilevamento grazie all'abuso di processi legittimi come strumenti di amministrazione, servizi SaaS o persino i workflow di identità

Condurre ulteriori attacchi utilizzando credenziali compromesse in precedenza

Mantenere una presenza persistente negli ambienti compromessi, anche creando "piattaforme d'identità ombra", tenant o infrastrutture d'identità al di fuori della governance e della visibilità dell'organizzazione

[1] https://www.verizon.com/business/resources/reports/dbir/
[2] https://www.crowdstrike.com/en-us/resources/reports/global-threat-report-executive-summary-2025/
[3] https://www.ibm.com/reports/data-breach

Le identità umane non sono gli unici bersagli delle compromissioni. Anche le identità non umane (non-human identities, NHI) sono sotto attacco. Si tratta comunemente di token API utilizzati per autenticare processi IT automatizzati, certificati, container, strumenti di automazione, account di servizio e agenti di AI.

Secondo alcune stime, oggi le NHI superano gli utenti umani con un rapporto di 82 a 1.[4] Questo aumenta in modo notevole la superficie d'attacco per gli attori delle minacce, e continuerà a crescere con la diffusione dell'AI agentica.

Gli attori delle minacce prendono di mira identità umane e NHI per ragioni diverse, a seconda dei loro obiettivi. Capire quali identità vengono prese di mira e per quali scopi è fondamentale per difendere ogni categoria:

	Identità umane (Accessi dipendenti, credenziali amministrative, ecc.)	**Identità non umane** (Account di servizio, chiavi API, token, ecc.)
Obiettivo principale	Accesso iniziale, ricognizione e utilizzo dei privilegi dell'utente	Stealth, persistenza e accesso a livello di sistema
Rischio principale	Vulnerabilità all'ingegneria sociale	Rischio di configurazioni errate, tendenza a proliferare rapidamente
Evasione delle difese	Più difficile da mantenere: gli account umani sono di solito protetti da MFA, criteri di accesso e analisi comportamentale (es. viaggi impossibili)	Più facile da mantenere: le identità non umane spesso non sono protette da MFA, hanno meno controlli e le loro attività automatizzate si confondono facilmente nel traffico legittimo
Privilegi	Solitamente legati a un ruolo specifico, come ingegnere o commerciale	Spesso sistemici ed eccessivi, ad esempio un account di servizio che può accedere a tutti i database
Persistenza	Facile da revocare: un account umano può essere bloccato, la password modificata, la sessione terminata in pochi minuti durante un incidente	Difficile da revocare: le identità non umane possono essere longeve, dimenticate o essenziali per operazioni critiche, rendendo la rotazione difficile e rischiosa

[4] https://www.cyberark.com/resources/white-papers/2025-identity-security-landscape-executive-summary

L'OSSESSIONE DEGLI ATTORI DELLE MINACCE PER LE IDENTITÀ

Le identità, umane e non, sono state al centro di una serie di recenti incidenti di cybersecurity di alto profilo.

Entra ID e n0Auth utilizzati per il movimento laterale

Nel giugno 2025, Entra ID, il servizio IAM cloud-based di Microsoft, è stato trovato ancora vulnerabile a un difetto che consentirebbe agli attori delle minacce di spostarsi da alcune applicazioni SaaS compromesse verso le risorse centrali di Microsoft 365 di un'organizzazione, ottenendo così accesso ai dati aziendali sensibili.[5]

Manipolando un singolo attributo della mail per farlo coincidere con l'indirizzo della vittima, un utente poteva accedere sfruttando la funzione "Accedi con Microsoft" di un'applicazione SaaS vulnerabile. Questo tipo di attacco, che prende di mira la logica di attestazione dell'identità di un'applicazione, permette un movimento laterale rapido e un accesso illimitato agli strumenti principali di produttività aziendale, come SharePoint e Teams.

Sebbene il difetto fosse stato segnalato già nel 2023, si ritiene che ancora oggi interessi decine di migliaia di applicazioni SaaS. Poiché n0Auth richiede un intervento lato tenant, non è possibile applicare una correzione in modo centralizzato. In questo caso, la popolarità di Microsoft amplifica enormemente il raggio d'impatto di questa vulnerabilità a livello di identità applicativa. Gli attacchi contro Entra ID sono proseguiti nel 2025, spesso con lo scopo di ottenere l'escalation dei privilegi.

Attacchi ToolShed contro server SharePoint on-premise

Le vulnerabilità critiche sfruttate negli attacchi ToolShed del luglio 2025 mostrano in che modo elementi dell'identità, come l'autenticazione tramite chiave, possano essere manipolati dagli attori delle minacce. In questo caso, hacker presumibilmente legati a stati nazionali hanno puntato al furto di machine key utilizzate per autenticare server SharePoint on-premise appartenenti a obiettivi di alto valore, probabilmente per avviare campagne di spionaggio prolungate all'interno degli ambienti compromessi.[6]

Questo dimostra quanto le NHI siano importanti per gli attori delle minacce più motivati, che mirano a condurre attacchi prolungati per finalità come lo spionaggio. Poiché le chiavi hanno una durata più lunga rispetto ai token, è fondamentale che i team di sicurezza diano priorità alla loro rotazione immediata in seguito a un incidente o alla scoperta di una CVE come quella sfruttata negli attacchi ToolShed.

Scattered Spider sfrutta la natura umana

Gli appartenenti al gruppo Scattered Spider fingono spesso di essere personale IT o dell'help desk per convincere le persone a fornire credenziali o ad aggirare l'autenticazione a più fattori (MFA). Il successo del gruppo si basa fondamentalmente sulle debolezze della psicologia umana, in particolare sulla disponibilità ed empatia dei team di supporto, spesso sotto pressione per risolvere i problemi in fretta. Pare che ad agosto 2023 il gruppo sia riuscito a causare alla multinazionale Clorox danni per 380 milioni di dollari, semplicemente chiamando l'help desk esterno dell'azienda e richiedendo il reset di una password.[7]

Il successo di Scattered Spider non dipende dalla scoperta di vulnerabilità zero-day nei software, ma dall'accesso iniziale ottenuto tramite ingegneria sociale, seguito dall'abuso di strumenti nativi come PowerShell e servizi SaaS. Questo significa che le soluzioni tecniche, da sole, non bastano a garantire la protezione. Le organizzazioni devono invece investire in una sicurezza centrata sulle persone, che includa formazione continua e adattiva sulla consapevolezza della sicurezza, oltre a una maggiore resilienza dell'infrastruttura identitaria

[5] https://www.infosecurity-magazine.com/news/microsoft-noauth-flaw-2025/
[6] https://www.recordedfuture.com/blog/toolshell-exploit-chain-thousands-sharepoint-servers-risk
[7] https://www.cybersecuritydive.com/news/clorox-380-million-suit-cognizant-cyberattack/753837/

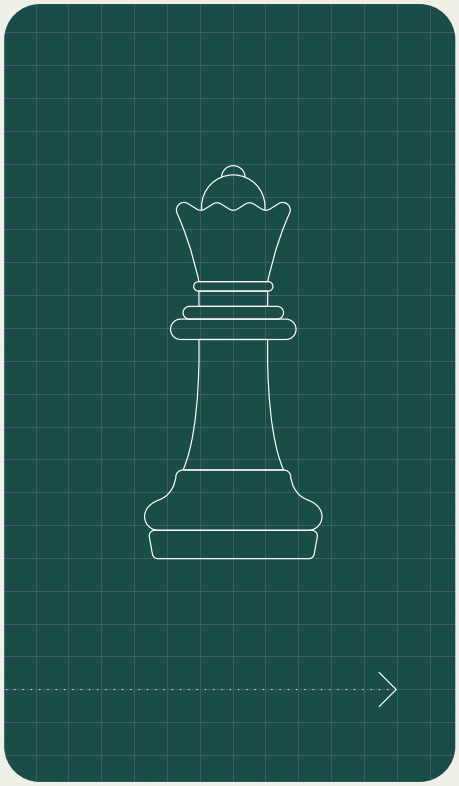
CONSEGUENZE DELLE VIOLAZIONI BASATE SULL'IDENTITÀ

Compromettere un'identità equivale a ottenere le "chiavi del regno": consente ai cybercriminali di agire dall'interno, usando strumenti legittimi per fare sorveglianza ed esfiltrare dati.

Basta osservare i danni provocati anche da una sola compromissione andata a segno per capire perché l'identità sia diventata una priorità crescente:

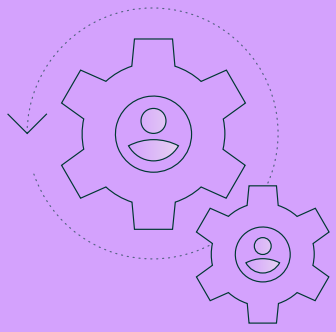
Categoria di impatto	Conseguenza	Asset organizzativi coinvolti
Violazione dei dati	Esfiltrazione di PII, proprietà intellettuale, dati finanziari o altri dati sensibili	Dati dei clienti, dati dei dipendenti, segreti industriali, vantaggi competitivi, registri finanziari
Perdita finanziaria	Frodi dirette, costi di risposta all'incidente, spese legali, sanzioni normative	Budget, entrate, risorse legali
Danno reputazionale	Perdita di fiducia dei clienti, erosione del brand, pubblicità negativa	Valore del marchio, relazioni con clienti e partner, valore di mercato
Interruzione operativa	Downtime dei sistemi, interruzione dei servizi, blocco degli account	Entrate, investimenti nell'infrastruttura IT, controlli di sicurezza
Persistenza ed escalation dei privilegi	Installazione di backdoor (service principal, modifiche alla federazione), creazione di piattaforme di identità ombra	Infrastruttura IT, gestione di identità e accessi, controlli di sicurezza
Rischio legale e di compliance	Non conformità alle normative sulla privacy dei dati (GDPR, CCPA), azioni legali	Risorse legali, ufficio compliance
Compromissione della supply chain	Violazione di partner commerciali e altri soggetti terzi, con attacchi a catena	Ecosistema dei partner, integrità della supply chain, reputazione

COME STANNO REAGENDO LE ORGANIZZAZIONI?



90%

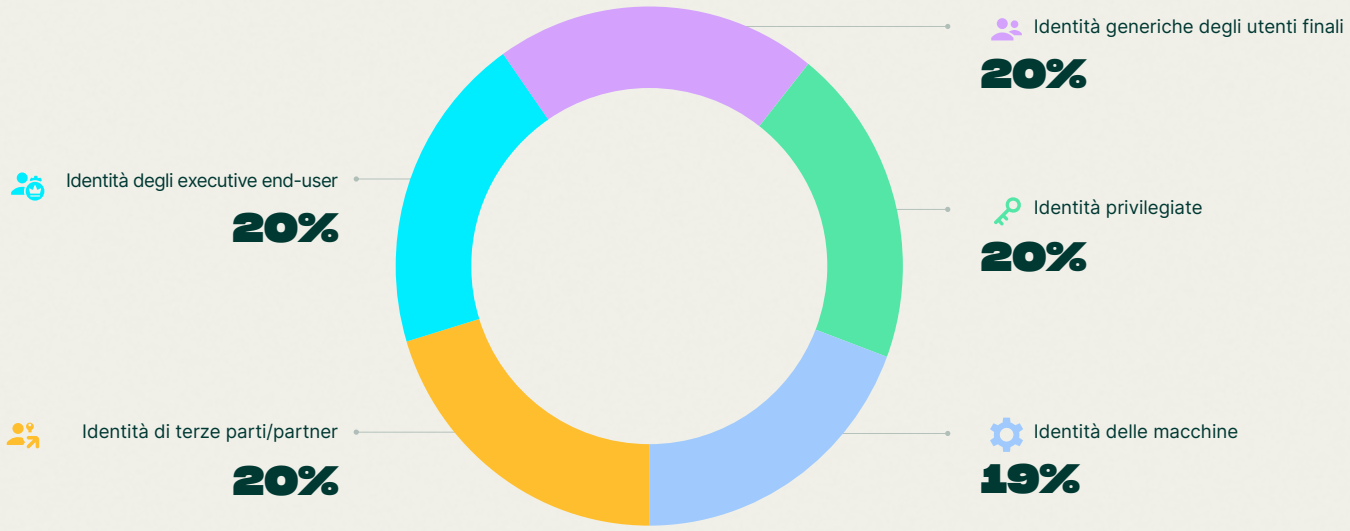
dei leader IT e della sicurezza intervistati concorda sul fatto che gli attacchi informatici basati sull'identità rappresentano la minaccia principale per la propria organizzazione.



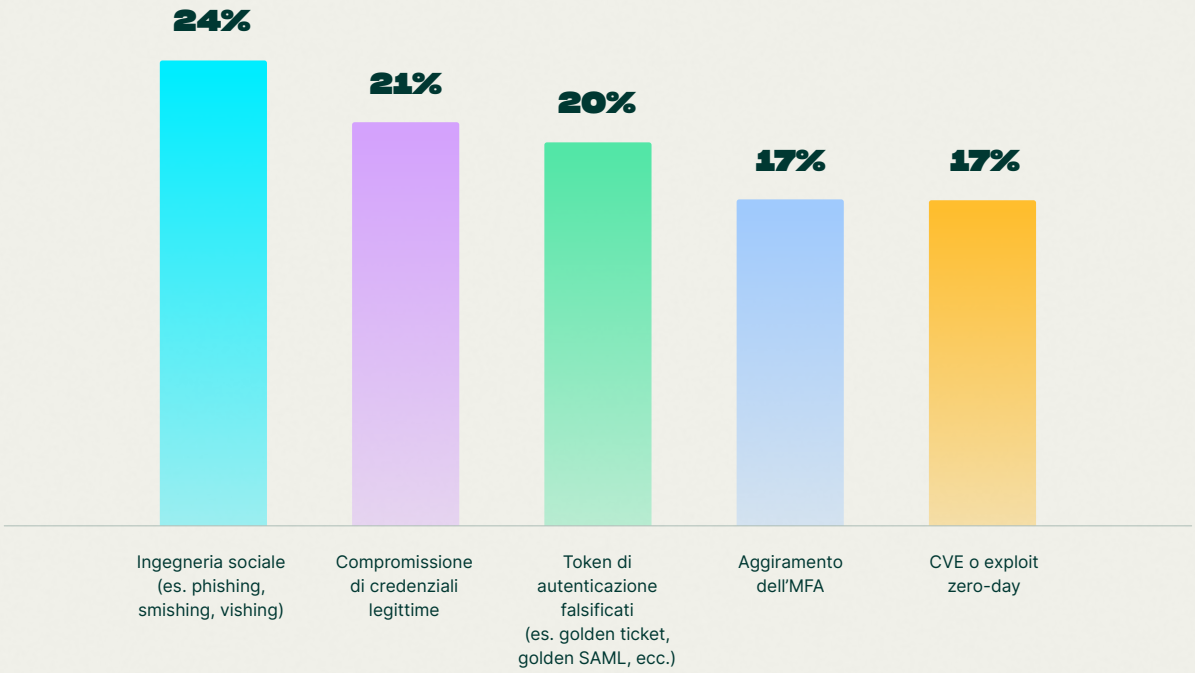
89%

prevede di assumere professionisti dedicati alla gestione o al miglioramento della gestione dell'identità digitale, dell'infrastruttura identitaria e/o della sicurezza delle identità nei prossimi 12 mesi.

Quali tipi di identità preoccupano di più in caso di compromissione?



Se in passato i leader si concentravano solo sugli account privilegiati, oggi c'è un chiaro consenso: ogni identità è critica. Si riconosce che qualsiasi account compromesso, indipendentemente dai permessi iniziali, rappresenta un punto d'appoggio pericoloso a favore di un aggressore, che può così avviare movimento laterale ed escalation dei privilegi.



I dati indicano anche un cambiamento di priorità in materia di sicurezza. Anche se l'ingegneria sociale rimane in testa (24%), l'aggiramento della MFA (17%) e i token di autenticazione falsificati (20%) sono oggi considerati pericolosi quanto gli exploit zero-day (17%).

Si tratta di un cambiamento importante. Dimostra che i leader hanno preso coscienza di una nuova realtà: oggi l'attacco tramite "accesso" basato su sofisticate tecniche di falsificazione dell'identità è una minaccia più diffusa rispetto al classico "sfondamento" delle difese.

Mandiant ha segnalato che nel 2024 si è registrato un numero record di incidenti nel cloud,[8] attribuendo il fenomeno soprattutto a soluzioni di gestione delle identità prive di adeguati controlli di sicurezza. Ora che l'identità sta diventando un vettore d'attacco, le soluzioni IAM (Identity and Access Management) faticano a stare al passo con le tecniche più recenti.

Probabilmente perché:

L'identità è un ambito complesso

Il privilegio degli accessi (PAM), i controlli di accesso basati sui ruoli (RBAC) e la sicurezza delle API sono tutte sotto-discipline dell'IAM, spesso fornite da vendor diversi, e questo amplia la superficie d'attacco.

Continuano a emergere nuovi tipi di identità

I bot e gli agenti AI sono varianti di NHI che non esistevano fino a cinque anni fa, e oggi le API vengono utilizzate in un numero crescente di casi d'uso. Gli agenti daranno origine a un'esplosione del volume di identità macchina-macchina, che spesso non dispongono di un ciclo di vita maturo (es. provisioning, rotazione, deprovisioning) come avviene per gli account umani.

Il modo in cui gli attori delle minacce sfruttano l'identità è in continua evoluzione

Le difese perimetrali e degli endpoint sono sempre più efficaci, e gli attori delle minacce danno sempre più priorità al furto di credenziali per "accedere con un login, non con un attacco".

Il cloud introduce nuovi rischi

La complessità e la granularità dei sistemi IAM nativi del cloud li rendono altamente vulnerabili a errori umani e configurazioni errate. Gli aggressori cercano attivamente queste configurazioni errate, come ruoli con privilegi eccessivi o autorizzazioni pubbliche assegnate per errore.

[8] https://services.google.com/fh/files/misc/m-trends-2025-en.pdf

Non sorprende quindi che:

87%

dei responsabili IT e della sicurezza sta pianificando di cambiare fornitore IAM o ha già avviato il processo.

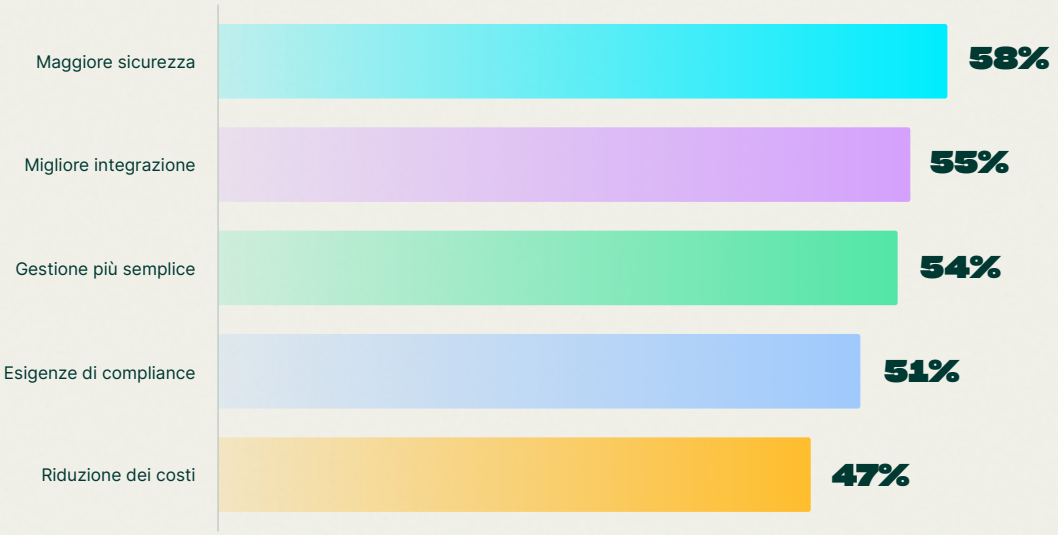
58%

lo fa per motivi di sicurezza, segno che molte soluzioni singole non offrono funzionalità adeguate per contrastare le minacce basate sull'identità.

60%

E questo nonostante il fatto che il 60% abbia già cambiato fornitore IAM negli ultimi tre anni.

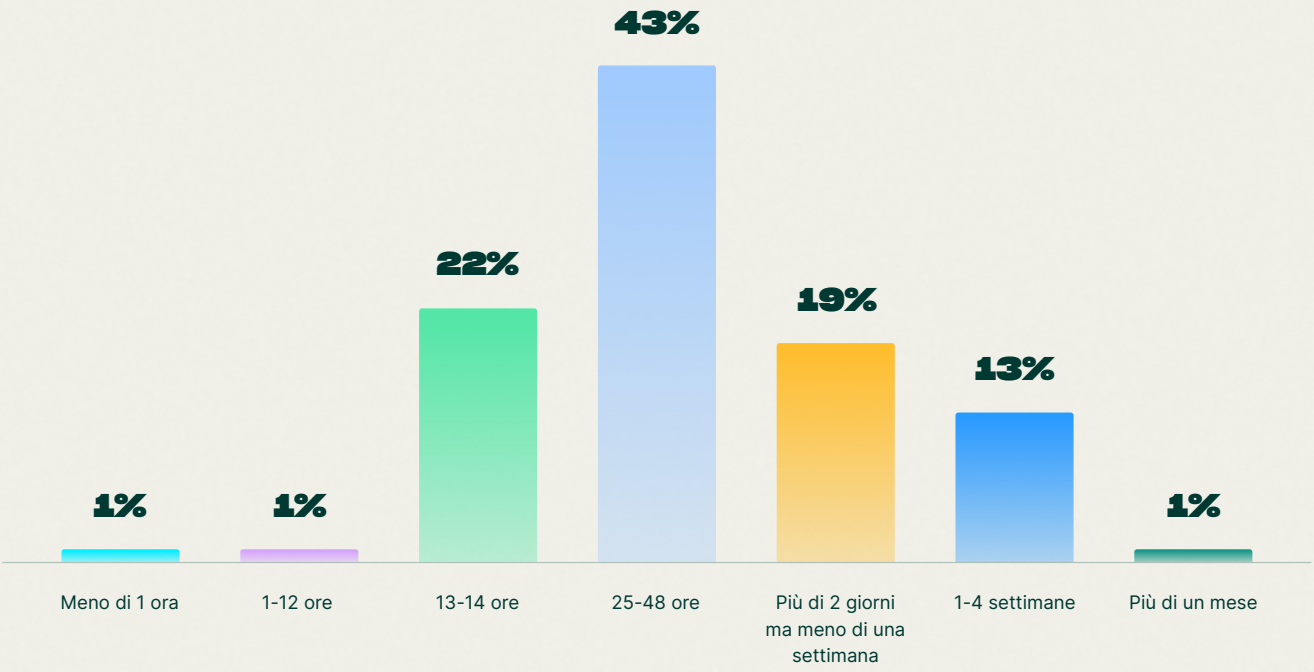
Motivi principali per cambiare provider di identità:



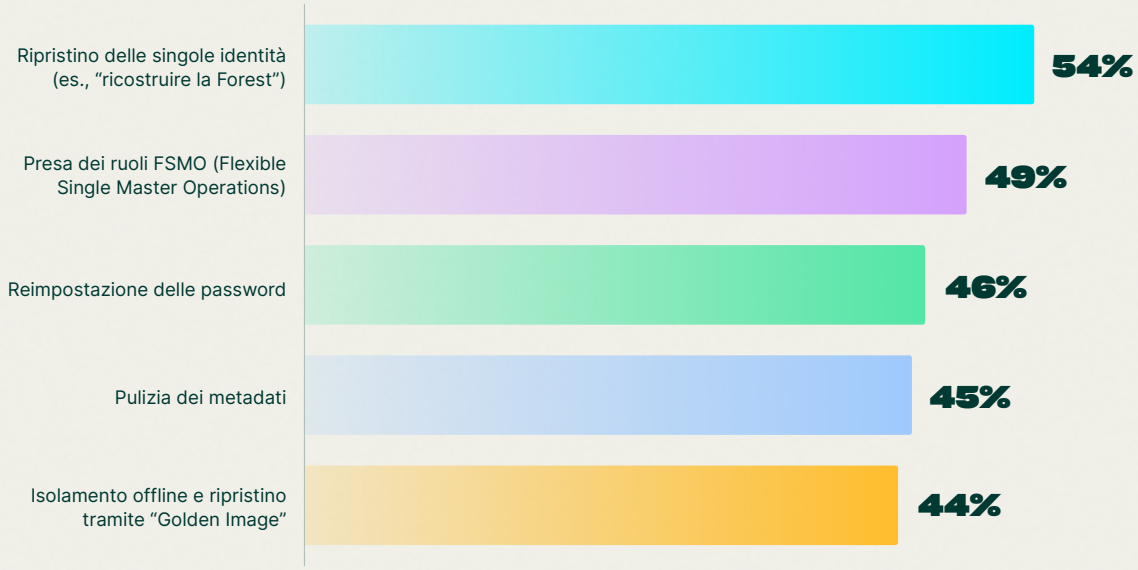
Ancora più preoccupante è il tempo di cui la maggior parte delle aziende ha bisogno per ripristinare la propria infrastruttura identitaria dopo una compromissione. Con il costo di un downtime che può arrivare a $ 6.000 al minuto,[9] le organizzazioni si trovano rapidamente ad affrontare spese crescenti se si affidano a processi di recovery manuali (54%).

[9] https://www.isaca.org/resources/news-and-trends/industry-news/2024/centralized-services-and-their-impact-on-business-continuity

Tempo dichiarato per ripristinare l'infrastruttura dell'identità dopo una compromissione:



Processi che richiedono procedure di recovery manuale:



È interessante notare che l'89% degli intervistati ha integrato agenti AI in modo completo o parziale all'interno della propria infrastruttura delle identità. Per impedirne l'utilizzo malevolo, anche queste nuove forme di identità non umane devono essere protette su vasta scala e lungo tutto il loro ciclo di vita. Già oggi, oltre la metà degli intervistati (58%) stima che entro il prossimo anno metà o più degli attacchi informatici sarà guidata da AI agentica.

Un altro elemento che ostacola la capacità delle organizzazioni di misurare e migliorare i tempi di risposta e ripristino è la scarsa comprensione di quali attori delle minacce prendano di mira quali identità, e per quale motivo.

PERCHÉ IL RECOVERY È COSÌ LUNGO?

MTTR COME METRICA BASATA SUI DATI

Molte organizzazioni puntano alla cyber resilience, ma faticano a quantificarla. Come possiamo misurare la capacità di anticipare, resistere, adattarsi e riprendersi dalle minacce informatiche?

L'obiettivo di tempo di ripristino (RTO) e l'obiettivo del punto di ripristino (RPO) sono misure tradizionali, ma non raccontano l'intera storia. Magari l'RTO previsto era di quattro ore, ma il ripristino effettivo ha richiesto 32 giorni. Un RPO misurato in minuti, in settori come quello bancario, può comunque tradursi nella perdita di dati relativi a centinaia di migliaia di transazioni. In questi esempi, sappiamo che i team di recovery hanno ampiamente superato gli obiettivi prefissati, ma non sappiamo perché.

Inoltre, il settore si affida spesso a metriche diverse, rendendo difficile una comprensione standardizzata dei tempi di ripristino tra i vari comparti. Per alcuni il cronometro si ferma quando la minaccia viene rilevata. Per altri solo quando è stata completamente eradicata. Questo rende difficile comprendere a fondo il livello di cyber resilience di un'organizzazione.

Ecco perché Rubrik Zero Labs consiglia di adottare il Mean Time to Recover (MTTR) come metrica standard di settore, basata su fasi e dati, per misurare la capacità di un'organizzazione di riprendersi da un incidente informatico.

IL NUOVO FRAMEWORK PER SCOMPORRE IL VALORE MTTR

L'MTTR non è una singola misurazione. È un processo articolato in più fasi distinte, pensato per fornire indicazioni utili e identificare le aree da migliorare. Questo modello di recovery include:

Rilevamento	È il punto di partenza di qualsiasi incidente, che sia un attacco informatico o una cancellazione accidentale.
Definizione dell'ambito (Scoping)	Questa fase prevede uno sforzo completo per comprendere tutti i sistemi e gli asset coinvolti, nonché le loro dipendenze. Capire quali applicazioni e database dipendono l'uno dall'altro è fondamentale.
Identificazione di un punto di ripristino pulito	È spesso la fase più lunga e critica. È il tempo necessario per individuare un backup affidabile e privo di malware da cui ripristinare le operazioni. In passato, ciò significava settimane o mesi di lavoro per configurare un laboratorio "clean room" dedicato. Gli strumenti moderni, come l'infrastruttura cloud e l'automazione, stanno riducendo sensibilmente questo tempo.
Ripristino	È la fase concreta in cui avviene il ripristino dei dati. Se questa fase richiede settimane, potrebbe indicare un problema di throughput, una motivazione basata sui dati per investire in infrastrutture volte a ridurre i tempi di recovery ad alto rischio. Visto l'attuale volume di dati posseduto dalle organizzazioni, questa fase potrebbe superare l'identificazione del punto di ripristino pulito come passaggio più lungo dell'intero processo.
Convalida	Quanto tempo serve per garantire la piena operatività delle applicazioni e l'accesso ai dati? Quanto tempo è necessario per assicurarsi che le identità umane e non umane funzionino e comunichino correttamente?

Misurando ogni fase singolarmente, un'organizzazione si allontana da un numero unico e privo di contesto, avvicinandosi invece a un livello di analisi granulare utile a identificare i colli di bottiglia e a prendere decisioni basate sui dati.

Metrica a fasi	Inizio conteggio	Fine conteggio	Descrizione
Mean-Time-to-Detect (MTTD)	Timestamp dell'impatto dell'attacco o momento dell'allarme	Alla conferma dell'ambito di recovery noto	Basato su rilevamento, analisi delle anomalie e correlazione dei dati SIEM
Mean-Time-to-Scope (MTTS)	Rilevamento convalidato	Elenco degli oggetti da ripristinare bloccato	Fase guidata da Ricerca globale, Classificazione dei dati e metadati degli SLA
Mean-Time-Select-Clean-Snapshot	Ambito bloccato	Snapshot pulita e non compromessa identificata	L'immutabilità, la scansione delle minacce e il punteggio di integrità delle snapshot riducono questo tempo
Mean-Time-to-Restore (MTTR)	Attivazione del ripristino	Dati resi disponibili per il carico di lavoro	Funzionalità come il ripristino istantaneo, il live mount e l'orchestrazione del disaster recovery in cloud agevolano questo processo
Mean-Time-to-Validate (MTTV)	Accesso ai dati pronto	Integrità delle applicazioni verificata	Ottenuto tramite coerenza applicativa, playbook di automazione e scansioni malware post-ripristino

MTTR totale (operativo) = MTTD + MTTScope + MTTCS + MTTRestore + MTTValidate

PERCHÉ L'MTTR È IMPORTANTE

Oggi molte organizzazioni trascurano le informazioni che si possono ricavare dai propri dati di backup. L'MTTR trasforma questo "gioiello della corona" in uno strumento non solo per garantire il ripristino, ma anche per misurare la resilienza.

In definitiva, l'MTTR è una fase di un ciclo continuo di valutazione della maturità in 4 step:

1 Determinare la resilienza

Capire le capacità attuali di resistere a un attacco basandosi sulle applicazioni più critiche e sugli scenari di attacco più probabili, attraverso un sistema di punteggio ben progettato, simile a una valutazione del rischio.

2 Definire il minimum viable business

Andando oltre i questionari e le liste applicative a livelli per comprendere realmente quali applicazioni e database sono essenziali, e quali sono le loro dipendenze, per mantenere la continuità operativa dando priorità a ciò che è mission-critical.

3 Validare la capacità di ripristino

Attraverso vere e proprie simulazioni di crisi, con scenari software realistici che includono esercitazioni interattive, per produrre metriche di recovery misurabili in tempi di pace, da utilizzare come base per miglioramenti futuri.

4 Analizzare e migliorare

In ogni fase del processo di recovery per determinare dove si verificano i colli di bottiglia e come intervenire. Per esempio, ridurre i dati di recovery mission-critical da 20 TB a 2 TB comporta una significativa riduzione del throughput necessario durante il ripristino.

E soprattutto, anonimizzando e aggregando i dati MTTR, le organizzazioni possono creare benchmark efficaci da confrontare con quelli di aziende del proprio settore o area geografica. Questo consente ai responsabili di ottenere finanziamenti per la cyber resilience e contribuisce ad abbattere i silos, offrendo a team di sicurezza, IT e recovery una visione condivisa di indicatori chiave come la velocità e l'affidabilità del ripristino.

COSTRUIRE LA RESILIENZA DELL'IDENTITÀ:

RACCOMANDAZIONI E CAPACITÀ DI RISPOSTA

L'identità non dovrebbe essere considerata solo una risorsa da proteggere. Andrebbe trattata come un piano di controllo primario per tutte le decisioni di sicurezza all'interno di un'azienda moderna.

Gli investimenti devono passare da una protezione focalizzata solo su endpoint e rete a una governance identitaria completa, con gestione degli accessi privilegiati e soluzioni avanzate di autenticazione. Un'identità compromessa oggi rappresenta un accesso diretto, e spesso invisibile, agli asset più critici di un'organizzazione. Per questo motivo, l'identità è oggi il punto di controllo più critico.

Considerato l'elevato numero di attacchi che coinvolgono le identità, le organizzazioni devono dare priorità a:

Visibilità e recovery delle identità

Se una chiave API cloud viene compromessa, quali sistemi devono essere scollegati? Se viene violato un account admin di Okta o Active Directory, si è in grado di isolare rapidamente il problema e forzare la ri-autenticazione per gli utenti coinvolti? Per rispondere e intervenire in questi casi servono visibilità in tempo reale e capacità di recovery negli ambienti ibridi di identità.

Costruire la resilienza delle identità

La resilienza è la capacità di riprendersi rapidamente e con sicurezza. I backup sicuri e offline di Active Directory o dei dati delle directory cloud sono fondamentali per ricostruire rapidamente i servizi di identità, nel caso in cui vengano crittografati o cancellati. Pianificando i passaggi di recovery insieme alla sicurezza, le organizzazioni riducono fortemente i tempi di inattività e l'impatto finanziario di un attacco alle identità.

Limitare la superficie di attacco e il raggio d'azione con i principi del modello Zero Trust

L'identità deve essere considerata il nuovo perimetro. Ogni richiesta di accesso, proveniente dall'interno o dall'esterno della rete, deve essere autenticata, autorizzata e crittografata in modo continuo. In termini pratici, ciò significa applicare una forte autenticazione MFA, policy di accesso condizionato e accesso con privilegi minimi già in fase di progettazione.

APPLICAZIONI DEL MODELLO ZERO TRUST ALLA SICUREZZA DELLE IDENTITÀ

Minimo privilegio e controllo degli accessi basato sui ruoli (RBAC)

Tutti gli utenti e i dispositivi, indipendentemente dalla loro posizione, ricevono solo i diritti di accesso strettamente necessari per svolgere le proprie funzioni specifiche.

Accesso Just-in-Time (JIT)

Permessi elevati o accessi sensibili vengono concessi solo per il tempo strettamente necessario a completare una specifica attività, dopodiché i privilegi vengono automaticamente revocati.

Verifica continua

Monitoraggio costante e rivalutazione dell'identità dell'utente, dello stato del dispositivo e del contesto (come posizione e orario) per mantenere o revocare l'accesso per l'intera durata della sessione, oltre alla MFA.

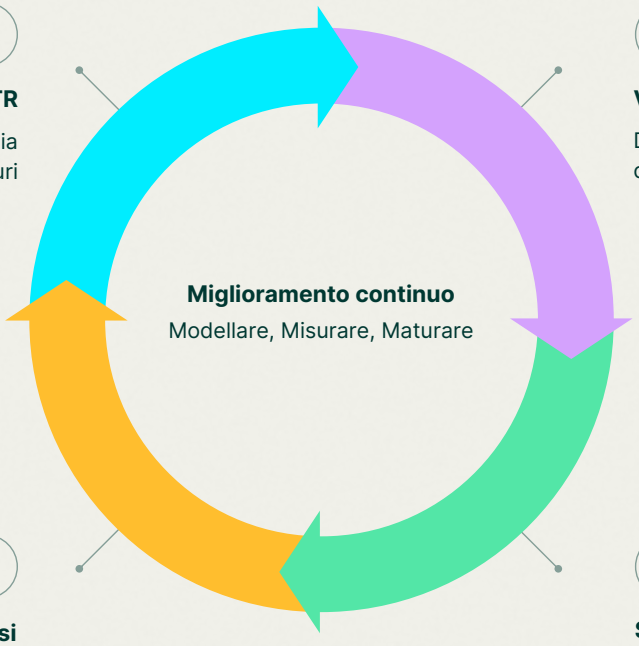
Microsegmentazione

Le reti dovrebbero essere suddivise in segmenti per contenere eventuali violazioni e impedire a utenti non autorizzati di spostarsi lateralmente alla ricerca di risorse da compromettere.

IL CICLO DI VITA DELLA CYBER RESILIENCE

La vera resilienza informatica va oltre la cybersecurity integrando gestione del rischio, continuità operativa e risposta agli incidenti in una strategia unificata. L'obiettivo non è solo prevenire gli attacchi, ma anche resistere e reagire rapidamente limitando al minimo l'impatto.

Il ciclo di vita della cyber resilience



1

Valutazione della resilienza

Definire e comprendere lo stato attuale della sicurezza e il profilo di rischio

2

Stabilire il Minimum Viable Business (MVB)

Identificare asset e infrastrutture chiave per garantire la continuità operativa minima

3

Situazione di crisi

Mettere alla prova le difese e la postura di sicurezza per misurarne l'efficacia

4

Analisi MTTR

Individuare e correggere i colli di bottiglia per migliorare i risultati futuri

Miglioramento continuo

Modellare, Misurare, Maturare

Il framework Rubrik Zero Labs, in linea con le linee guida NIST[10] per anticipare, resistere, adattarsi e riprendersi dagli attacchi informatici, mira a rendere operativa la resilienza per i team tecnici, offrendo al contempo metriche di benchmarking e miglioramento ai decisori aziendali.

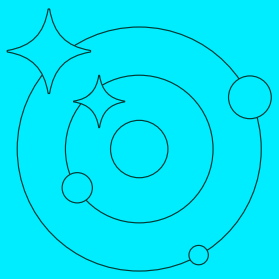
Integrando la pianificazione della resilienza identitaria in un approccio più ampio alla cyber resilience, le organizzazioni compiono passi concreti per ridurre le interruzioni, proteggere gli asset critici e rafforzare la fiducia dei propri stakeholder.

[10] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

DATI E METODOLOGIA

L'obiettivo di Rubrik Zero Labs è fornire informazioni pratiche e imparziali per aiutare le organizzazioni a ridurre i rischi legati alla sicurezza dei dati.

A tale scopo, questo report include informazioni provenienti da tre fonti principali:

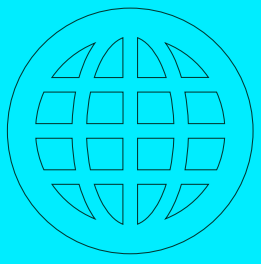


TELEMETRIA RUBRIK

Abbiamo utilizzato la telemetria di Rubrik per ottenere informazioni sull'ambiente dati tipico delle aziende e sui rischi associati

RICERCA INDIPENDENTE

I punti di vista di oltre 1600 leader del settore IT e della sicurezza tramite la ricerca Wakefield



ORGANIZZAZIONI CHE HANNO CONTRIBUITO

Ricerche di autorevoli organizzazioni e istituzioni di cybersecurity