O'REILLY®
Report

La Resa Dei Conti Della Cyber Resilience

Una nuova strategia per sopravvivere al panorama delle minacce Agentiche

Govind Rangasamy

Commvault

Visit commvault.com

97 9 834 18 5 986 5

La resa dei conti della Cyber Resilience

Una Nuova Strategia per Sopravvivere Al Panorama delle Minacce Agentiche

Govind Rangasamy

O'REILLY®

The Cyber Resilience Reckoning
by Govind Rangasamy

Published by O'Reilly Media, Inc., 141 Stony Circle, Suite 195, Santa Rosa, CA 95401.

O'Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (https://oreilly.com). For more information, contact our corporate/institutional sales department: 800-998-9938 or corporate@oreilly.com.

Acquisitions Editor: Simina Calin
Development Editor: Michele Cronin
Production Editor: Jonathon Owen
Copyeditor: Paula L. Fleming
Cover Designer: Susan Brown
Cover Illustrator: Ellie Volckhausen
Interior Designer: David Futato
Interior Illustrator: Kate Dullea

September 2025: First Edition

Revision History for the First Edition
2025-09-19: First Release

Questo lavoro fa parte di una collaborazione tra O'Reilly e Commvault. Si veda la nostra dichiarazione di indipendenza editoriale.

979-8-341-65986-5

[LSI]

Indice

Ringraziamenti

Desidero esprimere la mia sincera gratitudine a Katherine Demacopoulos per il suo eccezionale contributo in tutti gli aspetti della realizzazione di questo libro, ad Anna Griffin per aver riconosciuto l'importanza di questo progetto e averlo sostenuto, e a Chris DiRado per la sua preziosa competenza nel campo della sicurezza e per il suo supporto.

Vorrei inoltre ringraziare mia moglie Bhuvana e i miei meravigliosi figli Pranav e Sanjit per essere sempre presenti nella mia vita e per ricordarmi quotidianamente ciò che veramente conta. Il loro amore, la loro curiosità, le loro battute e i loro abbracci mi hanno infuso la gioia e l'energia necessarie per andare avanti.

CAPITOLO 1

Il cyber attacco è imminente. Sei in grado di recuperare in modo sicuro?

L'infrastruttura di un'organizzazione, comprese le reti, le applicazioni e gli archivi di dati, rappresenta la sua linfa vitale. Tuttavia, questi sistemi cruciali sono sempre più esposti a minacce informatiche frequenti e sofisticate. I criminali informatici stanno già utilizzando strumenti avanzati potenziati dall'intelligenza artificiale, ma una minaccia ancora più pericolosa sta emergendo. L'intelligenza artificiale agentica (AI), capace di ragionare, pianificare e agire autonomamente, sta per rivoluzionare le tattiche della criminalità informatica, rendendo gli attacchi più scalabili ed efficienti.

A differenza degli attacchi di ransomware tradizionali, che seguono script predefiniti, l'IA agentica può adattare la propria strategia in tempo reale, imparando dalle risposte difensive e accelerando l'evoluzione degli attacchi oltre la capacità di risposta dei difensori umani. Ciò rappresenta una sfida significativa per la sicurezza informatica moderna, poiché richiede un approccio più proattivo e adattivo alla resilienza informatica.

La capacità di recupero delle applicazioni aziendali critiche in tempi rapidi è fondamentale per la resilienza informatica. Non si tratta solo di prevenire gli attacchi, ma anche di essere in grado di ripristinare rapidamente le operazioni dopo un incidente. L'implementazione di una funzione di "ricostruzione" (Rebuild), che include test regolari e completi delle capacità di recupero, può aiutare le organizzazioni a raggiungere questo obiettivo.

Incidenti di alto profilo dimostrano che nessun settore o area geografica è immune alle minacce informatiche. Esempi recenti includono l'avvelenamento di un impianto di trattamento delle acque in Florida, la chiusura per 11 giorni della Colonial Pipeline, la paralisi di distretti scolastici a causa di attacchi ransomware e la crittografia totale dei sistemi di hotel e casinò.

Anche le difese perimetrali più robuste e i programmi avanzati di intelligence sulle minacce, come il Financial Services Information Sharing and Analysis Center (FS-ISAC) e la US Cybersecurity & Infrastructure Security Agency (CISA), rappresentano solo una parte della soluzione. Gli avversari odierni sono ben finanziati, estremamente pazienti e concentrati sull'obiettivo di compromettere la capacità di recupero delle organizzazioni bersaglio.

Comprendere l'attuale panorama delle minacce informatiche: l'industrializzazione del crimine informatico

Solo pochi anni fa, gli attacchi ransomware erano per lo più limitati a un ristretto numero di gruppi di hacker sofisticati. Oggi, le piattaforme Ransomware as a Service (RaaS) sono disponibili sul dark web per qualsiasi criminale con competenze moderate che desideri affittarle. Il modello di business RaaS funziona come qualsiasi piattaforma corporate Software as a Service (SaaS), offrendo tariffe di abbonamento e accordi di condivisione dei ricavi che rendono il cybercrime accessibile a chiunque sia disposto a pagare.

Queste imprese criminali forniscono accesso chiavi in mano a framework di estorsione sofisticati, completi di call center per il supporto alle vittime, assistenza alla negoziazione per i riscatti e persino "garanzie" di cancellazione dei dati se le vittime rifiutano di pagare. Questo approccio su scala industriale ha portato a un'esplosione degli attacchi. I criminali non hanno più bisogno di sviluppare malware

personalizzati. Possono semplicemente scegliere da un menu: LockBit, REvil, DarkSide, Conti, BlackCat e molti altri.

Ogni variante di ransomware offre caratteristiche specializzate diverse, progettate per massimizzare i danni e la leva negoziale. Le moderne varianti di ransomware esfiltrano regolarmente i dati prima della crittografia per minacciare la divulgazione pubblica, prendono di mira sistematicamente e distruggono i sistemi di backup per eliminare le opzioni di ripristino, e distribuiscono payload in grado di cancellare intere reti o account cloud in pochi minuti.

Ransomware con intelligenza artificiale agentica: quando gli attacchi pensano, imparano e si adattano

L'emergere dell'intelligenza artificiale (IA) agentica segna un cambiamento fondamentale rispetto alle tradizionali piattaforme Ransomware as a Service (RaaS). A differenza dell'IA generativa, che assiste in compiti specifici, l'IA agentica è proattiva e può risolvere problemi complessi e prendere decisioni autonomamente. Questi agenti di IA non si limitano a eseguire attacchi pre-programmati, ma apprendono e adattano le loro strategie in base all'ambiente specifico che incontrano.

Ad esempio, in test controllati, i ricercatori di Unit 42 hanno dimostrato un intero attacco, dalla compromissione iniziale all'esfiltrazione dei dati, in soli 25 minuti. La differenza di velocità è impressionante: mentre gli attaccanti umani avevano bisogno di due giorni (in media) per effettuare l'esfiltrazione dei dati, gli attacchi assistiti dall'IA hanno raggiunto lo stesso obiettivo circa 100 volte più velocemente.

Doppia estorsione e oltre: attacchi che vanno più a fondo

Il ransomware moderno segue spesso un piano d'azione in due fasi:

1. Esfiltrazione di dati sensibili.
2. Crittografia dei sistemi critici.

Anche se una vittima dispone di backup off-site o in una seconda regione cloud, la minaccia di esposizione pubblica dei dati sensibili e- sercita una pressione enorme per pagare il riscatto. A fine 2024, la violazione di LastPass ha esposto i backup delle casseforti crittografate di milioni di utenti, e anche se le password principali sono rimaste sicure, il semplice fatto che un attaccante avesse una copia di ogni cassaforte ha creato una crisi di fiducia.

Nel frattempo, gli attori nation-state utilizzano il ransomware non per profitto, ma per impatto strategico, ad esempio, interrompendo le operazioni chiave di oleodotti, servizi pubblici, sistemi sanitari e servizi governativi su larga scala, influenzando direttamente le tecnologie operative.

L'attacco ransomware WannaCry del 2017 offre un esempio lampante di questo problema. Ha gravemente interrotto i sistemi ospedalieri in tutto il Servizio Sanitario Nazionale del Regno Unito, portando alla cancellazione di procedure mediche e alla deviazione delle ambulanze. Questo attacco dimostra chiaramente come gli attacchi informatici possano mettere in pericolo vite umane quando l'infrastruttura critica fallisce.

L'ubiquità degli obiettivi

La democratizzazione dell'IA agentica attraverso piattaforme accessibili ha infranto l'illusione che determinati settori possano essere immuni dagli attacchi. L'IA agentica può aiutare a pianificare gli attacchi e poi eseguirli autonomamente, rendendoli più scalabili ed efficienti, riducendo al contempo la barriera all'ingresso per i criminali informatici.

Ciò significa che gli attacchi informatici non sono più limitati a gruppi di hacker sofisticati, ma possono essere condotti da chiunque abbia accesso a queste piattaforme. La conseguenza è un aumento significativo della minaccia informatica, poiché gli attacchi diventano

più frequenti e sofisticati.

- *Istruzione:* nel 2022, Vice Society ha tenuto in ostaggio i dati del Los Angeles Unified School District, colpendo oltre 1.000 scuole e 600.000 studenti.

- *Energia:* nello stesso anno, Suncor Energy in Canada ha subito un attacco ransomware che ha messo fuori uso i sistemi di pagamento Petro-Canada, lasciando bloccati i conducenti alle pompe di benzina in tutto il paese.

Comprendere l'attuale panorama delle minacce informatiche: l'industrializzazione del crimine informatico

- *Ospitalità:* nel 2024, il gruppo di hacker BlackCat ha lanciato un attacco informatico contro MGM Resorts, compromettendo le operazioni di 30 proprietà, comprese le slot machine e i sistemi di prenotazione.

- *Retail e servizi:* nell'aprile 2025, la catena di negozi Marks & Spencer nel Regno Unito è stata costretta a chiudere i suoi punti vendita a causa di un attacco informatico condotto dal gruppo DragonForce, che ha crittografato i suoi sistemi aziendali. Nello stesso periodo, anche le società Mailchimp e SendGrid hanno subito campagne di phishing su scala globale,

La morale è chiara: i nostri avversari hanno sia gli strumenti che gli incentivi per colpire ovunque. Man mano che la trasformazione digitale accelera, collegando sempre più dispositivi, processi e partner, la superficie di attacco cresce. I giorni in cui l'IT poteva isolare i "sistemi critici" dietro un firewall simile a una fortezza sono finiti. Ogni endpoint, servizio cloud e integrazione di terze parti è un potenziale punto di ingresso. Inoltre, l'interfaccia umana stessa, sia attraverso una chiamata deepfake generata dall'IA convincente che un dipendente che utilizza un dispositivo personale compromesso per lavoro, può diventare un'efficace porta d'ingresso per un attaccante.

Perché le organizzazioni sono ancora sorprese dagli attacchi informatici?

Nonostante le crescenti prove di maggiore vulnerabilità alle minacce informatiche, molte organizzazioni continuano a essere colte di sorpresa. Questa persistente vulnerabilità deriva da assunzioni radicate sulla sicurezza informatica che non corrispondono più alla realtà odierna. Tre punti ciechi critici - una mentalità incentrata solo sulla prevenzione, team e runbook in silos e una fede nella resilienza del cloud - lasciano anche le organizzazioni ben difese più esposte.

La mentalità di prevenzione: una falsa sensazione di sicurezza

La sicurezza informatica ha attraversato diverse fasi evolutive, con gli esperti che credevano di aver finalmente raggiunto la piena padronanza della protezione delle informazioni. Tuttavia, questa mentalità incentrata esclusivamente sulla prevenzione può creare un falso senso di sicurezza. La storia della sicurezza informatica mostra come le organizzazioni abbiano adottato approcci diversi nel tempo, convinte di aver trovato la soluzione definitiva. La tabella 1-1 illustra questa traiettoria evolutiva.

Tabella 1-1. Evoluzione della sicurezza informatica in ondate distinte

Anni	Focus	Falsa promessa	Realtà
1990s	Difese perimetrali	I firewall e i router impedirebbero l'accesso non autorizzato.	Gli attacchi hanno aggirato le difese attraverso il phishing, il social engineering e gli insider.
2000s	Email security	La scansione eliminerebbe i messaggi malevoli	Il malware si celava all'interno di flussi di dati e file legittimi.
2005+	Network security	Il monitoraggio avrebbe identificato le anomalie.	Le minacce sofisticate sembravano inoffensive fino a quando non hanno causato violazioni.
2010+	Endpoint protection	L'antivirus bloccherebbe l'esecuzione.	Malware senza file e exploit zero-day: una sfida per la sicurezza
2015+	Identity security	Zero trust avrebbe consentito solo l'accesso autenticato	I token rubati, le chiavi API e le autorizzazioni configurate in modo errato hanno creato delle lacune
2020+	Cloud security	I providers gestirebbero la sicurezza.	I cyber attacchi si sono focalizzati su autorizzazioni cloud e registri container configurati in modo scorretto

Nonostante l'aumento delle minacce informatiche, molte organizza- zioni rimangono ancorate a una mentalità incentrata sulla prevenzione. Investiamo pesantemente in firewall di nuova generazione, rilevamento e risposta agli endpoint (EDR), piattaforme di gestione delle informazioni e degli eventi di sicurezza (SIEM), feed di minacce e esercizi di red team, solo per scoprire che questi controlli sono necessari ma non sufficienti. Non appena un attaccante riesce a guadagnare un punto d'appoggio, sia attraverso il furto di credenziali, l'esecuzione di exploit zero-day, phishing o compromissione della catena di approvvigionamento, la difesa perimetrale crolla. La Figura 1-1 illustra la difesa stratificata nella quale l'industria della sicurezza informatica ripone la sua fiducia.

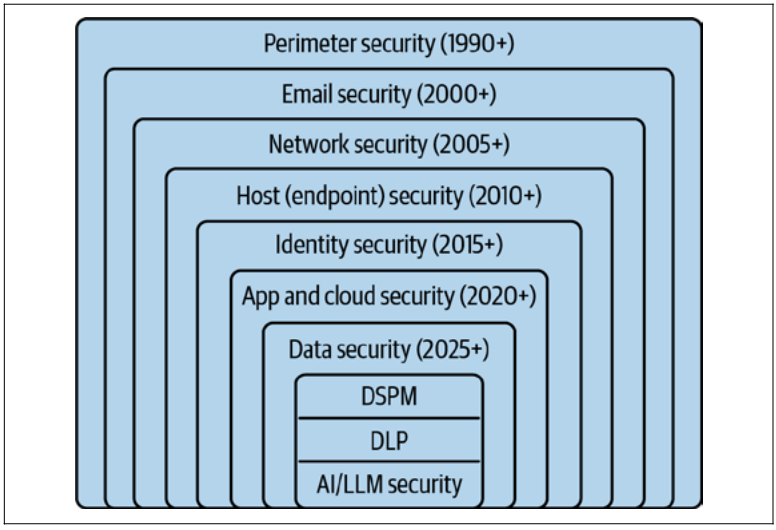

Figura 1-1. La difesa a più livelli del settore della cybersecurity

Qui si scatena il paradosso: concentrarsi eccessivamente sulla prevenzione porta a trascurare il ripristino e i test di ripristino. I backup sono spesso trattati come una mera formalità normativa, piuttosto che come una risorsa strategica fondamentale. I test di ripristino informatico sono spesso ridotti a un'esercitazione annuale di disaster recovery (DR), se non addirittura trascurati.

Quando si verifica un incidente, ci si affretta a seguire procedure ad hoc, solo per scoprire che sono obsolete, incomplete, non testate e incompatibili con gli ambienti dinamici odierni. Questo approccio non è più sostenibile di fronte alle minacce informatiche moderne.

Team isolati e runbooks scollegati

I team che si occupano di cybersecurity, cloud operation, sviluppo di applicazioni, architettura aziendale e continuità operativa spesso lavorano in silos, ciascuno con i propri processi, strumenti e priorità.

Il risultato? Le politiche e i runbook sono conservati in presentazioni PowerPoint, documenti Word e sistemi di ticketing e raramente, se non mai, vengono effettivamente utilizzati durante una crisi reale. Le connessioni e le dipendenze tra applicazioni, configurazioni di rete, sistemi di identità, repository GitHub, registri di container, server di database e copie di backup dei dati sono raramente documentate.

La prima volta che si tenta di ricostruire è il momento peggiore per scoprire che manca un pezzo.

Le illusioni della cloud resilience

Molti CIO, CTO e CISO credevano che il passaggio al cloud, con il pretesto della trasformazione digitale, avrebbe risolto magicamente il problema del ripristino organizzativo. I provider di servizi cloud pubblicizzano multizone, regioni, snapshot, copie replicate e strumenti di backup nativi che promettono di ridurre drasticamente i tempi di ripristino. Per raggiungere una corretta resilienza, i team spesso devono mettere insieme più di una dozzina di strumenti e servizi.

La scalabilità amplifica il problema. Le organizzazioni non gestiscono correttamente la loro postura di backup dei dati su tutti i loro account cloud. La cultura dello "shift left", che attribuisce agli sviluppatori maggiori responsabilità operative, ha probabilmente creato più rischi di quanti ne abbia mitigati.

I provider di servizi cloud continuano a rilasciare nuovi servizi e strumenti per semplificare il modello self-service, ma proprio questo

modello ha portato a processi interrotti, lasciando le organizzazioni ad un rischio ancora maggiore. Queste lacune diventano evidenti sotto pressione. In un caso recente, una società di servizi finanziari ha tentato di eseguire il failover su una seconda regione dopo una violazione simulata, ma ha scoperto che le chiavi di crittografia dei dati e i ruoli delle identità non erano stati replicati. Lo script di "region-failover" non ha funzionato, lasciando il sito di ripristino inutilizzabile.

Il cloud da solo non è una soluzione universale. Richiede ricostruzioni complete e testate dell'ambiente applicativo per assicurarsi che ogni configurazione, ogni credenziale e ogni oggetto sia al proprio posto.

Senza recupero, la resilienza è impossibile.

La dura realtà è che la maggior parte delle organizzazioni ha costruito la propria strategia di cybersecurity su un'illusione pericolosa: quella di poter prevenire ogni attacco. Questa mentalità incentrata sulla prevenzione crea un falso senso di sicurezza che si sgretola nel momento in cui un attaccante viola il perimetro. Senza una comprovata capacità di ripristinarsi rapidamente e completamente, anche le difese più sofisticate diventano prive di significato. Ciò è dovuto al fatto che la resilienza non riguarda l'evitare il fallimento, ma il riprendersi da esso.

Perchè le organizzazioni continuano a essere sorprese dagli attacchi Ridefinire la resilienza come "ripristinare la fiducia"

Se la resilienza significa qualcosa, significa fiducia. Fiducia nel fatto di poter riaccendere le luci quando si spengono. La resilienza informatica non è il tempo di attività del firewall, né la frequenza degli aggiornamenti. È la nostra capacità di ripristinare i servizi applicativi critici per l'azienda (ad esempio, portali dei clienti, sistemi di pagamento, linee di produzione o cartelle cliniche elettroniche) in pochi minuti o ore anziché giorni o settimane. Il motto "Rebuild is imperative" richiede tre cambiamenti fondamentali:

- *Dal backup alla ricostruzione completa dell'ambiente applicativo:* l'attenzione deve andare oltre la semplice copia dei file e gli snapshot a livello di blocco, per avere la capacità di ricostruire ogni componente dell'applicazione (cioè rete, calcolo, archiviazione, identità e soprattutto le loro dipendenze) per riattivare i servizi critici.

- *Da esercizi di DR (Disaster Recovery) infrequenti a test di ripristino regolari:* invece di eseguire esercizi di failover una volta all'anno, i team devono eseguire "esercizi automatizzati di ricostruzione" mensilmente in account cloud isolati dalla produzione.
- *Da playbook isolati a Recovery as Code (RaC) cross-funzionale:* i team di sicurezza, cloud, architettura, sviluppo e DR devono concordare su runbook condivisi che siano versionati come codice e testati all'unisono.

E se RaC potesse essere creato automaticamente e aggiornato regolarmente?

Il costo dell'autocompiacimento

Quando pochi minuti di downtime possono costare ad un'organizzazione migliaia di dollari, è importante rendersi conto di cosa significhi veramente rimanere offline per un'intera giornata. Anche un solo giorno può scatenare conseguenze devastanti: milioni di dollari persi in fatturato, multe normative schiaccianti e danni gravi alla reputazione (spesso irreparabili).

I rivenditori sono costretti a chiudere, impossibilitati a vendere; i produttori sono fermi, incapaci di spedire; e gli ospedali sono paralizzati, impossibilitati ad accedere ai registri vitali dei pazienti. Ogni minuto perso può significare un cliente arrabbiato, un partner tradito e un brand gravemente danneggiato.

Al contrario, le organizzazioni che adottano strategie di rebuild coerenti riferiscono di aver ridotto i loro tempi medi di ripristino da 48 ore (circa 2 giorni) a meno di 2 ore e di avere la certezza che anche l'attacco più sofisticato non possa tenerli fermi.

Questo è il ritorno sull'investimento della ricostruzione: non solo dollari risparmiati, ma anche fiducia salvata. Il prossimo capitolo esplorerà più in fondo lo sviluppo di una funzione di Ricostruzione.

CAPITOLO 2

Perché i vecchi metodi di ripristino non funzionano e perché il NIST dovrebbe includere la ricostruzione nel suo approccio alla sicurezza informatica. Questo è il punto debole della sicurezza che dobbiamo affrontare.

Non puoi spegnere un incendio in un bosco con una tazza di tè piena d'acqua.
— Tratto dalla saggezza dei pompieri che lavorano nelle foreste

Alla fine del XIX secolo, gli ingegneri costruirono imponenti argini tra le città di frontiera e il fiume Mississippi, fiduciosi che la loro massa imponente potesse trattenere qualsiasi inondazione. Le famiglie facevano picnic in cima a questi argini, credendo di aver vinto la bat- taglia contro l'acqua. Tuttavia, quando le acque primaverili rilasciarono torrenti senza precedenti, gli argini si ruppero come gusci d'uovo e l'acqua si riversò annegando la città.
La lezione da imparare: nessuna difesa, per quanto grandiosa, è inespugnabile quando si basa su presupposti errati.
L'infrastruttura digitale odierna affronta una crisi simile di fiducia mal riposta. I settori della cybersecurity e del backup hanno costruito i propri argini, ciascuno convinto dell'adeguatezza della propria soluzione:

- La cybersecurity erige barriere: perimetri, firewall, difese degli endpoint, cloud security e identity framework.
- Il settore del backup si concentra su archivi di dati, archivi su nastro, snapshot e strategie di replica.

Tuttavia, le violazioni di alto livello e gli incidenti ransomware hanno infranto questa illusione. Non importa quanto alte siano le barriere, gli attaccanti trovano un modo per superarle. Allo stesso modo, i metodi di backup tradizionali si rivelano del tutto inadeguati quando si tenta di ripristinare ecosistemi completamente compromessi dopo gli attacchi ransomware moderni. Questo capitolo esplorerà perché gli approcci di backup convenzionali sono insufficienti e perché una funzione di ricostruzione può migliorare sostanzialmente gli esiti di ripristino.

La pericolosa tendenza a trascurare il backup e la protezione dei dati

Per oltre 50 anni, abbiamo creduto che proteggere i dati fosse sufficiente. I sistemi di protezione dei dati hanno enfatizzato la conservazione a lungo termine a costi contenuti, non la protezione dell'intero ecosistema applicativo. Pertanto, quando le organizzazioni tentano di ripristinare i dati dopo un attacco ransomware, spesso scoprono una valanga di errori critici che rendono i loro backup quasi inutili.

Ad esempio, gli archivi su nastro preservano i file, ma il ripristino dei server richiede giorni. I backup su disco migliorano la velocità, ma risiedono su reti vulnerabili. I siti di ripristino di emergenza promettono un failover senza interruzioni, ma falliscono costantemente a causa di procedure obsolete, perdita della configurazione e lacune nella conoscenza.

Il difetto fondamentale non è nella protezione dei dati, ma nell'illusione che il backup equivalga alla capacità di ripristinare sistemi funzionanti. Un vero ripristino richiede non solo l'archiviazione dei dati offline, ma anche capacità di ripristino del sistema complete che la maggior parte delle strategie di backup non riesce a fornire.

Il Ransomware Moderno: la fine del backup tradizionale

Gli attacchi ransomware non si limitano a identificare i backup, ma li cercano attivamente come prima cosa, assicurandosi che il Piano B sia compromesso prima dell'inizio della Fase Due. Una volta che gli attaccanti ottengono i diritti di amministratore del dominio, smantellano sistematicamente le capacità di ripristino dell'organizzazione disabilitando o eliminando gli snapshot, manomettendo le politiche di

conservazione dei backup e corrompendo i vault che dovrebbero essere immutabili. Compromettono persino i livelli di orchestrazione che gestiscono questi sistemi, rendendo ogni potenziale percorso di ripristino un vicolo cieco.

La minaccia va oltre la semplice distruzione. Gruppi specializzati nella pratica della doppia estorsione hanno perfezionato un approccio calcolato: prima rubano dati sensibili per minacciare la divulgazione pubblica, poi crittografano ciò che rimane per paralizzare le operazioni. Questo duplice attacco massimizza la leva, poiché le organizzazioni si trovano ad affrontare sia l'interruzione operativa che il disastro reputazionale.

L'illusione dello storage immutabile

L'archiviazione immutabile è progettata in modo che, una volta scritti, gli snapshot non possano essere modificati. Tuttavia, gli attaccanti hanno sviluppato contromisure sofisticate che rivelano i limiti fondamentali di questa tecnologia. I criminali informatici dirottano il piano di gestione o il livello di controllo per alterare le politiche e le imposta- zioni di immutabilità prima che gli snapshot siano completati, neutra- lizzando effettivamente la protezione prima che abbia effetto. Sfruttano inoltre le vulnerabilità di configurazione per concedersi il potere di eliminare o re-criptare gli archivi, trasformando i controlli di sicurezza dell'organizzazione contro di essa.

Anche quando i vault rimangono tecnicamente sicuri, il loro ambito di protezione rimane pericolosamente limitato, salvaguardando i dati ma lasciando completamente esposte alla minaccia le configurazioni di rete, le mesh dei microservizi e gli identity trees.

Data Security Tools: utili ma incompleti

I recenti progressi in sicurezza hanno introdotto strumenti sofisticati come il Data Security Posture Management (DSPM) per una visibilità completa dei dati, la Data Loss Prevention (DLP) per monitorare il movimento dei dati e strumenti di sicurezza supportati dall'AI che consentono una rilevazione e risposta intelligenti alle minacce. Sebbene queste tecnologie rappresentino un significativo passo avanti nelle

capacità di cybersecurity, si concentrano principalmente sulla prevenzione e rilevazione piuttosto che sul ripristino completo, lasciando le organizzazioni vulnerabili quando gli attaccanti riescono a violare le loro difese.

Il canto delle sirene e gli scogli nascosti nel ripristino in cloud

I provider di servizi cloud hanno promesso capacità infinita, snapshot istantanei replicati in più regioni e pipeline di disaster recovery (DR) self-service. Molte organizzazioni, rassicurate sulla sicurezza dei loro dati, hanno migrato terabyte di dati in poche settimane. Tuttavia, queste promesse hanno mascherato lacune fondamentali che sono diventate evidenti solo quando le organizzazioni hanno avuto più bisogno delle loro capacità di ripristino.

In altre parole, le promesse dei cloud provider hanno creato aspettative elevate, ma non hanno garantito la capacità di ripristino effettiva in caso di emergenza. Le organizzazioni hanno scoperto che le loro capacità di ripristino erano insufficienti proprio quando ne avevano più bisogno.

Oltre il Backup tradizionale

I metodi di backup tradizionali non sono in grado di catturare le complesse interazioni tra i servizi cloud, né di rilevare i cambiamenti nelle configurazioni di rete e di identità, o di individuare malware e configu- razioni errate nascosti in container, funzioni serverless o librerie di applicazioni. Senza una copia completa e pulita dell'applicazione e dei dati, presa in un preciso momento nel tempo, i tentativi di ripristino sono instabili e soggetti a errori.

Affidarsi al vecchio approccio di "sperare che il backup funzioni" è come scommettere il proprio business su un paracadute che non è mai stato testato: è un rischio troppo grande da correre.

L'elemento cruciale mancante: test di ricostruzione regolari e completi

Sia le strategie di cybersecurity basate sulla difesa che quelle tradizionali di backup dei dati rimangono fondamentalmente incomplete. La soluzione risiede nel test regolare e realistico delle capacità di ricostruzione completa.

Il test di ricostruzione rappresenta un cambiamento fondamentale rispetto alla speranza che i backup funzionino, passando invece a testarne l'efficacia con una validazione completa. Questo approccio ricostruisce l'intero ambiente digitale esattamente come esisteva in un momento noto come "pulito", fornendo un ripristino olistico dell'ambiente che va ben oltre il semplice ripristino dei dati.

Il processo prevede il ripristino di ogni livello dell'infrastruttura dell'organizzazione - non solo dei dati, ma anche delle configurazioni di rete, delle risorse di calcolo, dei framework di identità, dei container, delle configurazioni serverless e dei gateway API - in modo che l'ambiente ripristinato rispecchi l'originale.

Soprattutto, il test di ricostruzione incorpora una scansione completa per malware, vulnerabilità, perdita della configurazione e alterazioni non autorizzate che potrebbero aver infiltrato l'ambiente prima dello snapshot. Questo passaggio di validazione trasforma il ripristino dei backup da un salto nel buio a un processo di ripristino verificato e sicuro di cui le organizzazioni possono fidarsi quando la loro sopravvivenza dipende da esso.

Il punto cieco del Cybersecurity Framework del NIST

Il National Institute of Standards and Technology (NIST) ha sviluppato un framework di cybersecurity che comprende sei funzioni principali: identificare le minacce, proteggere i sistemi, rilevare gli attacchi, rispondere agli incidenti, ripristinare i servizi e governare la sicurezza. Tuttavia, la funzione di ripristino è spesso fraintesa, creando una lacuna critica nella sicurezza delle organizzazioni.

In pratica, questo significa che molte organizzazioni credono di essere protette, ma in realtà sono esposte a rischi significativi a causa della mancanza di una comprensione approfondita della funzione di ripristino. La resilienza informatica non riguarda solo la prevenzione degli attacchi, ma anche la capacità di ripristinare rapidamente i servizi critici.

Per essere veramente resilienti, le organizzazioni devono andare oltre la semplice protezione e concentrarsi sulla capacità di ripristinare i loro sistemi e servizi in modo rapido ed efficace. Ciò richiede un approccio olistico che includa test regolari e completi delle capacità di ripristino.

Ripristinare verso Ricostruire: due funzioni distinte

La funzione di Ripristino (Recover) del NIST si concentra sul ripristino dei sistemi per riportarli a uno stato funzionale dopo un incidente. Questo approccio considera il ripristino come un controllo dei danni, enfatizzando la velocità rispetto alla validazione.

Le organizzazioni ripristinano dai backup, eseguono script di DR e celebrano quando le applicazioni sembrano funzionare, spesso senza verificare l'integrità o la completezza di ciò che è stato ripristinato.

Al contrario, la funzione di Ricostruzione (Rebuild) rappresenta un cambiamento di paradigma verso la ricostruzione con fiducia. Invece di limitarsi a ripristinare ciò che è stato perso, la funzione Rebuild è progettata per creare un ambiente applicativo pulito e verificato a partire da componenti noti come buoni.

È la differenza tra rattoppare un muro danneggiato e costruirne uno nuovo a partire da progetti affidabili. Entrambi i muri possono sembrare funzionali, ma solo uno può mantenere l'integrità strutturale.

Dove il Ripristino (Recover) è carente

Nella pratica, il processo di ripristino (Recover) è spesso ridotto a una serie di attività di conformità superficiali che non garantiscono effettivamente la capacità di ripristino. Le organizzazioni eseguono esercizi teorici di Disaster Recovery (DR) annualmente, ma non verificano mai se il ripristino effettivo dei sistemi funziona correttamente. Inoltre, eseguono ripristini sporadici dei database e test periodici delle macchine virtuali (VM), toccando solo una parte della loro infrastruttura e ignorando le complesse interazioni tra le diverse componenti delle applicazioni moderne.

Le organizzazioni raramente eseguono ripristini completi delle applicazioni con validazione regolare per assicurarsi che tutti i componenti siano coerenti con i dati di snapshot e funzionino insieme come un sistema integrato. La tabella 2-1 evidenzia le carenze dell'attuale framework del NIST rispetto alle esigenze moderne e mostra come la fun- zione di Ricostruzione (Rebuild) possa colmare queste lacune.

Elevare la Ricostruzione (Rebuild) a un pilar autonomo del framework di cybersecurity, come estensione della funzione di Ripristino (Recover), significa concentrarsi su un test più rigoroso della resilienza. Ciò include la capacità di tornare a un punto specifico nel tempo, selezio- nare una copia sicura e ricostruire l'applicazione dalla rete allo strato dei dati su richiesta.

"Tabella 2-1. I gap nell'attuale framework NIST e come la funzione Rebuild colma queste lacune

Funzione	Punti di forza tradizionali	Gap attuale	Gap attuale Come Rebuilt colma il gap
Identificare	Inventari delle risorse, BIA	Nessuna fiducia in un regolare recupero	Catalogo storico delle golden copies
Proteggere	IAM, crittografia, firewalls	Impossibile bloccare gli attacchi zero-day o gli attacchi interni	Snapshots immutabili per ricostruire gli artefatti
Rilevare	SIEM, XDR, UEBA	Alert ≠ ripristino garantito	Test di ricostruzione automatizzati attivati dai feed degli eventi
Rispondere	IR playbook, quarantene	I playbook raramente convalidano il ripristino completo	Il Rebuild integrato viene eseguito come parte della risposta
Recuperare (Recover)	Script di backup e failover	Ripristini parziali e manuali; runbook non testati	Orchestrazione definita tramite codice per la ricostruzione completa dell'ambiente
Ricostruire (Rebuild)			Esercitazioni regolari e automatizzate di ricostruzione ad un punto nel tempo

Il Framework Esteso

Per mantenere la resilienza, dobbiamo aggiungere la funzione Rebuild al framework NIST. Il Recover rimane la politica, il piano e il post-mortem — il quadro strategico che definisce cosa dovrebbe accadere quando si verifica un disastro. La Rebuild è il motore vivente che può rendere la ripresa una realtà comprovata piuttosto che una possibilità teorica, come mostrato nella Figura 2-1.

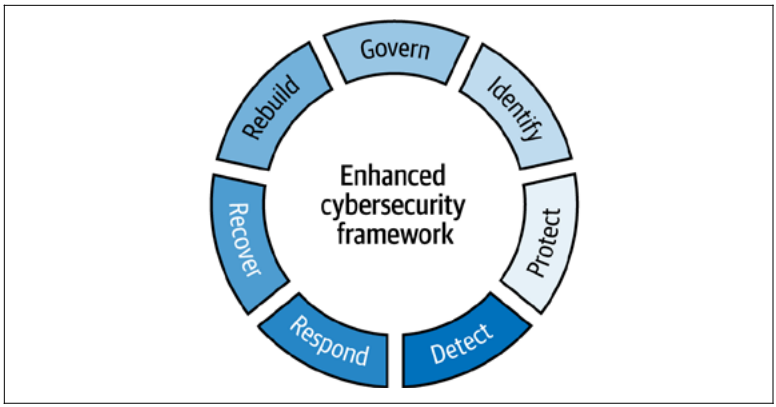

Figura 2-1. Il framework NIST con l'aggiunta della funzione Rebuild

La funzione Rebuild comprende diversi elementi chiave:

Ripristino dell'infrastruttura ad un punto nel tempo
: Questa funzionalità cattura snapshot completi e puntuali dei componenti dell'infrastruttura, comprese configurazioni di rete, risorse di calcolo, immagini delle applicazioni e le loro interdipendenze. A differenza dei backup tradizionali che si concentrano sui dati, questi snapshot sono progettati per ricreare il contesto infrastrutturale necessario alle applicazioni per funzionare correttamente.

Golden copies
: Queste sono immagini in un punto nel tempo che hanno subito una scansione completa per malware, configurazioni errate e vulnerabilità di sicurezza, fornendo così punti di ripristino validati e puliti. Non sono semplici copie di dati, ma snapshot verificate e pulite di interi stack applicativi di cui ci si può fidare implicitamente, eliminando la paura che il ripristino possa reintrodurre i problemi che si stanno cercando di risolvere.

Ripristino come codice (Recovery as Code, RaC)
: RaC trasforma le procedure di ripristino ad hoc in processi automatizzati, controllati e ripetibili. Invece di affidarsi a runbook obsoleti, RaC tratta le procedure di rebuild come software vivente che evolve con l'infrastruttura, in modo che le capacità di ripristino migliorino nel tempo anziché deteriorarsi per negligenza.

Il Framework Esteso

Il Rebuild trasforma lo "Spero che il backup funzioni" in "Ho fiducia che questa ricostruzione funzionerà". Ciò è possibile perché è stato testato, perfezionato e dimostrato funzionante decine di volte prima di essere effettivamente necessario.

CAPITOLO 3

Sbloccare il vantaggio del Rebuild: Testare l'imprevisto nel Cloud

All'inizio del XX secolo, la sicurezza automobilistica è migliorata drasticamente, non solo perché le auto sono diventate più robuste, ma anche perché i crash test sono diventati centrali nel processo di sviluppo dei veicoli, trasformando la sicurezza da una semplice speranza in un risultato garantito. Analogamente, nei primi giorni dell'aviazione, i piloti credevano che padroneggiare il volo significasse costruire aerei più forti.

Tuttavia, quando si verificavano disastri aerei, non era solo la robustezza dell'aereo a salvare vite, ma piuttosto la capacità del pilota di riprendersi da eventi imprevisti. Non importa quanto fosse ben progettato l'aereo, la sopravvivenza spesso dipendeva da un addestramento approfondito e rigoroso attraverso simulazioni di ogni possibile emergenza.

Oggi, la resilienza digitale si trova di fronte a un momento di trasformazione simile. Le organizzazioni devono andare oltre l'assunzione che i backup e le difese di cybersecurity funzionino. Un elemento mancante, e forse il più critico, è il test regolare. I test regolari consentono alle organizzazioni di ricostruire in modo affidabile i loro ambienti digitali dopo guasti catastrofici. Questo capitolo si concentrerà su come le organizzazioni possano implementare test di rebuild continui.

Racconti di backup che hanno fallito e piani di recupero che non hanno avuto successo

I recenti incidenti rivelano la fragilità dei nostri ecosistemi digitali nonostante i considerevoli investimenti che le organizzazioni hanno fatto nella sicurezza informatica e nei backup dei dati. La scala e l'intensità degli attacchi ransomware sono aumentate drasticamente negli ultimi anni, dimostrando che anche piani di ripristino di emergenza completi falliscono quando non sono stati testati rispetto alle realtà delle moderne minacce informatiche.

Consideriamo come le principali imprese abbiano subito perdite negli ultimi anni quando i loro piani di ripristino, nonostante la documentazione meticolosa e gli investimenti significativi, sono falliti in modo spettacolare

MGM Resorts e Caesars Entertainment
: Queste società hanno subito attacchi debilitanti alla fine del 2023, causando estese interruzioni. Nonostante i loro piani di DR completi, entrambe le società hanno faticato a ripristinare prontamente le funzioni aziendali critiche. Esisteva una documentazione solida, ma il ripristino effettivo è fallito a causa di dipendenze non testate, configurazioni obsolete e integrazioni mancanti tra i backup dei dati e il ripristino delle applicazioni.

Servizio Sanitario Nazionale (NHS), Londra, Regno Unito
: Un attacco nel 2024 con ransomware Qilin ha rivelato una cruda realtà: quasi un milione di cartelle cliniche di pazienti e sistemi critici di dati sanitari sono stati compromessi, nonostante la presenza di backup robusti. L'NHS ha dovuto imparare a proprie spese che ripristinare solo i database era insufficiente; senza procedure di ripristino verificate per applicazioni, identità e architetture di rete, i backup si sono rivelati inutili.

Attacchi ai Bucket AWS S3
: *In questo scenario del 2025*, il ransomware Codefinger ha preso di mira i bucket di archiviazione cloud dell'azienda, rendendo inefficaci le strategie tradizionali di cloud backup. Molte organizzazioni, nonostante i cloud backup regolari, si sono svegliate scoprendo che questi erano bloccati dietro la crittografia del ransomware. Tali incidenti evidenziano la necessità critica di un approccio completamente nuovo per testare le procedure di ripristino.

Queste storie illustrano una realtà preoccupante: le nostre assunzioni tradizionali sulla protezione dei dati e sulla sicurezza informatica sono incomplete. L'aumento esponenziale di ransomware sofisticati, unito alle sempre più frequenti interruzioni delle regioni cloud, richiede una nuova disciplina nella resilienza digitale: testare regolarmente, in modo completo e rigoroso, la ricostruzione dell'intero ambiente.

Oltre il ripristino tradizionale: la sfida moderna della ricostruzione in cloud

La ricostruzione degli ambienti cloud implica molto più del semplice ripristino dei dati dai backup. Le applicazioni moderne operano in ecosistemi altamente dinamici, composti da numerosi servizi cloud-native, che cambiano costantemente attraverso molteplici pipeline DevOps simultanee. Ora, queste stesse pipeline stanno diventando sempre più guidate dall'AI.

Dipendenze nascoste e deriva della configurazione

Ogni pipeline DevOps può aggiornare indipendentemente le configurazioni, distribuire microservizi e modificare le politiche di sicurezza, aumentando il rischio di deriva della configurazione e oscurando le dipendenze critiche. I team che utilizzano strumenti di integrazione continua e distribuzione continua (CI/CD) come AWS CodeDeploy, CodePipeline e CodeBuild alterano frequentemente gli ambienti senza una chiara visibilità sull'impatto delle loro modifiche. Pertanto, spesso creano vulnerabilità nascoste o dipendenze trascurate, rendendo difficile una ricostruzione completa e precisa in caso di crisi.

L'obiettivo principale è creare un piano strategico di operatività minima per facilitare la ricostruzione

La realtà pratica che la maggior parte delle organizzazioni affronta è che ricostruire tutto contemporaneamente non è né pratico né necessario. È qui che il concetto di operatività minima (o "minimum viable company") diventa il ponte strategico tra la teoria del Rebuild e l'implementazione riuscita.

Il framework di operatività minima riconosce che le organizzazioni hanno bisogno di una comprensione approfondita dei loro asset più critici e di ciò che è necessario per ripristinarli allo stato operativo. Invece di tentare l'impresa ardua di testare la ricostruzione completa dell'ambiente, le organizzazioni possono implementare la funzione Rebuild in modo incrementale concentrandosi su ciò che conta veramente per la sopravvivenza dell'azienda.

Le organizzazioni possono implementare efficacemente la funzione Rebuild classificando le loro applicazioni e servizi utilizzando framework consolidati come ISO 22301 (sistemi di gestione della continuità aziendale) o le linee guida per l'analisi dell'impatto aziendale del NIST. Questi framework aiutano le organizzazioni a classificare i sistemi in base alla loro criticità operativa:

- *Mission critical:* Sistemi senza i quali non è possibile operare (ad esempio, Active Directory, sistema di gestione degli ordini, sistemi di cura del paziente). Queste applicazioni costituiscono la base della minima operatività — senza di esse, l'organizzazione non può funzionare affatto.

- *Business critical:* Sistemi necessari per il pieno recupero delle operazioni (ad esempio, email, contabilità, gestione della supply chain). Questi sistemi consentono una capacità operativa ampliata oltre la semplice sopravvivenza.

- *Non-critical:* Tutti gli altri sistemi che supportano la piena funzio- nalità ma non sono essenziali per la continuità aziendale immediata.

Questo approccio a più livelli trasforma la funzione Rebuild da una sfida ingombrante in cui "tutto deve funzionare" in un processo di ripristino strategico e graduale. Le organizzazioni possono raggiungere l'operatività minima concentrando i test di Rebuild inizialmente sui sistemi business-critical, per poi espandersi sistematicamente alle applicazioni mission-critical e non critiche.

Questo approccio riduce drasticamente gli obiettivi iniziali di tempo di ripristino (RTO) per le funzioni aziendali essenziali, mantenendo al contempo l'obiettivo di ripristinare completamente l'ambiente.

La ricostruzione completa: metadati, automazione e orchestrazione

La ricostruzione efficace implica catturare tutti i metadati rilevanti — non solo i dati dell'applicazione, ma anche configurazioni dettagliate, dipendenze delle risorse, politiche di gestione dell'identità e dell'accesso (IAM), topologie di rete ed endpoint API.

È fondamentale che le organizzazioni replichino questi metadati completi in modo sicuro e immutabile su più regioni cloud o account isolati per minimizzare i singoli punti di guasto e migliorare la sicurezza contro ransomware e modifiche non autorizzate.

La ricostruzione deve sfruttare tecniche di *infrastruttura come codice (IaC) automatizzate*, integrando processi di ripristino precedentemente frammentati in pipeline di automazione eseguibili. Questo approccio consente alle operazioni di resilienza di rimanere adattabili, coerenti e verificabili.

Centralizzare e aggiornare continuamente il codice di ripristino consente ai team di gestire la resilienza in modo proattivo anziché rispondere alle crisi in modo reattivo. Pertanto, un processo di ricostruzione completo significa non solo ripristinare i dati, ma anche orchestrare l'intero ambiente cloud in modo fluido e coerente.

Implementazione della Funzione di Ricostruzione: Point-in-Time Infrastructure Recovery e Recovery as Code

Commvault's Cloud Rewind (precedentemente noto come Appranix) affronta le debolezze critiche nelle pratiche tradizionali di Disaster Recovery (DR) con due concetti innovativi per la ricostruzione on-demand degli ambienti applicativi: il ripristino dell'infrastruttura ad un punto nel tempo (PITR) e il Ripristino come Codice (RaC).

Storicamente, le organizzazioni hanno lottato con runbook di ripristino frammentati, gestiti in modo indipendente dai team di sicurezza, applicazioni, architettura aziendale e backup. In caso di crisi, i team di continuità aziendale hanno subito ritardi significativi mentre

assemblavano questi documenti di ripristino sparsi in azienda, portando a tempi di inattività prolungati.

Il ripristino dell'infrastruttura ad un punto nel tempo risolve questo problema fornendo uno snapshot automatizzato e completo di un intero ecosistema digitale — non solo i dati, ma l'intero stack applicativo, microservizi, funzioni serverless, configurazioni di identità e accesso, topologie di rete e le loro dipendenze.

Catturando regolarmente questi stati completi ad un punto nel tempo, in base alle politiche definite, PITR consente alle organizzazioni di mantenere golden copies validate e complete, prontamente disponibili sia per il ripristino dell'operatività minima che per la ricostruzione completa dello stack applicativo.

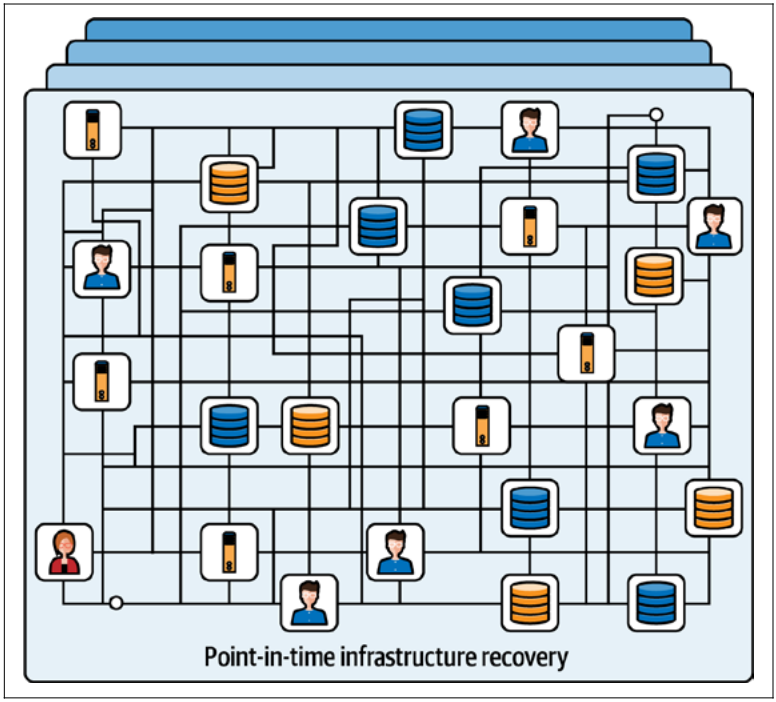

Figura 3-1. Illustrazione di come PITR fornisce uno snapshot completo di un intero ecosistema applicativo cloud

La capacità di PITR di catturare snapshot a più livelli diventa particolarmente preziosa per le strategie di operatività minima. Le organizzazioni possono configurare politiche che danno priorità alle applicazioni business-critical per snapshot più frequenti, forniscono sistemi mission-critical con punti di ripristino verificati e mantengono una protezione di base per le applicazioni non critiche.

Questo approccio a più livelli consente un rapido ripristino delle operazioni minime vitali mantenendo una protezione completa in tutto l'ambiente.

Sfruttare le piattaforme cloud hyperscale come AWS, Azure o Google Cloud migliora ulteriormente questa capacità. Le vaste risorse di calcolo on-demand e le funzionalità di isolamento integrate dei cloud hyperscale consentono alle organizzazioni di eseguire frequenti test su larga scala con facilità ed efficienza. Queste piattaforme semplificano le complesse convalide di ripristino, trasformando esercizi di disaster recovery costosi e infrequenti in esercizi di rebuild routinari ed economici.

Il Ripristino come Codice (RaC) completa PITR trasformando il ripristino in un processo unificato e automatizzato che operativizza la funzione di Ricostruzione. Invece di mantenere runbook separati e ingombranti, RaC incorpora tutti i passaggi di ripristino necessari direttamente nelle pipeline di automazione eseguibili (Figura 3-2).

Il codice controllato da versioni serve come unica fonte di verità per il ripristino, allineando i team di sicurezza, gli architetti, gli sviluppatori di applicazioni e gli specialisti di backup intorno a un processo centralizzato e coerente. Questo approccio guidato dal codice integra i test di ricostruzione regolari senza soluzione di continuità nei flussi di lavoro DevOps quotidiani, riducendo significativamente la complessità operativa.

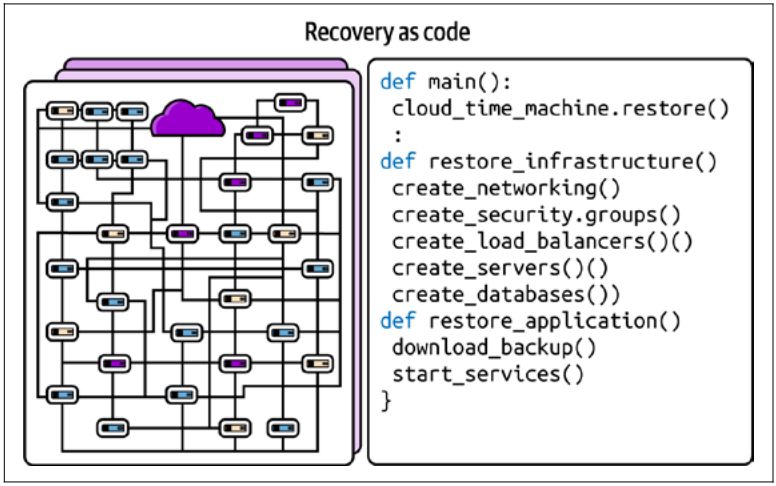

Figura 3-2. PITR e RaC a braccetto: come RaC incorpora tutti i passaggi di ripristino nelle pipeline di automazione eseguibili.

Utilizzo Strategico di Rebuild

RaC può essere strutturato per supportare i flussi di lavoro in opera- tività minima, con pipeline di automazione separate per livelli di applicazione business-critical, mission-critical e non critici. Ciò consente alle organizzazioni di eseguire un ripristino rapido dell'operatività minima mentre si preparano contemporaneamente per il recupero completo dell'ambiente, rendendo la funzione Rebuild sia strategica che pratica.

Insieme, PITR e RaC cambiano fondamentalmente la resilienza organizzativa. Queste innovazioni abilitano le organizzazioni a passare dall'incertezza e dalla gestione reattiva delle crisi a una capacità proattiva e dimostrabile, riducendo significativamente i tempi di ripristino e semplificando i requisiti di conformità e per costruire una fiducia ineguagliata con le parti interessate. Il test di rebuild regolare diventa così non solo realizzabile, ma anche un imperativo strategico per la resilienza digitale moderna.

Il Valore Aziendale dei Test di Rebuild Regolari con Ottimizzazione dei Costi

L'adozione di test di ricostruzione regolari con PITR e RaC trasforma fondamentalmente la resilienza organizzativa, rendendo la funzione di Rebuild sia economicamente sostenibile che strategicamente preziosa. Invece di affidarsi a piani di ripristino incerti e alla gestione delle crisi guidata dalla paura, le organizzazioni possono raggiungere capacità di ripristino chiare, misurabili e dimostrabili.

Consideriamo un'organizzazione sanitaria che affronta un attacco ransomware. Invece di aspettare il ripristino completo dell'infrastruttura, la pianificazione dell'operatività minima aiuta il ripristino rapido dei sistemi di cura del paziente, delle operazioni del pronto soccorso e delle capacità di comunicazione critiche. L'organizzazione può ripristinare successivamente i suoi sistemi amministrativi, piattaforme di pianificazione e strumenti di reporting, senza influire sulla cura del paziente.

Questo approccio a più livelli fornisce una serie di benefici aziendali chiave misurabili.

Miglioramento delle Operations e Fiducia dei Clienti

Dando priorità ai sistemi che generano ritorni economici nella pianificazione dell'operatività minima, le organizzazioni possono riprendere rapidamente le operazioni aziendali fondamentali mantenendo la fiducia dei clienti. Questa fiducia diventa un vantaggio competitivo, soprattutto nei settori in cui l'affidabilità digitale impatta direttamente sulle relazioni con i clienti.

Benefici legati alle normative e alla conformità

La pianificazione dell'operatività minima aiuta le organizzazioni a soddisfare i requisiti regolatori per il mantenimento dei servizi essenziali durante le interruzioni. Il test di rebuild automatizzato semplifica i processi di conformità generando regolarmente prove complete, rendendo più efficienti le preparazioni per gli audit.

Le organizzazioni possono dimostrare l'aderenza a standard regolatori come l'Health Insurance Portability and Accountability Act (HIPAA) e framework di settore come SOC 2, ISO 27001 e il Digital Operational Resilience Act (DORA) con uno sforzo manuale minimo, fornendo agli auditor informazioni immediate sulle capacità di resilienza.

Riduzione dei Costi e dei Tempi

L'automazione delle attività di rebuild riduce sostanzialmente la complessità e i costi. I test tradizionali di disaster recovery sono costosi, disruttivi e soggetti a errori umani. Adottando RaC, le organizzazioni possono effettivamente ricostruire e testare su richiesta utilizzando la programmabilità e i modelli di distribuzione del cloud hyperscale.

Si possono automatizzare processi di rebuild intricati, trasformando runbook manuali sparsi in procedure basate su codice, snelle e ripetibili. Questa automazione non solo riduce l'overhead operativo ed elimina le spese di test manuali, ma promuove anche la coerenza e l'affidabilità in ogni test.

Fiducia e Affidabilità Organizzativa

Forse più significativamente, i test regolari di Rebuild generano una fiducia e un'affidabilità organizzativa senza pari. Le capacità di ripristino validate regolarmente offrono ai team di leadership una chiara e dimostrabile garanzia della loro prontezza a gestire le interruzioni.

Gli organismi regolatori, i clienti e i partner acquisiscono la certezza che l'organizzazione sta mitigando proattivamente i rischi e può riprendersi rapidamente da qualsiasi attacco informatico o guasto cloud. Questa fiducia diventa un vantaggio strategico, distinguendo le organizzazioni resilienti in un mondo sempre più definito da minacce e interruzioni digitali.

Rendere i Test di Ricostruzione Pratici: Infrastruttura e Metodi di Validazione

Dopo aver stabilito il quadro strategico per l'operatività minima, la domanda diventa: come fanno le organizzazioni a eseguire effettivamente test di ricostruzione regolari su larga scala per le applicazioni critiche? La risposta risiede in due elementi abilitanti, che rendono i test frequenti sia accessibili che realistici:

- Innanzitutto, le piattaforme cloud hyperscale forniscono l'infrastruttura flessibile necessaria per creare ambienti di test completi su richiesta.
- In secondo luogo, i principi dell'ingegneria del caos aiutano questi test a simulare guasti del mondo reale piuttosto che scenari prevedibili.

Insieme, questi approcci trasformano i test di ricostruzione da un esercizio annuale costoso in una capacità operativa di routine.

Utilizzo delle piattaforme cloud come motore per i test

Piattaforme cloud come AWS, Azure e Google Cloud offrono un am- biente ideale per test di ricostruzione regolari grazie alla loro flessibilità, scalabilità e convenienza senza pari. A differenza dei data center tradizionali, i cloud hyperscale consentono alle organizzazioni di creare ambienti sandbox completamente isolati istantaneamente, eseguire test rigorosi e distruggerli senza influire sulla produzione.

Questa flessibilità rimuove le barriere ingombranti tradizionalmente associate ai test di disaster recovery, consentendo test più frequenti, approfonditi e significativi.

Un vantaggio significativo di queste piattaforme è la loro vasta disponibilità di risorse di calcolo e archiviazione on-demand, che consentono alle organizzazioni di scalare rapidamente le risorse in base alle esigenze specifiche dei test. L'uso strategico delle istanze spot fornisce capacità di calcolo a costi drasticamente ridotti — spesso dal 70% all'80% in meno rispetto ai prezzi on-demand tipici — consentendo una maggiore frequenza di test senza vincoli di budget aggiuntivi.

L'ambiente cloud consente inoltre la simulazione di guasti parziali dell'infrastruttura, il test delle capacità di failover cross-regionale per sistemi business-critical e la convalida che le procedure di ripristino dell'operatività minima funzionino in varie condizioni di guasto — tutto all'interno di ambienti di test isolati ed economici.

I test di ricostruzione regolari, un tempo considerati complessi e costosi, sono ora pratici e accessibili, consentendo a quella che una volta era un'attività di conformità occasionale di diventare una capacità organizzativa fondamentale.

Test del Caos: Costruire la Resilienza Attraverso il Fallimento Intenzionale

Il test del caos è la pratica di introdurre deliberatamente interruzioni controllate in un sistema per scoprire debolezze nascoste e validare la resilienza in condizioni realistiche. Questo approccio introduce

intenzionalmente scenari di guasto, come interruzioni dell'infrastruttura, latenza di rete o picchi di risorse imprevisti, per testare se i sistemi continuano a funzionare in modo affidabile sotto stress.

A differenza degli esercizi standard di DR, che spesso simulano scenari prevedibili, il test del caos prospera sull'imprevedibilità, sfidando continuamente le assunzioni e rivelando punti ciechi nella resilienza delle applicazioni e dell'infrastruttura.

Nel contesto dei test di rebuild, il test del caos diventa particolarmente critico. Poiché gli ambienti di produzione evolvono costantemente, nuovi servizi vengono distribuiti, le configurazioni cambiano e i carichi di lavoro fluttuano. I test di rebuild statici tradizionali diventano rapidamente obsoleti. Le piattaforme cloud consentono alle organizzazioni di eseguire test di rebuild adattivi che riflettono la natura dinamica delle applicazioni moderne. Integrando i principi dell'ingegneria del caos con le pratiche di rebuild, i test evolvono proattivamente, riflettendo la complessità della produzione e adattandosi continuamente ai cambiamenti.

Il test del caos diventa ancora più prezioso quando applicato al concetto di operatività minima. Invece di testare guasti casuali in interi ambienti, le organizzazioni possono concentrare gli esperimenti di caos sui sistemi business-critical per capire come i guasti potrebbero propagarsi e influire sul ripristino della minima operatività.

Ad esempio, durante un esercizio di ripristino dell'operatività minima, il test del caos potrebbe disabilitare deliberatamente i servizi di Active Directory per validare che i sistemi di autenticazione di backup possano mantenere le operazioni aziendali essenziali. Oppure potrebbe simulare guasti di partizione di rete tra microservizi critici per confermare che le applicazioni di minima operatività rimangano funzionanti anche quando i servizi dipendenti non sono disponibili.

Eseguire regolarmente test di Rebuild: dalla teoria ai risultati concreti

Stabilire test di ricostruzione regolari trasforma la resilienza organizzativa da rassicurazione teorica in capacità concreta e misurabile. Proprio come lo sviluppo software ora incorpora pratiche regolari di garanzia della qualità (QA), la resilienza digitale deve adottare similmente test di ricostruzione regolari. I CIO e i CISO possono aspettarsi risultati tangibili: capacità di ripristino dimostrabile, riduzioni misurabili del rischio e chiaro allineamento tra i team di sicurezza, cloud operations e ripristino.

Esecuzione di strategie di testing su più livelli

Un approccio strutturato inizia pianificando giorni di test mensili o trimestrali che incorporano sia scenari di operatività minima che di ripristino completo dell'ambiente. Questi eventi devono essere pianificati con cura e includere esercizi regolari di ripristino, esercizi di operatività ed esperimenti di caos controllato.

Giornate di Test per l'operatività minima

Le organizzazioni dovrebbero condurre esercizi separati focalizzati specificamente sul ripristino dei sistemi business-critical entro finestre temporali definite. Questi test validano che le funzioni aziendali essenziali possano essere ripristinate rapidamente, tipicamente entro ore piuttosto che giorni.

I parametri di successo per questi test includono il tempo necessario per ripristinare i servizi di identità, il tempo per portare online le applicazioni aziendali core e la verifica che le operazioni minime vitali possano essere sostenute mentre continua il ripristino completo.

Test completo di ricostruzione dell'ambiente

È anche importante condurre test più ampi che verifichino il ripristino completo dell'infrastruttura, confermando che i sistemi mission-critical e non critici possano essere ripristinati con successo dopo aver raggiunto la minima operatività. Questi test validano la capacità dell'organizzazione di tornare alla piena capacità operativa.

Definizione dei Ruoli e delle Responsabilità

Definire chiaramente i ruoli e le responsabilità diventa cruciale per test efficaci, soprattutto quando si bilanciano le priorità della minima operatività e il ripristino completo dell'ambiente.

Team di Sicurezza

I team di sicurezza verificano che gli ambienti ripristinati siano rigorosamente scansionati e liberati da vulnerabilità, firme di ransomware e configurazioni errate. Durante il ripristino dell'operatività minima, questi team danno priorità alla convalida dei sistemi business-critical mentre conducono parallelamente valutazioni di sicurezza complete dell'ambiente più ampio.

Team di Cloud Operations e Applications

Questi team si concentrano sul provisioning dell'infrastruttura, sull'allineamento delle configurazioni e sull'orchestrazione di rebuild completi dagli snapshot PITR dell'ambiente. Gestiscono l'esecuzione tecnica sia del ripristino della minima operatività che dei rebuild completi dell'ambiente, confermando che le dipendenze dell'infrastruttura sono sequenziate correttamente e che i servizi ripristinati soddisfino i re- quisiti funzionali.

Team di Ripristino

Sovrintendendo all'intero processo di rebuild, i team di ripristino forniscono coordinamento tra tutti i gruppi e documentazione accurata dei risultati. Gestiscono la transizione dall'operatività minima alla piena capacità operativa e coordinano i diversi scenari di test.

Misurare il successo e dimostrare il valore

Per valutare l'efficacia e dimostrare il valore dei test di ricostruzione, è necessario stabilire e comunicare metriche chiare. Queste metriche vanno oltre i semplici obiettivi di tempo di ripristino (RTO) e obiettivi di punto di ripristino (RPO). Esse includono:

Metriche di Operatività Minima

: Tempo necessario per ripristinare interamente i sistemi business-critical e le dipendenze associate, tasso di successo delle procedure di minima operatività in condizioni di stress e capacità di sostenere le operazioni essenziali durante il ripristino completo.

Metriche di ripristino completo

La frequenza e l'approfondimento dei test del caos eseguiti, il numero di vulnerabilità o configurazioni errate identificate e risolte attraverso i test e il miglioramento delle prestazioni di ripristino nel corso del tempo sono tutti aspetti cruciali per valutare l'efficacia dei test di resilienza

Valutazioni delle capacità di resilienza mediante test

Frequenza e approfondimento dei test del caos eseguiti, numero di vulnerabilità o configurazioni errate identificate e risolte attraverso i test e miglioramento delle prestazioni di ripristino nel tempo

Metriche di impatto sul Business

La riduzione delle potenziali perdite economiche durante gli incidenti informatici, il miglioramento delle metriche di fiducia dei clienti e la dimostrazione della conformità normativa attraverso test regolari sono tutti aspetti cruciali. I CIO e i CISO dovrebbero aspettarsi rapporti regolari che evidenzino queste metriche, fornendo trasparenza e prova concreta del miglioramento nel tempo.

I test di ricostruzione regolari forniscono una prova concreta delle capacità di ripristino a tutti gli stakeholder — dai team di sicurezza che desiderano validare la mitigazione delle minacce ai dirigenti che cercano di dimostrare la resilienza operativa.

Da tempo considerata una best practice, i test di ricostruzione regolari diventano un elemento fondamentale della gestione del rischio aziendale. Integrando i principi di operatività minima con test completi, le organizzazioni possono dimostrare con fiducia la loro capacità di ripristinare rapidamente le funzioni aziendali essenziali mantenendo una completa resilienza digitale. Questa capacità è diventata essenziale per la sopravvivenza organizzativa poiché le minacce informatiche continuano a evolversi e intensificarsi.

CAPITOLO 4

La chiave per una resilienza informatica efficace: implementare la capacità di ricostruzione Cyber Resiliente

La vera resilienza informatica dipende da una capacità critica che va oltre i framework di sicurezza tradizionali. Come stabilito nel Capitolo 2, il Framework di Cybersecurity del NIST richiede una settima funzione: Rebuild. Questa funzione trasforma l'incertezza in fiducia, rendendo obsoleto l'approccio "Spero che il backup funzioni" grazie alla prova delle capacità di ripristino attraverso test regolari.

L'approccio di operatività minima delineato nel Capitolo 3 rende questa trasformazione realizzabile. Invece di tentare di testare tutto contemporaneamente, le organizzazioni possono implementare Rebuild in modo sistematico, partendo dai sistemi business-critical e ampliandosi agli ambienti completi. Questo quadro strategico trasforma una sfida ingombrante in un processo gestibile, passo dopo passo, che fornisce valore immediato mentre si procede verso una resilienza completa.

La minaccia Agentica: come cambiano la velocità degli attacchi e i requisiti per un ripristino efficace

Gli esperti prevedono che potremmo vivere in un mondo di agentic attackers già quest'anno, con agenti AI che rappresentano una prospettiva attraente per i criminali informatici perché sono molto più economici rispetto all'assunzione di hacker professionisti e possono orchestrare attacchi più rapidamente e su scala molto più ampia rispetto

agli esseri umani.

Il ransomware agentic rappresenta una collezione di bot AI che eseguono tutti i passaggi necessari per attacchi ransomware di successo, ma più velocemente e meglio degli operatori umani.

Questi sistemi non solo accelerano i metodi di attacco esistenti, ma cambiano fondamentalmente il gioco operando a velocità macchina con capacità di apprendimento automatico.

Le implicazioni per il ripristino sono profonde. In quasi un caso su cinque, l'esfiltrazione dei dati avviene entro la prima ora di compromissione. Gli approcci tradizionali di backup e ripristino, progettati per minacce a velocità umana che fornivano giorni o settimane di preavviso, diventano obsoleti quando gli attacchi passano dalla rico- gnizione alla crittografia in pochi minuti.

È per questo che la funzione di ricostruzione rapida e automatizzata diventa ancora più critica nell'era degli agentic. Solo attraverso test regolari e automatizzati le organizzazioni possono rimanere al passo con gli avversari che imparano e si adattano a velocità superumana.

Il percorso strategico per raggiungere la resilienza informatica: dalle soluzioni minime praticabili alla resilienza completa

Il percorso per raggiungere la fiducia nella ricostruzione inizia con l'identificazione dei sistemi business-critical essenziali per l'operatività minima durante una crisi. Le organizzazioni implementano quindi tecnologie come snapshot PITR e automazione RaC per questi sistemi prioritari, rendendo possibile un test completo e strutturato.

Raggiungere l'operatività minima consente alle organizzazioni di espandere successivamente le loro capacità di ricostruzione. Possono concentrarsi inizialmente sui sistemi mission-critical, come la contabilità e la gestione della supply chain, per poi includere le applicazioni non critiche. Man mano che le organizzazioni acquisiscono esperienza e perfezionano i loro processi possono estendere la loro capacità di ricostruzione a tutto l'ecosistema digitale.

Le piattaforme cloud hyperscale discusse nel Capitolo 3 rendono questo progresso economicamente sostenibile. Le istanze spot riducono i costi dei test fino al 90% rispetto ai prezzi on-demand, mentre l'infrastruttura flessibile consente una convalida frequente senza influire sui sistemi di produzione.

Il test del caos verifica che gli scenari dei test siano rappresentativi di guasti reali, aumentando così la fiducia nelle capacità di ripristino dell'organizzazione.

Superare le sfide dell'implementazione

Il percorso verso la fiducia nella ricostruzione segue il concetto di operatività minima che rende possibile un test completo. Le organizzazioni iniziano identificando i loro sistemi business-critical, quelli essenziali per la minima operatività durante una crisi. Implementano quindi snapshot PITR e automazione RaC per questi sistemi prioritari, come prima azione.
Il successo dell'operatività minima crea una base per l'espansione. Le organizzazioni possono quindi estendere le capacità di ricostruzione a sistemi mission-critical come la contabilità e la gestione della supply chain, seguiti dalle applicazioni non critiche. Ogni espansione si basa su processi comprovati e sulla crescente esperienza organizzativa, e alla fine si raggiunge una capacità di ricostruzione completa in tutto l'ecosistema digitale.
Le piattaforme cloud hyperscale discusse nel Capitolo 3 rendono questo progresso economicamente sostenibile. Le istanze spot riducono i costi dei test fino al 90% rispetto ai prezzi on-demand, secondo la documentazione ufficiale di AWS e Azure, mentre l'infrastruttura flessibile consente una convalida frequente senza influire sui sistemi di produzione.
Il test del caos conferma che gli scenari di test riflettono scenari di guasto del mondo reale, costruendo una genuina fiducia nelle capacità di ripristino.

Vincoli di bilancio e risorse limitate

L'automazione RaC unifica i runbook frammentati in pipeline controllate da diverse versioni. I team di sicurezza, cloud operations, applications e ripristino collaborano sulla stessa base di codice invece di mantenere documentazioni separate e isolate. Questo consolidamento elimina la necessità di esercizi separati tra i team, fornendo coerenza e riducendo lo sforzo manuale.

Il ritorno sull'investimento diventa chiaro quando le organizzazioni misurano i tempi di ripristino dell'operatività minima. Ridurre l'RTO da 48 ore a 2 ore per i sistemi business-critical produce valore immediato. L'automazione della raccolta delle prove per la conformità a SOC 2, ISO 27001 e DORA riduce l'onere degli audit fornendo una convalida continua delle capacità di ripristino.

Coinvolgimento della Direzione e allineamento organizzativo

Nulla garantisce il supporto della Direzione come la dimostrazione di capacità. Le organizzazioni possono mostrare metriche di ripristino live attraverso dashboard, offrire rapporti di audit ai dirigenti e dimostrare il completamento del ripristino in meno di un'ora anziché in giorni o settimane.

L'approccio di minima operatività si rende immediatamente visibile in azienda. Quando la Direzione vede che i sistemi core che generano entrate economiche possono essere ripristinati rapidamente e in modo affidabile, il finanziamento e il supporto organizzativo seguono naturalmente. Ogni test di operatività minima riuscito costruisce fiducia per un'implementazione più ampia di Rebuild.

La ricostruzione come pratica standard: il futuro della resilienza informatica

Il futuro della resilienza informatica sta già emergendo, guidato dalla realtà delle minacce agentic. Man mano che l'agentic AI diventa più capace, i team di sicurezza delegheranno più compiti ad agenti autonomi con istruzioni minime, consentendo ai sistemi e alle reti di tenere il passo con le tattiche di minaccia in continua evoluzione. Nel giro di cinque anni, la funzione di Ricostruzione (Rebuild) sarà fondamentale per la sicurezza informatica quanto le attuali funzioni del framework NIST. La pianificazione dell'operatività minima diventerà una pratica standard, con le organizzazioni che manterranno procedure di ripristino testate per i sistemi business-critical con lo stesso rigore con cui mantengono i controlli finanziari.

Questa trasformazione rivoluzionerà il modo in cui le organizzazioni affrontano la resilienza digitale:

- *Funzionalità di ricostruzione potenziate dall'intelligenza artificiale:* I futuri sistemi di Ricostruzione utilizzeranno l'AI per identificare automaticamente la perdita della configurazione, prevedere potenziali scenari di guasto e condurre test di caos sistematici che anticipano nuovi vettori di attacco prima che vengano implementati. Questi sistemi di ripristino agentici lavoreranno insieme agli operatori per assumere autonomamente compiti di routine, migliorare le decisioni umane e automatizzare i flussi di lavoro.
- *Risposte Veloci:* Man mano che gli attacchi accelerano, le capacità di Ricostruzione devono accelerare di conseguenza. Le organizzazioni implementeranno sistemi di ripristino potenziati dall'AI progettati per eseguire il ripristino completo dell'ambiente più velocemente di quanto gli agentic attackers possano adattare le loro strategie.
- *Vantaggio Competitivo:* Le organizzazioni che possono dimostrare un ripristino rapido e affidabile otterranno significativi vantaggi competitivi. I clienti e i partner preferiranno i fornitori che possono dimostrare una continuità del servizio affidabile. Nei settori regolamentati, le capacità di Ricostruzione dimostrate diventeranno un requisito per mantenere licenze e certificazioni.

Le organizzazioni che adottano oggi la funzione di Ricostruzione (Rebuild) — partendo dall'operatività minima e scalando verso una copertura completa — diventeranno quelle che non solo sopravvivranno agli attacchi di domani, ma ne emergeranno più forti. Trasformeranno gli incidenti informatici da disastri che minacciano l'azienda in sfide operative gestibili.

Dal dubbio alla certezza: il tuo percorso verso un futuro resiliente

La scelta che ogni organizzazione deve affrontare è chiara: continuare a sperare che i metodi tradizionali di backup e ripristino siano sufficienti contro le minacce moderne o iniziare a costruire una capacità di Ricostruzione (Rebuild) che fornisca una fiducia reale.

L'approccio di operatività minima rende questa scelta attuabile. Inizia con un singolo sistema business-critical. Implementa snapshot PITR e automazione RaC. Conduce test di caos per validare il ripristino sotto stress. Misura e dimostra i risultati.

Il successo con un sistema crea le basi per un'espansione sistematica. Ogni sistema aggiuntivo beneficia della crescente esperienza organizzativa, dei processi comprovati e dell'automazione stabilita. Il percorso dalla speranza di backup alla fiducia nella ricostruzione accelera man mano che le capacità maturano.

Per prima cosa testa l'operatività minima, quindi espandila sistematicamente. Ripristina con fiducia attraverso capacità di Rebuild dimostrate. Favorisci la resilienza per ottenere un vantaggio competitivo.

Le minacce informatiche di domani saranno più sofisticate, più persistenti e più devastanti rispetto agli attacchi di oggi. Le organizzazioni che attendono soluzioni perfette o condizioni ideali si troveranno impreparate quando la sopravvivenza dipenderà dalla velocità e dall'affidabilità del ripristino.

Il tuo percorso inizia con la comprensione dei sistemi business-critical e l'implementazione del framework di operatività minima. La tecnologia esiste. Le metodologie sono state provate. L'unica domanda è se inizierai ora o aspetterai fino a quando il prossimo attacco ticostringerà ad agire.

Scegli di avere fiducia nelle tue capacità di ripristino. Opta per Rebuild come strategia per affrontare le incertezze del futuro. Decidi di crescere nonostante le sfide, trasformando le minacce in opportunità di crescita.

Note sull'Autore

Govind Rangasamy è fondatore e CEO di Appranix, ora parte di Commvault, e un autore riconosciuto dal Forbes Technology Council. Con una lunga esperienza come imprenditore nella gestione del cloud aziendale, Govind ha fondato Appranix per innovare i modelli di resilienza tradizionali, considerati inadeguati per le moderne applicazioni cloud distribuite e dinamiche. È un esperto riconosciuto nel campo della resilienza cloud e collabora regolarmente con Forbes, partecipando inoltre a podcast e conferenze come relatore.