eBOOK

Manuale di preparazione al Cyber Recovery

SCOPRI COME RIMANERE RESILIENTE
DI FRONTE ALLE SFIDE

Commvault®

INDICE

I team di sicurezza, IT e operations di molte organizzazioni hanno considerato cyber recovery e disaster recovery come la stessa cosa. Tuttavia, l'emergere del cyber recovery a seguito di recenti incidenti ha evidenziato alcune particolarità rispetto alla pratica tradizionale del disaster recovery. La diversità delle strategie, delle metodologie e delle procedure utilizzate dagli aggressori ha dimostrato la necessità di considerare i piani per la cyber recovery:

- **Imprevedibilità e minacce in evoluzione:** A differenza delle catastrofi naturali, gli attacchi informatici sono intenzionali e gli aggressori sono abili nel coprire le proprie tracce. Pertanto, è complesso determinare l'inizio dell'attacco, i sistemi colpiti e l'entità dei danni.
- **Attacchi secondari:** Durante il processo di ripristino, gli aggressori hanno inserito del codice che consentiva loro di lanciare attacchi successivi o hanno creato backdoor persistenti che si attivavano automaticamente dopo il ripristino.
- **Backup compromessi:** In alcuni casi, gli aggressori hanno preso di mira i backup proprio per rendere inefficaci gli sforzi di ripristino. Questo rende più reale la necessità di pagare un riscatto per recuperare i dati di produzione.
- **Limiti di tempo**: Le imprese sono spesso sottoposte a una forte pressione per riprendersi velocemente dopo un attacco informatico. È stato dimostrato che il tempo di inattività può costare alle aziende in media 14.056 dollari al minuto, aumentando a 23.750 dollari per le grandi organizzazioni con più di 10.000 dipendenti. E inoltre, un ripristino fatto in fretta può portare al recupero di sistemi già compromessi, aggravando ulteriormente i danni
- **Utilizzo delle risorse:** Il processo di recupero dei dati può essere molto impegnativo e richiedere l'intervento di team specializzati in ambito informatico, sicurezza, legale e, a volte, anche delle forze dell'ordine. Ciò può mettere a dura prova le risorse limitate di un'azienda e potrebbe distogliere l'attenzione dei team di sicurezza e operativi da altre possibili minacce informatiche.

Per affrontare queste difficoltà, le aziende possono integrare gli elementi essenziali del disaster recovery nel loro piano di cyber recovery, in modo da prevedere e gestire efficacemente eventuali attacchi.

Il presente manuale ha lo scopo di accompagnarti nella preparazione per il recupero dei dati, fornendo le nozioni, le idee e le procedure essenziali per creare il piano, seguendo gli schemi più comunemente adottati.

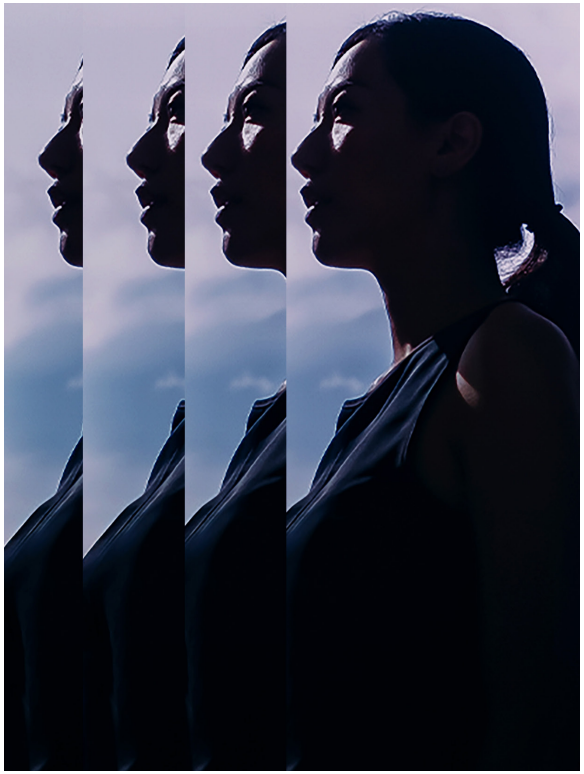
[1] Enterprise Management Associates, "IT outages: 2024 costs and containment," Valerie O'Connell, Research Director, April 2024.

NIST CYBERSECURITY FRAMEWORK COME GUIDA

Il Cybersecurity Framework del National Institute of Standards and Technology (NIST CSF) è da tempo una guida per i team di sicurezza per costruire e allineare i programmi di sicurezza e difendersi dalle minacce informatiche nuove e in evoluzione.

Per ottenere un recupero informatico efficace, è consigliabile seguire il framework Identify, Detect, Protect, Respond, and Recover e utilizzare ciascun elemento in modo appropriato.

1. **Identificare.** Conoscere i dati, compresi quelli sensibili/critici, dove si trovano e chi ne è responsabile.
2. **Rilevare.** Utilizzare i controlli di sicurezza e la tecnologia per osservare ciò che accade all'ambiente e ai dati.
3. **Proteggere.** Implementare meccanismi per bloccare i dati sensibili o critici e prepararli per il ripristino.
4. **Rispondere**. Eliminare l'aggressore dall'ambiente e rimuovere o proteggere il vettore di attacco utilizzato per infiltrarsi nell'organizzazione. Se non è possibile farlo rapidamente, preparare un nuovo spazio di lavoro intatto e non compromesso da ripristinare e utilizzare per continuare le operazioni.
5. **Recuperare.** Ricostruire una versione non compromessa dell'intero ambiente, compresi i dati, le applicazioni e l'infrastruttura.



PREPARARSI ALL'IMPREVISTO

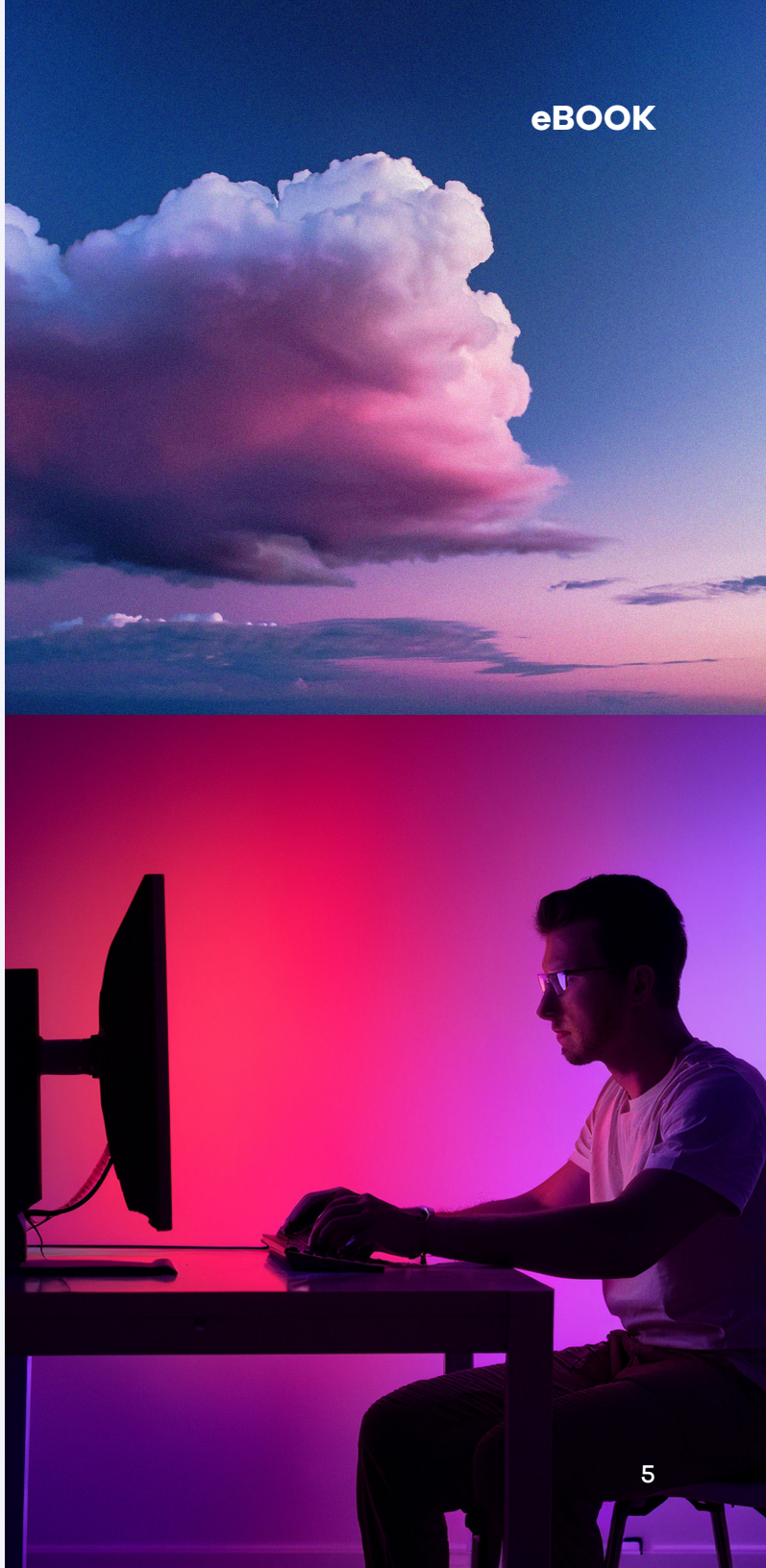
Per loro stessa natura, gli incidenti informatici sono spesso attacchi furtivi orchestrati dietro le quinte per giorni o settimane prima che si verifichi la distruzione o il caos.

194 giorni, o più di 6 mesi

il tempo medio di permanenza - la quantità di tempo in cui un attaccante è effettivamente all'interno di un'organizzazione durante un attacco.[1]

Le organizzazioni hanno a lungo condotto test di penetrazione per evidenziare aree in cui le loro difese sono deboli ed esercitazioni di simulazione per testare il ripristino dopo un disastro. Ma data la variabilità degli attacchi informatici, la pratica deve tenere conto del fatto che quasi nulla può essere implicitamente considerato attendibile in uno scenario di vero recupero informatico.

I backup devono essere scansionati per rilevare malware persistenti. L'infrastruttura deve essere pulita per confermare la presenza solo di utenti autorizzati. E le applicazioni e i dati devono essere controllati per rilevare eventuali backdoor e ripristinati a uno stato precedente all'attacco (o all'infiltrazione).



[1] Cost of a Data Breach Report 2024, IBM.

MINIMA VIABILITÀ (OPERATIVITA' MINIMA): IL PRIMO PASSO VERSO IL RECUPERO INFORMATICO

Una volta che la tua azienda è stata colpita da un attacco informatico, sei sotto una pressione enorme per tornare alla normalità il più presto possibile. Il modo migliore per riprendere le operazioni? Ripristinare l'operatività minima (minimum viability) - gli asset più critici necessari per mantenere la continuità aziendale. In questo modo, puoi continuare a svolgere gli aspetti più vitali della tua organizzazione mentre è in corso un ripristino completo.

Una volta identificati i sistemi, i processi e i dati più critici che ti permetteranno di tornare alla minima viabilità, dovrai creare un piano per come li ripristinerai in caso di incidente. È necessario comprendere l'impatto dei tempi di inattività e testare e aggiornare il piano secondo le necessità. Leggi La Guida alla Minimum Viability per saperne di più sui passaggi per ripristinare le operazioni aziendali e sulle pratiche consigliate.

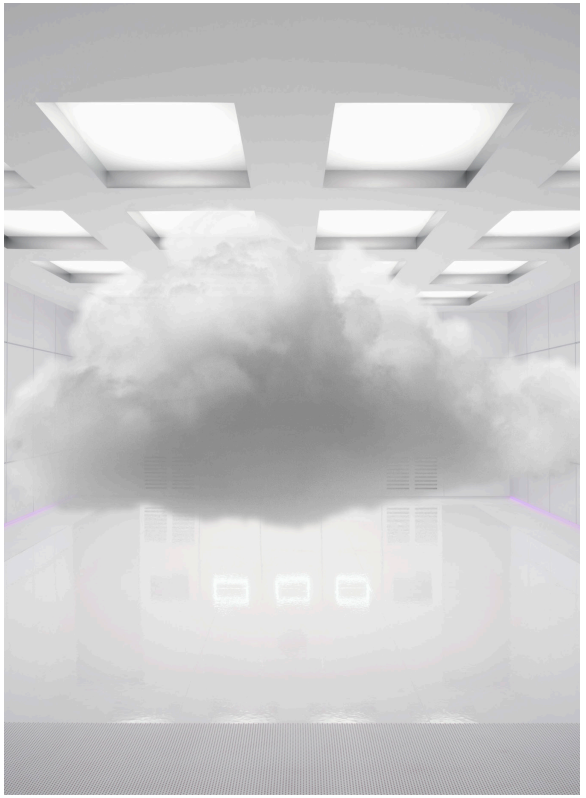
CYBER RECOVERY PIÙ VELOCE E COMPLETO

Commvault offre soluzioni per proteggere, testare e ripristinare i dati, le applicazioni e i carichi di lavoro, garantendo un recupero completo e una vera resilienza informatica.

Commvault® Cloud Cleanroom™ Recovery consente di testare e ripristinare in un ambiente cloud sicuro, on-demand e basato sul cloud. È possibile ripristinare facilmente applicazioni e dati e condurre analisi forensi dopo un evento. Avrai a disposizione un ambiente di ripristino isolato per la continuità aziendale in caso di attacco.

Commvault Cloud Rewind™ abilita il ripristino quasi istantaneo e scrive automaticamente il codice per recuperare i dati e ricostruire le applicazioni, permettendoti di tornare operativo entro pochi minuti da un guasto - il tutto senza la necessità di intervento manuale.

Commvault Cloud per Active Directory Enterprise Edition offre un ripristino rapido per gli ambienti AD e Entra ID. Aiuta ad automatizzare e orchestrare il ripristino di AD a livello di foresta dopo un incidente, consentendoti di tornare rapidamente alla minimum viability (operatività minima).



eBOOK

Una certezza nella sicurezza informatica: gli attori malevoli continueranno a innovare per trovare vulnerabilità. Rimani un passo avanti con un piano e una strategia di cyber recovery ben ponderati per proteggere i tuoi asset e mantenere la continuità aziendale di fronte alle minacce.

Scopri di più su: **www.commvault.com/minimum-viability**

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®