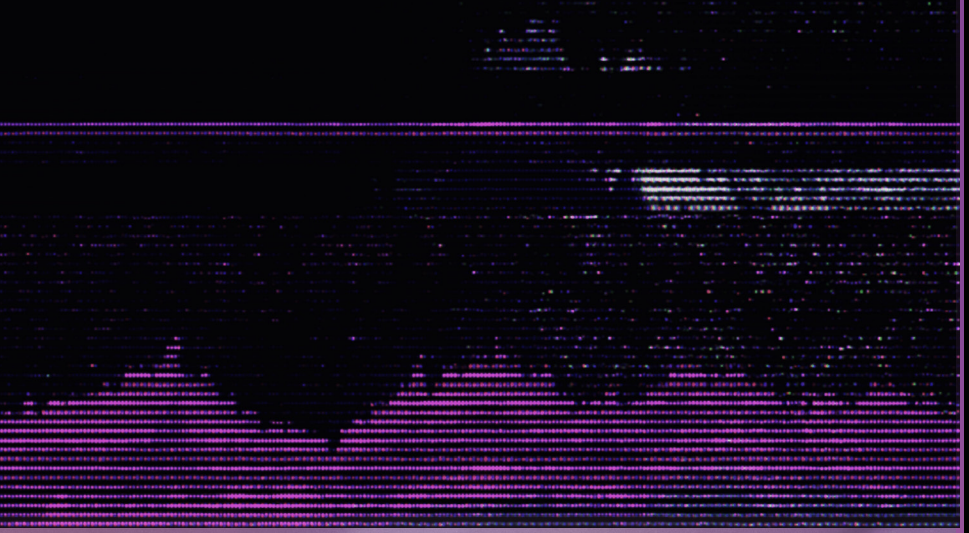


Commvault

eBOOK

Oltre il Disaster Recovery

PERCHÉ È NECESSARIA UNA STRATEGIA DIVERSA QUANDO SI VERIFICANO ATTACCHI INFORMATICI

SOMMARIO

DISASTER RECOVERY

È necessario un piano di disaster recovery per gestire eventi prevedibili come guasti hardware o disastri naturali come incendi e inondazioni. In genere, questi incidenti non sono intenzionali e non prendono di mira attivamente i dati.

Il disaster recovery di solito si attiene a un piano predefinito con passaggi stabiliti per ripristinare rapidamente i sistemi. Il ripristino dai backup consente di tornare online anche se alcuni dati sono andati persi. Questo processo mira a garantire la continuità aziendale, a ridurre al minimo l'impatto a lungo termine e a proteggere i dati critici.

CYBER RECOVERY

Il cyber recovery interviene in caso di attacchi dannosi come ransomware o violazioni dei dati, in cui gli aggressori cercano attivamente di danneggiare i sistemi e corrompere i dati. Può trattarsi di un sottoinsieme di dati o dell'intera infrastruttura, compreso un sito di failover per il disaster recovery.

I cyberattacchi spesso comportano indagini e bonifiche prima del ripristino, il che può allungare i tempi. È necessario contenere l'attacco e assicurarsi che non rimangano tracce di exploit. Ogni elemento dell'ambiente, dall'hardware ai dati e ai backup, deve essere esaminato per verificare la presenza di virus prima del ripristino, poiché gli aggressori potrebbero aver nascosto malware o alterato i file di backup. È necessario ridurre al minimo i danni, prevenire la perdita di dati e preservare la sicurezza.

CYBER RECOVERY–READY DESIGN SCOPE

SCENARI

Il cyber recovery in genere ha esigenze diverse rispetto ai piani di disaster recovery/continuità aziendale

ELEMENTI	DISASTER RECOVERY/ CONTINUITÀ AZIENDALE	CYBER RECO-VERY
COMPROMISSIONE	Perdita dell'operatività dell'intero sito	Dati, reti, sicurezza
RECOVERY	Failover/back RTO, ricostruzione	Ripristino selettivo per la riparazione
RISORSE	Full availability stack	Convalida, ripristino, ricostruzione
PIANIFICAZIONE	Costante	Elastica

Queste strategie possono essere combinate tra loro in modo da far convergere le risorse e i processi.

ORGANIZZAZIONE

Il Cyber Recovery implica la collaborazione e la condivisione di responsabilità in tutta l'organizzazione (persone, processi)

L'integrazione e l'automazione delle notifiche, delle azioni informate e dei flussi di lavoro continui tra i team possono accelerare i risultati.

FUNZIONALITÀ

I requisiti di cyber recovery dipendono dagli obiettivi dell'organizzazione

- Backup vault sicuri, isolati e immutabili
- Rilevamento precoce di pattern sospetti
- Analisi informatica e sanificazione dei dati
- Convalida automatica del ripristino
- Ripristino rapido e pianificato

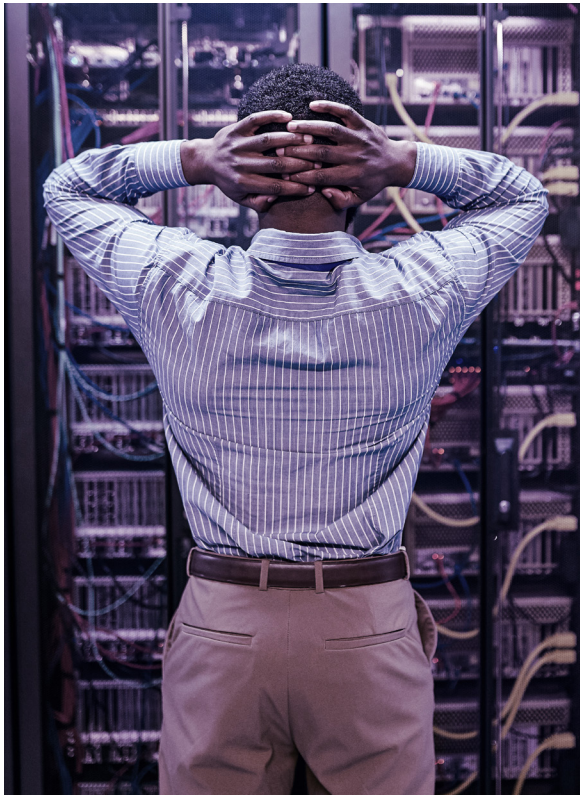
DISASTER RECOVERY I TEST NON BASTANO

I test di disaster recovery sono importanti, ma il cyber recovery è decisamente più completo. Sebbene entrambi mirino a ripristinare la funzionalità operativa dopo le interruzioni, alcune differenze fondamentali richiedono risposte distinte. I piani di disaster recovery tradizionali faticano ad affrontare in modo efficace le sfumature delle minacce e le complessità degli attacchi informatici.

Ecco perché:

- Natura della minaccia
- Ambito e obiettivo
- Metodi e strumenti
- Integrità e vulnerabilità dei dati

Pertanto, sebbene i piani di disaster recovery forniscano una base preziosa per la risposta agli incidenti, è pericoloso farvi affidamento di fronte a un attacco informatico. Un piano di cyber recovery dedicato, supportato da strumenti specializzati, personale e test frequenti, è essenziale per mitigare i rischi e le complessità specifiche di questi attacchi malevoli.



I TEST DI CYBER RECOVERY SONO FONDAMENTALI

Il test di cyber recovery è l'esecuzione pratica (o test operativo) del ripristino di un'applicazione e dei suoi dati da un backup. È il tipo di processo di ripristino che si verifica in caso di incidente informatico ed è il processo raccomandato dal NIST. I test di disaster recovery e di cyber recovery[1] svolgono ciascuno il proprio ruolo negli scenari applicabili, ma il cyber recovery è molto più completo.

I test di cyber recovery consentono la resilienza dei sistemi e dei dati e la continuità aziendale. Il ripristino delle applicazioni e dei dati critici può essere complesso e problematico. I test di cyber recovery aiutano a scoprire e risolvere gli errori quando la posta in gioco è bassa.

Grazie ai test, i team potranno esercitarsi e acquisire dimestichezza nel recupero di applicazioni e dati critici quando si verifica un incidente informatico. In effetti, il NIST raccomanda di "eseguire, proteggere, manutenere e testare i backup dei dati" perché "è meglio individuare un problema imprevisto durante i test che durante un vero e proprio evento informatico".[1] Ma la realtà è che pochissime organizzazioni eseguono test completi, frequenti e riusciti.

[1] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf

204 GIORNI

Tempo medio di permanenza di un hacker in un'azienda[2]

IL 92%

delle aziende che pagano il riscatto non recupera tutti i dati[4]

Gli hacker iniziano a utilizzare il lateral movement entro

84 MINUTI

da un attacco[3]

[2] https://www.ibm.com/reports/data-breach
[3] https://www.crowdstrike.com/resources/reports/threat-hunting-report/
[4] https://www.sophos.com/en-us/content/state-of-ransomware

IL SUPPORTO DI COMMVAULT CLOUD

È possibile ottenere la resilienza informatica proattiva con **Commvault® Cloud Auto Recovery**, riducendo al minimo l'impatto delle minacce ai dati su tutti i carichi di lavoro e promuovendo la continuità aziendale. Auto Recovery offre un ripristino informatico proattivo automatizzato attraverso una protezione dei dati a più livelli, per ridurre i tempi di ripristino durante i cyberattacchi e altri disastri. Con un Recovery Time Objective (RTO) potenziale quasi in tempo reale e Recovery Point Objectives (RPO) inferiori al minuto, Auto Recovery riduce al minimo l'impatto delle minacce ai dati su tutti i carichi di lavoro cloud, on-premise e SaaS per la continuità aziendale.

Commvault® Cloud Cleanroom™ Recovery offre un ambiente di ripristino isolato, pulito e sicuro, a prezzi accessibili e su richiesta, per testare i piani di ripristino informatico, condurre analisi forensi sicure e garantire una continuità aziendale ininterrotta.

Le continue minacce informatiche e il ransomware introducono rischi esistenziali e creano confusione e ansia a livello organizzativo. Cleanroom Recovery offre un banco di prova unico per convalidare l'efficacia dei piani, delle tecnologie e dei processi di ripristino informatico.

Il Cleanroom Recovery offre un ambiente sicuro in cui i dati e le risorse critiche sono isolati e protetti dagli attacchi. I responsabili della sicurezza e dell'IT possono ottenere informazioni preziose sugli attori sconosciuti delle minacce, rafforzare le loro strategie e contribuire a garantire una continuità aziendale ininterrotta.

DISASTER RECOVERY

SFIDA

Disaster recovery per la continuità operativa e il ripristino del sito in caso di disastri naturali o blackout.

SOLUZIONE

Commvault® Cloud Auto Recovery è la piattaforma di replica dei dati più flessibile e conveniente.

- Funzionalità RPO inferiori al minuto
- Possibilità di RTO vicino allo zero per il recupero istantaneo dei dati
- Trasformazione dei dati durante la replica
- Dall'orchestrazione al disaster recovery in un clic e viceversa
- Fire drill di disaster recovery per la conferma di un pronto recupero

CYBER RECOVERY

SFIDA

Cyber recovery per recuperare i dati e le applicazioni colpite da malware dopo un incidente informatico.

SOLUZIONE

Commvault® Cloud Cleanroom™ Recovery offre un ripristino semplice, sicuro e rapido delle applicazioni.

- Stabilire e automatizzare le cleanroom per il ripristino
- Raggruppamento logico di carichi di lavoro eterogenei
- Scansione sicura con strumenti integrati e personalizzabili
- Dipendenza dal ripristino e azioni personalizzate
- Control plane Commvault accessibile nel clean site
- Monitoraggio, reporting e auditing incentrati sul ripristino

Sebbene un piano di disaster recovery sia essenziale per proteggere l'infrastruttura aziendale, non si potrà essere completamente protetti se non si dispone anche di un piano di cyber recovery e di una strategia di test. Sono strumenti fondamentali per mantenere al sicuro sia i propri dati che la propria reputazione di fronte ad attacchi efferati.

eBOOK

Scopri di più su come Commvault può aiutare a proteggere la tua organizzazione e ricevi una demo di Commvault® Cloud Cleanroom™ Recovery.

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

Commvault®