DELL Technologies

Solution Brief

Dell EMC PowerProtect Cyber Recovery

Protezione moderna e comprovata dei dati critici da ransomware e attacchi informatici distruttivi

PERCHÉ SCEGLIERE CYBER RECOVERY?

L'obiettivo degli attacchi informatici è distruggere, rubare o in qualche modo compromettere i dati più importanti, inclusi i backup. Proteggere e ripristinare i dati critici secondo un approccio sicuro orientato all'integrità è fondamentale per riprendere il normale svolgimento delle attività aziendali in seguito a un attacco. L'azienda sarebbe in grado di sopravvivere? Di seguito sono descritti i cinque componenti alla base di una soluzione di ripristino dagli attacchi informatici moderna e comprovata:

Isolamento e governance dei dati Un ambiente di data center isolato, scollegato dalle reti aziendali e di backup e con limitazioni di accesso per utenti diversi da quelli con autorizzazione adeguata.

Copia automatizzata dei dati ed air gap Creazione di copie di dati non modificabili all'interno di un vault digitale protetto e processi che generano un air gap operativo tra l'ambiente di produzione/backup e il vault.

Analisi e strumenti intelligenti Apprendimento automatico e indicizzazione completa dei contenuti sulla base di analisi efficaci, con tutta la sicurezza del vault, oltre a controlli automatizzati dell'integrità volti a individuare i dati interessati da malware e strumenti per un'eventuale correzione.

Ripristino e correzione Flussi di lavoro e strumenti per eseguire il ripristino dopo un incidente utilizzando processi di restore dinamici e procedure DR esistenti.

Pianificazione e progettazione della soluzione Istruzioni per la selezione di data set, applicazioni e altri asset critici al fine di stabilire gli obiettivi RTO/RPO e semplificare il ripristino.

Attacchi informatici: il nemico delle aziende con un approccio basato sui dati

I dati sono la "valuta" dell'Internet Economy, nonché asset critici da proteggere e rendere disponibili da un momento all'altro, garantendone al contempo la riservatezza. Il mercato globale di oggi è caratterizzato da un flusso costante di dati su reti interconnesse, dove le iniziative di Digital Transformation mettono a rischio i dati più sensibili.

In questo modo, i dati delle organizzazioni diventano un obiettivo appetibile dei criminali informatici, il cui scopo è lucrare a spese degli utenti.

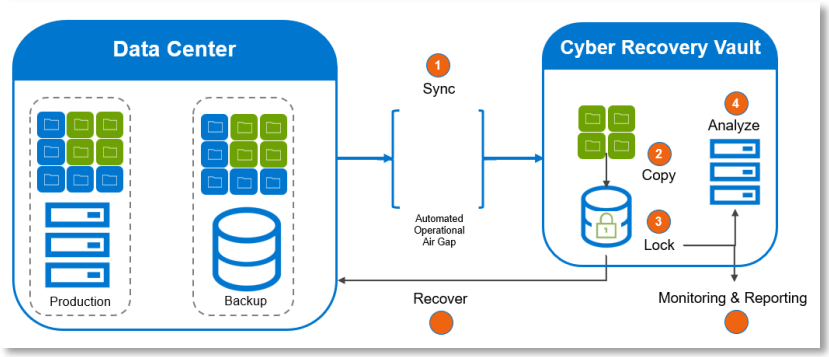
Il crimine informatico è stato definito come il "più grande trasferimento di ricchezza della storia" e al centro di tutto ciò vi sono i dati. Secondo le stime di Accenture, nei prossimi 5 anni il crimine informatico metterà a rischio un valore globale pari a 5,2 trilioni di dollari.[i]

A prescindere dal settore o dalle dimensioni di un'azienda, gli attacchi informatici espongono continuamente organizzazioni ed enti pubblici a una serie di rischi, tra cui compromissione dei dati, perdita di entrate dovuta a downtime, danno alla propria reputazione e ingenti sanzioni dovute al mancato rispetto delle normative. Per le aziende, il costo annuo medio del crimine informatico ha raggiunto i 13 milioni di dollari nel 2018, registrando un aumento del 72% negli ultimi 5 anni.[ii]

Implementare una strategia di ripristino dagli attacchi informatici è diventato pressoché obbligatorio per le aziende e gli enti della pubblica amministrazione. Secondo uno studio condotto da Marsh e Microsoft nel 2019, gli attacchi informatici sono una delle principali priorità nella gestione dei rischi per il 79% dei dirigenti a livello globale.[iii]

Cosa si può quindi fare per proteggere l'organizzazione e i suoi dati?

La soluzione: PowerProtect Cyber Recovery

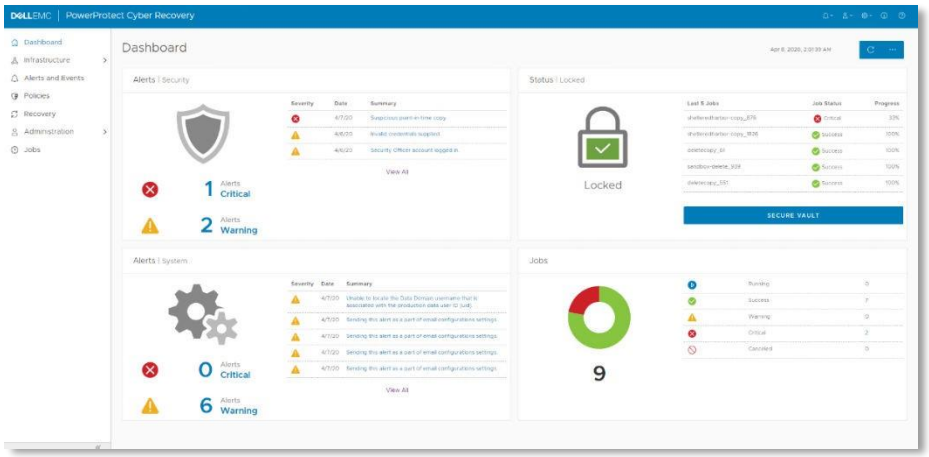


Al fine di ridurre i rischi per il business associati agli attacchi informatici e creare un approccio più cyber-resiliente alla protezione dei dati, è possibile modernizzare e automatizzare le strategie di ripristino e continuità aziendale, oltre a sfruttare gli strumenti più avanzati per rilevare eventuali minacce informatiche e difendersi da queste ultime.

Dell EMC PowerProtect Cyber Recovery offre una soluzione di protezione moderna, comprovata e intelligente per isolare i dati critici, identificare le attività sospette e accelerare il ripristino dei dati, affinché le aziende possano riprendere rapidamente le loro normali attività.

PowerProtect Cyber Recovery: protezione moderna, comprovata e intelligente per ridurre i rischi dovuti alle minacce informatiche

- **Vault Cyber Recovery:** il vault di PowerProtect Cyber Recovery offre più livelli di protezione per fornire resilienza contro gli attacchi informatici, anche in caso di minaccia interna. Questo sistema, che richiede credenziali di sicurezza separate e autenticazione a più fattori per l'accesso, consente di spostare i dati critici dalla superficie di attacco, isolandoli fisicamente in una zona protetta del data center.
  Ulteriori misure di protezione includono la creazione automatizzata di un air gap operativo per isolare la rete e l'eliminazione delle interfacce di gestione che potrebbero essere compromesse.
  PowerProtect Cyber Recovery automatizza la sincronizzazione dei dati tra i sistemi di produzione e il vault, creando copie non modificabili con policy di retention bloccate. In caso di attacco informatico, è possibile identificare rapidamente una copia pulita dei dati, ripristinare i sistemi critici e riprendere la normale attività.



- **CyberSense:** completamente integrato in PowerProtect Cyber Recovery, CyberSense aggiunge un livello di protezione intelligente per agevolare la ricerca dei dati danneggiati nel caso in cui l'attacco arrivasse al data center. Questo innovativo approccio offre funzionalità di indicizzazione completa dei contenuti e utilizza l'apprendimento automatico per analizzare più di 100 statistiche basate sui contenuti e rilevare eventuali segni di danneggiamento dovuti a ransomware. CyberSense rileva i dati danneggiati con un'attendibilità fino al 99,5%, aiutando le aziende a identificare le minacce, diagnosticare i vettori di attacco e proteggere i contenuti business-critical, il tutto con la sicurezza del vault.
- **Ripristino e correzione:** PowerProtect Cyber Recovery esegue procedure automatizzate di restore e ripristino per riportare online i sistemi critici in modo rapido e sicuro. Come parte di PowerProtect Data Manager, Cyber Recovery consente ai clienti che utilizzano Dell EMC NetWorker di automatizzare il ripristino dal vault. Insieme al suo ecosistema di partner, Dell EMC offre una metodologia completa per proteggere i dati, valutare eventuali danni ed eseguire analisi forensi al fine di correggere o ripristinare i sistemi e rimuovere eventuali malware.
- **Pianificazione e progettazione della soluzione:** con i Dell EMC Advisory Services opzionali è possibile stabilire quali sistemi business-critical proteggere e creare mappe di dipendenza per le applicazioni e i servizi associati, oltre all'infrastruttura necessaria per ripristinarli. Questi servizi prevedono anche la definizione dei requisiti di ripristino e di progettazioni alternative. In più, identificano le tecnologie per analizzare, ospitare e proteggere i dati, insieme alla creazione di un business case e alla definizione delle tempistiche di implementazione.

Per proteggere i dati più importanti dagli attacchi informatici servono soluzioni moderne e comprovate. PowerProtect Cyber Recovery consente di identificare con certezza e ripristinare i dati, affinché le aziende possano riprendere le loro normali attività in seguito a un attacco informatico.

Ulteriori informazioni su Dell EMC PowerProtect Cyber Recovery

Contatta un esperto Dell EMC

[Studio di Accenture sui costi della criminalità informatica, 2019]
[Studio di Accenture sui costi della criminalità informatica, 2019]
[Studio di Marsh e Microsoft sulla percezione del rischio informatico a livello globale, 2019]