SHOWCASE ESG

La cyber-resilienza è fondamentale per lo storage mission-critical

Data: ottobre 2022 Autori: Scott Sinclair, Practice Director, e Monya Keane, Senior Research Analyst

ABSTRACT: il panorama dell'IT è cambiato. Man mano che i dati acquisiscono un valore sempre più elevato come asset, le minacce informatiche diventano sempre più pervasive. La cyber-resilienza deve quindi essere un principio chiave alla base della scelta dello storage mission-critical. Grazie a PowerMax, Dell Technologies si è inoltre affermata come leader nello storage mission-critical creando e integrando funzionalità di cyber-resilienza essenziali direttamente in questi sistemi.

Panoramica

I dati sono una risorsa aziendale cruciale ed estremamente preziosa. Secondo una ricerca ESG, il 59% delle organizzazioni intervistate identifica i dati come parte sostanziale del business e tale percentuale dovrebbe raggiungere l'81% in due anni.[1] Il ruolo di un'infrastruttura di storage mission-critical è quello di preservare, proteggere e fornire i dati alla base dei carichi di lavoro e delle applicazioni, semplicemente senza downtime.

Per decenni, implementare lo "storage mission-critical" è stato sinonimo di offrire le prestazioni e la scalabilità richieste, garantendo al contempo una disponibilità always-on per la protezione da guasti dei componenti e del sito, errori degli utenti e calamità naturali. Ora, gli attacchi malevoli sono sempre più prevalenti. I principi chiave alla base della scelta dello storage mission-critical, quindi, devono andare oltre le funzionalità tradizionali per includere anche il miglioramento del livello di cyber-resilienza di un'organizzazione.

Dell Technologies, leader nello storage aziendale, continua a sviluppare la sua piattaforma di storage di punta, PowerMax, per soddisfare le esigenze mission-critical degli ambienti IT più complessi. Il recente sforzo di innovazione di Dell è stato rivolto a integrare nella linea PowerMax una serie di solide funzionalità per migliorare il livello di cyber-resilienza di qualsiasi organizzazione interessata a proteggere in modo più efficiente i dati e le applicazioni cruciali, preservando la reputazione del marchio e raggiungendo il successo a lungo termine.

L'era delle minacce informatiche costanti alla protezione dei dati

In seguito all'aumento delle minacce informatiche, è aumentata anche la complessità dell'IT. Quasi la metà (46%) dei partecipanti alla survey ESG afferma che l'IT è oggi più complesso rispetto a due anni fa. La rapida evoluzione del panorama della sicurezza informatica (citata dal 37%) e lo sforzo per rispettare le nuove normative sulla sicurezza e sulla privacy dei dati (citati dal 32%) sono stati generalmente considerati due fattori determinanti di tale complessità IT.[2]

Purtroppo, le organizzazioni hanno attualmente difficoltà ad assumere talenti di sicurezza informatica sufficientemente qualificati per prevalere su tale complessità in modo diretto. Il quarantotto percento delle organizzazioni intervistate lamenta l'insufficienza di specialisti di sicurezza informatica nel personale: è l'area di carenza di competenze nell'IT aziendale citata più spesso in questo momento.[3]

[1] Fonte: report di ricerca ESG, *Data Infrastructure Trends*, novembre 2021.
[2] Fonte: risultati completi della survey ESG, *2022 Technology Spending Intentions Survey*, novembre 2021.
[3] Ibid.

Prevalenza di ransomware e malware

Nel panorama delle minacce che le aziende devono affrontare, gli attacchi ransomware e malware esterni sono diventati praticamente inevitabili. In una recente survey di ricerca ESG condotta sui professionisti IT e della sicurezza informatica che supervisionano le tecnologie e i processi aziendali associati alla protezione ransomware, il 79% ha riferito di aver subito un tentativo di attacco ransomware negli ultimi 12 mesi. Di questi, il 30% ha inoltre affermato che tali attacchi si verificano ogni settimana o ancora più frequentemente.[4]

Il 73% delle organizzazioni che hanno subito un tentativo di attacco è stato vittima di almeno un attacco riuscito. Tuttavia, in queste circostanze, pagare il riscatto non è la strategia ottimale o intelligente. Il 56% delle organizzazioni vittime di un attacco riuscito ha pagato. Tuttavia, tra quelle che hanno pagato il riscatto richiesto:

- L'**87%** ha subito ulteriori tentativi di estorsione di altro denaro. Infatti, il 61% di coloro che hanno pagato all'inizio, in definitiva, ha finito per pagare ancora più denaro successivamente.[5]
- Solo il **14%** ha recuperato il 100% dei dati, dopo aver pagato il riscatto.
- Il **61%** ne ha ottenuti indietro al massimo il 75% in seguito al pagamento.

Chiaramente, la protezione ransomware completa richiede una strategia maggiormente diversificata, che include più tecnologie e strumenti incentrati sul rilevamento, sulla prevenzione e sul ripristino.

Molte organizzazioni stanno ora modellando le proprie strategie di cyber-resilienza dopo le indicazioni fornite nel NIST Cybersecurity Framework, che consiglia alle aziende di identificare le risorse critiche, proteggerle, rilevare guasti e violazioni e pianificare la risposta e il ripristino in seguito a incidenti informatici. Un altro componente del framework NIST che le organizzazioni stanno adottando ampiamente è l'architettura Zero Trust, che accantona il concetto di edge della rete di protezione a favore di una filosofia "Never Trust, Always Verify". In questo modello, la configurazione di sicurezza degli utenti (anche del personale che lavora all'interno dell'organizzazione) deve essere ripetutamente e regolarmente convalidata prima che tali utenti possano accedere ad applicazioni/dati.

I sistemi di storage devono assolutamente rientrare nell'ambito di questo approccio alla sicurezza informatica. Dopo tutto, il componente dell'infrastruttura più comune a cui sono mirati gli attacchi ransomware è l'hardware di storage, secondo la ricerca ESG. È stata la prima risposta per il 40% degli intervistati.

In che modo lo storage mission-critical migliora la resilienza ransomware

Gli attacchi ransomware sono incentrati sull'accesso ai dati aziendali importanti, quindi sulla loro crittografia. Molte strategie di cyber-resilienza si basano su strumenti e tecnologie con focus sulla **prevenzione** delle minacce, attraverso la protezione, e il **rilevamento** precoce di eventuali attacchi riusciti. Tuttavia, con il ransomware, è importante concentrarsi anche sul **ripristino accelerato**.

I sistemi di storage mission-critical risiedono in un punto del percorso dati ideale per supportare il ripristino rapido dei dati in seguito a un attacco. Ad esempio, con l'aumento degli attacchi ransomware riusciti, alcuni sistemi di storage hanno potuto sfruttare le rispettive funzionalità progettate per supportare il ripristino rapido, proteggendo e quindi proponendo copie dei volumi di dati sicure e immutabili.

[4] Fonte: report di ricerca ESG, *The Long Road Ahead to Ransomware Preparedness*, giugno 2022. Se non diversamente indicato, tutti i riferimenti alla ricerca ESG riportati in questa showcase sono tratti dal report di ricerca.
[5] Fonte: risultati completi della survey ESG, *The Long Road Ahead to Ransomware Preparedness*, giugno 2022.

Questo tipo di supporto è estremamente utile per accelerare il ripristino. Le snapshot possono essere rapidamente identificate come volumi "validi" e ripristinate velocemente dall'IT in modo da eseguire il restore dei data set al loro precedente stato originario. Tuttavia, per gli ambienti applicativi mission-critical, *la tecnologia di storage non può fermarsi a questo*.

Dell PowerMax può migliorare il livello di cyber-resilienza di un'organizzazione

I nomi dei prodotti sono cambiati e le funzionalità sono aumentate nel corso degli anni, tuttavia i sistemi di storage dell'infrastruttura mission-critical Dell Technologies hanno guidato questo settore dalla fine degli anni '80, quando lo storage aziendale è stato definito categoria IT separata da EMC. Oggi, Dell PowerMax offre più funzionalità progettate per soddisfare i requisiti di utilizzo intensivo dei carichi di lavoro mission-critical, tra cui:

- Un'architettura scale-out multi-controller all-NVMe per prestazioni estreme e coerenti su vasta scala.
- Eccezionale consolidamento dei carichi di lavoro, con supporto per diversi ambienti applicativi di blocchi e file che includono carichi di lavoro mainframe, sistemi bare metal, VM, container e altro ancora.
- I massimi livelli di sicurezza, disponibilità e resilienza. PowerMax offre una disponibilità del 99,9999% con crittografia dei dati end-to-end dagli host a PowerMax, crittografia dei dati inattivi e snapshot sicure; in particolare, supporta fino a *64 milioni di snapshot per array*, secondo Dell. Inoltre, il software di ripristino di emergenza Dell Symmetrix Remote Data Facility (SRDF) utilizza funzionalità di automazione e topologie avanzate per fornire una base solida per la resilienza. Con SRDF, le organizzazioni possono perfino creare un vault air-gap. All'interno di tale vault, i dati sono isolati e la connessione all'ambiente è intermittente e con elevate limitazioni.

Dell ha progettato PowerMax per la resilienza

Recentemente, Dell ha concentrato i propri sforzi sulla creazione e sull'integrazione di ulteriori funzionalità di protezione in PowerMax. Ad esempio, PowerMax è ora progettato per ambienti di sicurezza Zero Trust basati sui sette pilastri Zero Trust Dell, tra cui la protezione/sicurezza intrinseca del sistema stesso dagli attacchi tramite:

- **Funzionalità della radice di affidabilità hardware non modificabile:** queste funzionalità autenticano le modifiche hardware e software in tutti i nodi, in tutte le enclosure di supporti e nella Control Station. Le chiavi crittografiche a livello di componenti non modificabili integrate sono fisicamente fuse nella memoria da Dell Manufacturing.
- **Funzionalità della catena di affidabilità per l'avvio sicuro:** queste funzionalità stabiliscono ed estendono una "catena di affidabilità" del firmware contro i rootkit dannosi di avvio, kernel e driver. La catena di affidabilità per l'avvio sicuro utilizza l'autenticazione crittografica per i caricatori di avvio/caricamenti del firmware successivi basata su firme Dell.
- **Aggiornamenti firmware con firma digitale:** PowerMax sfrutta inoltre l'autenticazione con firma digitale Dell per la protezione da aggiornamenti firmware non autorizzati. Esegue scansioni dei componenti di nodi, supporti e Control Station utilizzando chiavi di autenticazione crittografica.

Oltre a questa progettazione affidabile, PowerMax offre funzionalità aggiuntive per migliorare la prevenzione, il rilevamento degli attacchi ransomware e altre minacce alla sicurezza informatica, nonché il ripristino in relazione a tali eventi.

Per la **prevenzione**, oltre alla sicurezza hardware integrata, PowerMax aiuta a prevenire gli attacchi grazie alla sicurezza avanzata per impedire l'accesso agli utenti non autorizzati, che include le certificazioni di Common Criteria, protezione avanzata STIG/APL e sicurezza certificata FIPS 140, nonché il supporto di meccanismi affidabili di controllo degli accessi di amministrazione, come:

- Autenticazione a più fattori SecurID per verificare l'identità di un amministratore.
- Supporto per smart card CAC/PIV contenente un certificato/una chiave privata per ottenere l'accesso alle risorse online del governo federale degli Stati Uniti
- Controlli degli accessi basati sui ruoli (RBAC), supporto LDAP e zDP a due attori (sono richieste due persone per eseguire comandi zDP specifici), consentendo solo agli utenti autorizzati di eseguire le operazioni designate, ad esempio il provisioning dello storage.

Per il **rilevamento**, sia l'hardware PowerMax che il software di AI Dell CloudIQ offrono il rilevamento di anomalie malware. Si tratta di avvisi di conformità basati su protocolli di avviso della sicurezza informatica, unitamente ad avvisi ed esportazioni syslog sicuri. In particolare, CloudIQ rileva rapidamente gli attacchi informatici monitorando l'utilizzo insolito dello storage PowerMax e le metriche di attività sospette. Avvisa, quindi, gli amministratori di eventuali variazioni importanti dovute alla possibile crittografia. Può inoltre monitorare continuamente l'infrastruttura di storage per identificare automaticamente i rischi per la sicurezza informatica derivanti da impostazioni di sistema non configurate correttamente e quindi fornire suggerimenti dettagliati per risolvere questi problemi.

Inoltre, per il **ripristino**, la tecnologia delle snapshot sicure di PowerMax ha portato la sicurezza e la protezione dei dati a un nuovo livello. A seconda dei Service Level Objectives dell'azienda, l'IT può configurare fino a 64 milioni di copie snapshot su ogni sistema PowerMax (vedere la Figura 1).

Figura 1. In che modo PowerMax supporta il Cyber Recovery rapido

Fonte: Dell Technologies

Questa funzionalità consente a PowerMax di supportare RPO (Recovery Point Objective) di appena pochi minuti prima della riuscita di un attacco. Inoltre, con il supporto di tutte queste snapshot, l'IT disporrà di copie sufficienti per proteggere anche gli ambienti di storage mission-critical consolidati di grandi dimensioni praticamente all'istante, ottenendo così un ripristino quasi istantaneo delle applicazioni mission-critical. Questo livello di flessibilità della protezione è rivoluzionario per gli ambienti di produzione su vasta scala. Secondo Dell, PowerMax offre il Cyber Recovery più granulare su vasta scala disponibile per ottimizzare l'RPO.

Dell può inoltre aggiungere un'opzione di vault di ripristino dagli attacchi informatici di PowerMax per le organizzazioni che richiedono un'opzione di ripristino air-gap su vault remoto (SRDF) con vaulting/ripristino coordinato per lo storage open system e mainframe. L'offerta del vault di ripristino dagli attacchi informatici di PowerMax sarà disponibile su larga scala entro la fine del mese e utilizzerà la replica remota di SRDF per la creazione di un air gap. Questa soluzione è progettata per i clienti che richiedono una copia dei dati al di fuori della rete di produzione con ripristino rapido (RTO). Sebbene i clienti PowerMax implementino questa configurazione manualmente da diverso tempo, con l'annuncio di questo mese, l'automazione dell'orchestration del deployment e i Dell Professional Services verranno integrati nel sistema per semplificare l'installazione.

Conclusioni

Dell non è di solito il primo vendor che viene in mente quando si pensa alla sicurezza. Questa percezione deve cambiare. Gli attacker malevoli stanno diventando più organizzati e le loro minacce più sofisticate. Dell ha effettuato e continua a effettuare notevoli investimenti per contrastare queste minacce, proteggere i dati e semplificare l'intera gestione della sicurezza e della resilienza.

I dati sono l'asset più critico di un'organizzazione: devono siano protetti e sempre disponibili. A minare questa disponibilità sono ransomware, malware e altri attacchi informatici. Sì, PowerMax discende da una linea di soluzioni per il supporto dei carichi di lavoro mission-critical di fascia alta. Dell si occupa di questo da molto tempo, ma le nuove funzionalità di PowerMax sono particolarmente adatte a qualunque acquirente di storage di oggi. Tutti si preoccupano dei ransomware, dei malware e di non apparire nelle prime pagine dei giornali.

E non si tratta di combattere ladri che tentano di arricchirsi. Questi hacker potrebbero semplicemente lavorare per un governo estero ed essere intenzionati a rubare la proprietà intellettuale per rafforzare la propria sicurezza nazionale o forza militare. Se riescono a crittografare i dati e a impedirne l'accesso, nessuno può immaginare quale altre azioni potrebbero compiere.

Se disponi di informazioni aziendali che non puoi assolutamente lasciare nelle mani di questi malintenzionati, avvia una conversazione con Dell per informazioni su come proteggere un'infrastruttura di storage nel modo adeguato.

Enterprise Strategy Group è una società di analisi, ricerche e strategie integrate che offre alla community IT globale servizi per contenuti Go-to-market, market intelligence e informazioni operative.

www.esg-global.com contact@esg-global.com + 1 508.482.0188