DELL Technologies

Infiltrazione dei backup: rafforzamento della sicurezza informatica e della resilienza con Dell Technologies

Executive Summary

L'infiltrazione dei backup, che sfrutta le vulnerabilità nei sistemi progettati per proteggere le informazioni critiche, rappresenta una minaccia crescente per le aziende di ogni settore. Questi attacchi compromettono i sistemi di ripristino dei dati, minando così la fiducia degli utenti e mettendo in pericolo le operazioni. Ingenti perdite finanziarie, lunghi downtime e danni alla reputazione: le ripercussioni possono essere gravi.

Dell Technologies fornisce una suite di difese end-to-end per proteggere i dati sensibili e prevenire questi attacchi, in cui figurano Dell Trusted Device, Dell Trusted Infrastructure e funzionalità di sicurezza estese integrate in tutte le nostre soluzioni. Con l'aggiunta di partnership strategiche e Professional Services, Dell aiuta le organizzazioni a stabilire framework resilienti di sicurezza multilivello per rilevare, contrastare e ripristinare con efficienza gli incidenti di infiltrazione dei backup.

Con l'implementazione delle soluzioni innovative e il supporto degli esperti Dell, le aziende saranno più pronte a proteggere la propria infrastruttura e a mantenere la continuità operativa.

Crescente minaccia di infiltrazione dei backup

I sistemi di backup, essenziali per la continuità aziendale, sono uno strumento essenziale per il ripristino dopo eventi informatici come ransomware o guasti hardware. Purtroppo, proprio questi punti nevralgici sono sempre più presi di mira dai criminali informatici. L'infiltrazione dei backup danneggia o elimina i dati di backup, rendendoli inaccessibili quando sono più necessari.

Queste minacce in continua evoluzione richiedono misure proattive. La mancata protezione dei sistemi di backup compromette le operazioni ed espone i dati sensibili. Le aziende di tutte le dimensioni, dalle piccole imprese alle multinazionali, sono potenziali obiettivi, con settori particolarmente a rischio, come quelli sanitario, finanziario e della produzione.

Dell Technologies riconosce l'urgenza di rafforzare gli ambienti di backup, offrendo linee guida e strumenti avanzati per contrastare questi attacchi sofisticati.

Attacchi di infiltrazione dei backup

L'infiltrazione dei backup si verifica quando i criminali informatici sfruttano le vulnerabilità nei sistemi di backup per compromettere, distruggere o crittografare i dati di ripristino critici. Per acuire le ripercussioni operative e finanziarie, questi attacchi sofisticati possono essere sferrati in concomitanza o dopo altri incidenti, come il deployment di ransomware o malware.

Come funzionano gli attacchi ai backup

1. **Violazione iniziale:** gli autori degli attacchi ottengono l'accesso non autorizzato alla rete, spesso tramite phishing, credenziali deboli o vulnerabilità senza patch.
2. **Movimento laterale:** una volta all'interno della rete, gli autori degli attacchi utilizzano degli strumenti per muoversi senza essere rilevati, puntando ai repository di backup e ai data set critici.
3. **Compromissione dei backup:** le tattiche principali includono la crittografia dei file di backup, l'eliminazione dei recovery point e il danneggiamento dei dati.

Tecniche comuni

- **Il furto di credenziali** viola gli account amministrativi per fornire un accesso completo ai sistemi di backup.
- **Il deployment di ransomware** crittografa sia i dati in tempo reale che i backup e richiede alla vittima un pagamento per la decrittografia dei dati.
- **La corruzione graduale** compromette progressivamente i backup per eludere i sistemi di rilevamento, lasciando le aziende esposte al momento di avviare il ripristino.

Tali tecniche evidenziano la complessità e la gravità di queste minacce, oltre alla necessità di attuare misure preventive.

Impatto sulle aziende

Perdite finanziarie

L'infiltrazione dei backup aumenta i costi di ripristino e il downtime, spesso raddoppiando o triplicando le spese per le risposte. Il ripristino dopo la crittografia o la compromissione dei backup può tradursi in pagamenti agli autori degli attacchi, nuove infrastrutture o costose consulenze.

Interruzione operativa

Senza backup validi, le organizzazioni devono affrontare lunghi tempi di ripristino che interrompono i servizi, ritardano i progetti e arrestano le funzioni critiche.

Ripercussioni sulla reputazione

La perdita permanente di dati o il downtime prolungato erode la fiducia delle entità interessate, danneggiando potenzialmente la redditività a lungo termine di un'azienda.

Esempio del mondo reale

Un fornitore di servizi sanitari globale ha scoperto che i backup erano stati danneggiati durante un attacco ransomware. Nonostante abbia pagato il riscatto, tre settimane di dati dei pazienti sono andate definitivamente perse, ritardando le operazioni chirurgiche e dando luogo a contenziosi legali. I costi totali di ripristino hanno superato i **$ 50 milioni.**

Il 57%
degli attacchi mirati ai backup riesce a infiltrarsi con successo nei repository di backup

Fonte: 2024, Index Engines

Statistiche allarmanti

Studi recenti stimano che, in media, le ripercussioni finanziarie della compromissione di un sistema di backup superino i **$ 4,45 milioni**[1], considerando multe, downtime e spese di ripristino. Particolarmente allarmante è la crescente frequenza di tali incidenti, con report globali che mostrano un aumento annuale del **39%** delle minacce correlate ai backup.

Contrasto alle infiltrazioni dei backup con Dell Technologies

Dell Technologies fornisce una solida suite di strumenti e servizi per affrontare le sfide specifiche poste dagli attacchi di infiltrazione dei backup, grazie alla quale le aziende possono prevenire, rilevare e ripristinare i sistemi in modo efficace.

Soluzioni per la sicurezza di server e storage

Le soluzioni di storage e server Dell offrono una resilienza senza precedenti in caso di attacchi mirati ai backup. Grazie alle funzionalità integrate, i backup restano protetti e le snapshot non vengono compromesse.

- **I backup e le snapshot immutabili** creano punti di ripristino a prova di manomissione.
- **Il ripristino con air gap** isola i dati dalle reti attive per evitare danneggiamenti.

[1] Report Ponemon - Cost of a Data Breach, 2024

Rafforzamento degli appliance Dell Data Protection

Gli appliance Dell Data Protection sono integrati con funzionalità che includono Dell SafeBIOS per l'integrità del firmware e SafeData per la crittografia sicura, che contribuiscono alla protezione contro gli attacchi ai backup. Inoltre, queste soluzioni dispongono di funzionalità come l'autenticazione a più fattori (MFA), i controlli degli accessi basati su ruoli (RBAC) e l'autenticazione doppia per impedire agli autori delle minacce di infiltrarsi nei sistemi.

Rilevamento delle minacce avanzato con CrowdStrike

L'integrazione tra CrowdStrike e Dell Data Protection si concentra sul miglioramento della sicurezza e del monitoraggio degli ambienti di protezione dei dati tramite una serie di funzionalità avanzate.

1. **Protezione degli endpoint e dei dati:** Dell integra la sicurezza degli endpoint di CrowdStrike e il rilevamento e la risposta estesi (EDR/XDR) con le sue soluzioni di protezione dei dati. Questo include la raccolta della telemetria con PowerProtect Data Manager e PowerProtect Data Domain di Dell, oltre alle informazioni sulla sicurezza della console CrowdStrike Falcon e del software SIEM di nuova generazione
2. **Monitoraggio e risposta:** il servizio Managed Detection and Response (MDR) di Dell gestisce il software CrowdStrike per conto dei clienti, raccogliendo i registri e analizzando eventuali anomalie o indicatori di compromissione (IoC) rilevati. Grazie a questa integrazione, Dell può offrire un monitoraggio continuo e collaborare con il SOC del cliente per garantire una correzione rapida ed efficace delle minacce
3. **Visibilità in tempo reale e controllo dello spostamento dei dati:** la piattaforma CrowdStrike Falcon Data Protection offre visibilità in tempo reale sullo spostamento dei dati tra varie origini e canali, classificando i dati in base al contenuto e al contesto. Questo consente di prevenire il furto di dati e garantire che le policy di protezione dei dati vengano applicate in modo efficace combinando i contenuti con l'analisi del contesto
4. **Gestione unificata e deployment semplificato:** grazie all'integrazione, un'unica piattaforma e un solo agent possono gestire la protezione sia degli endpoint che dei dati, riducendo la complessità e l'overhead operativo. Tutto questo viene facilitato dall'approccio leggero e nativo per il cloud della piattaforma CrowdStrike Falcon, che consente un deployment rapido e interruzioni minime

L'integrazione tra CrowdStrike e Dell Data Protection sfrutta funzionalità EDR/XDR avanzate, monitoraggio in tempo reale e gestione completa dei dati per migliorare la sicurezza complessiva e la resilienza degli ambienti di protezione dei dati.

Un importante istituto finanziario ha recentemente implementato PowerProtect Cyber Recovery, che ha impedito agli autori degli attacchi di accedere al 90% dei backup critici durante una violazione e ha permesso un ripristino fluido e senza alcun pagamento di riscatti.

Soluzioni Dell PowerProtect per l'integrità dei backup

Dell PowerProtect offre una protezione completa dei backup, basata su caratteristiche di immutabilità, isolamento e compressione che evitano la compromissione dei sistemi di backup. Grazie all'integrazione con gli strumenti di rilevamento ransomware, PowerProtect attiva avvisi in caso di modifiche sospette, permettendo di intervenire tempestivamente.

Approccio alla sicurezza multilivello

La protezione dei dati richiede strategie per la sicurezza coordinate e multiformi. Dell aiuta le aziende a implementare le best practice del settore per creare un ambiente di backup resiliente.

Passaggi chiave per rafforzare la difesa

- **Adozione dei principi Zero Trust:** convalida continuamente tutti gli utenti, i dispositivi e i processi, riducendo così il rischio di accessi non autorizzati.
- **Crittografia di tutti i backup:** assicura che sia i dati in transito che quelli inattivi rimangano illeggibili se compromessi.
- **Formazione dei dipendenti:** insegna ai dipendenti a riconoscere i tentativi di phishing e altre tattiche di social engineering che causano violazioni iniziali.
- **Test regolari delle vulnerabilità:** l'esecuzione frequente di test aiuta le organizzazioni a identificare e correggere i punti deboli prima che gli autori degli attacchi le sfruttino.

Dell abbina queste pratiche a soluzioni all'avanguardia, creando un'infrastruttura solida e reattiva pronta ad affrontare le sfide emergenti.

Partnership strategiche che migliorano la sicurezza

Dell collabora con leader della sicurezza informatica come Microsoft, CrowdStrike e Secureworks. Ogni partnership migliora le soluzioni Dell e offre ai clienti funzionalità di protezione ineguagliabili come Threat Intelligence avanzata, monitoraggio degli endpoint e strategie di risposta complete.

Uso di Dell Professional Services

Le soluzioni Dell Technologies Professional Services forniscono competenze e indicazioni per aiutare le aziende ad affrontare in modo efficace le complesse sfide della sicurezza informatica. Dalla creazione di piani di risposta agli incidenti all'implementazione di architetture Zero Trust, gli specialisti Dell garantiscono che gli ambienti client siano sempre resilienti contro le minacce moderne come l'infiltrazione dei backup.

Creazione della resilienza aziendale con Dell

Scegliendo Dell Technologies, le aziende possono superare in astuzia i sofisticati autori degli attacchi e mantenere al tempo stesso la continuità operativa. Grazie all'innovazione, alle partnership e all'esperienza, Dell aiuta le organizzazioni a prevenire, rilevare e ripristinare i sistemi anche nei casi di infiltrazione dei backup più gravi.

Fai la prossima mossa

Contatta Dell Technologies oggi stesso per proteggere il tuo business. Insieme, proteggiamo i tuoi asset critici, difendiamo la tua reputazione e creiamo un futuro resiliente.

Dell si impegna a promuovere la fiducia nell'era digitale e offre alle organizzazioni gli strumenti, le conoscenze e il supporto necessari per operare in modo sicuro e prosperare.

La resilienza dei backup inizia con Dell Technologies. Agisci subito per rendere le tue operazioni a prova di futuro e creare fiducia nel tuo profilo di sicurezza informatica.

Scopri come affrontare alcune delle principali sfide della sicurezza informatica di oggi alla pagina **Dell.com/SecuritySolutions**

Ulteriori informazioni su Soluzioni Dell

Contatta un esperto Dell Technologies

Visualizza più risorse

Partecipa alla conversazione con #HashTag

DELL Technologies