Ripristino accelerato in seguito ad attacchi ransomware con Dell PowerProtect Backup Services

Ripristino da attacchi ransomware in poche ore, anziché in giorni

Caratteristiche principali

Attacchi ransomware sempre più frequenti, evoluti e costosi

- Impossibilità di identificare e ripristinare rapidamente backup o file non infettati
- Diffusione della contaminazione e reinfezione dai dati di ripristino
- Perdita di dati, impossibilità di ripristinare un set di dati completo
- Difficoltà a coordinare l'orchestration per la risposta agli incidenti
- Richieste di tempi RPO/RTO più rapidi
- Costosi downtime aziendali che comportano perdite di entrate e danni alla reputazione del marchio
- Sanzioni legali e normative dovute a una protezione dei dati inadeguata

La sfida

I ransomware rappresentano una minaccia seria per ogni impresa. Gli attacchi informatici sono frequenti e possono causare danni catastrofici. Il 79% delle organizzazioni teme di subire un evento dirompente nei prossimi 12 mesi1. Le aziende che perdono i propri dati rischiano di dover dichiarare bancarotta dopo una situazione di emergenza. Gli attacchi ransomware stanno diventando più frequenti, ma anche tecnologicamente più avanzati e costosi.

La soluzione

Un ripristino rapido e affidabile elimina qualsiasi motivo per considerare il pagamento di un riscatto. Tuttavia, quando si verifica un incidente di sicurezza o un attacco informatico, le organizzazioni devono comprendere l'entità del danno e la root cause prima del ripristino. Grazie a snapshot immutabili e con air gap di carichi di lavoro e macchine virtuali disponibili 24 ore su 24, 7 giorni su 7, al monitoraggio continuo delle anomalie di utenti e dati, all'integrazione con gli strumenti di sicurezza e al ripristino automatizzato dei dati puliti, è possibile migliorare il profilo di sicurezza e trasformare un evento devastante in un incidente gestibile.

Le funzionalità

Per tutti i carichi di lavoro:

• Garantire backup immutabili e con air gap disponibili 24 ore su 24, 7 giorni su 7

• Ripristinare i dati puliti on-premise o nel cloud con RPO/RTO di ore, non giorni o settimane

• Il servizio Managed Data Detection and Response (MDDR) fornisce monitoraggio in tempo reale 24x7x365 degli ambienti di backup

• Ripristinare carichi di lavoro e macchine virtuali in qualsiasi account/regione AWS: quando si utilizzano i dati dell'organizzazione di produzione e si creano molte copie di tali dati, archiviandoli in più posizioni, si mette a rischio l'organizzazione.

Ripristino accelerato in seguito ad attacchi ransomware per carichi di lavoro chiave:

• Monitorare e rilevare in modo proattivo le anomalie con algoritmi basati su apprendimento automatico

• Orchestrare le attività di risposta e ripristino tramite integrazioni SIEM e SOAR

• Eseguire la scansione delle snapshot per individuare malware prima del ripristino ed eliminare le snapshot e i file infettati dai backup

• Ripristinare automaticamente la versione pulita più recente di ogni file in un intervallo di tempo specificato da una snapshot "golden"

Protezione

Il primo passo per prevenire i danni da ransomware è assicurarsi di avere una copia dei dati immutabile e con air gap. Basato su un'infrastruttura cloud altamente resiliente, Dell PowerProtect Backup Services rende impossibile per il ransomware crittografare i dati di backup. L'architettura Zero Trust, che include l'autenticazione a più fattori, la crittografia envelope e l'accesso con account distinti, garantisce che il ransomware non possa utilizzare credenziali compromesse dell'ambiente primario per manomettere l'ambiente o i dati di backup. Infine, le funzionalità di prevenzione delle eliminazioni in eccesso e delle eliminazioni temporanee (cestino) forniscono un ulteriore livello di sicurezza per proteggere i backup da eliminazioni accidentali.

Rilevamento

Rilevare un attacco ransomware il prima possibile può aiutare i team di risposta agli incidenti a prevenire la diffusione della contaminazione. Il modulo di ripristino accelerato in seguito ad attacchi ransomware Dell PowerProtect Backup Services fornisce un Security Command Center per monitorare il profilo dell'ambiente di backup. Con analisi degli accessi e rilevamento delle anomalie è possibile identificare rapidamente attività insolite nell'ambiente e nei dati. È possibile visualizzare informazioni su posizione, identità e attività per tutti i tentativi di accesso da parte di utenti e API. Le anomalie vengono rilevate da algoritmi ML proprietari che forniscono avvisi per attività di dati insolite (ad esempio, eliminazione, crittografia e così via). L'algoritmo apprende i modelli per l'ambiente di backup specifico, dunque non richiede configurazioni e ottimizzazioni di regole. Utilizza inoltre informazioni basate su entropia per ridurre i falsi positivi

Risposta

Quando un analista IT o della sicurezza rileva un evento sospetto o peggio, conferma un incidente ransomware, la velocità di risposta è cruciale. Sebbene siano disponibili molti strumenti di sicurezza dell'ambiente primario che possono essere utilizzati per l'orchestration del rilevamento e della risposta, le analisi e i dati dei registri delle modifiche ricavati da dati secondari (sistemi di backup) migliorano le attività di indagine, risposta e analisi forense. Il modulo di ripristino accelerato in seguito ad attacchi ransomware Dell PowerProtect Backup Services offre solide integrazioni API pronte all'uso che semplificano l'integrazione della soluzione nell'ecosistema di sicurezza globale. L'orchestration delle attività di risposta mediante soluzioni SIEM e SOAR può ridurre drasticamente il tempo medio di risposta (MTTR), automatizzando azioni come la quarantena di sistemi o snapshot infettate o la scansione dei backup alla ricerca di IOC in base a un playbook predeterminato per il ransomware.

Ripristino

Dopo la fase iniziale di risposta, inizia il lavoro più impegnativo: il ripristino. Per molte aziende si tratta di un processo manuale e dispendioso in termini di tempo. Il tempo di permanenza degli utenti malintenzionati e dei ransomware può variare da settimane a mesi, rendendo difficile capire quanto indietro bisogna andare per trovare dati puliti. Anche dopo aver identificato la snapshot migliore, malware nascosti possono causare nuove infezioni. Un recovery point precedente di 2 settimane non è accettabile per la maggior parte degli utenti aziendali, ma trovare e convalidare dati più recenti dopo un incidente di ransomware è un'attività manuale, tediosa e spesso insormontabile.

Dell PowerProtect Backup Services allevia questo peso con un'architettura di backup efficace e strumenti automatizzati per accelerare il ripristino. La piattaforma cloud Dell PowerProtect Backup Services esegue il backup dei carichi di lavoro direttamente nel cloud, pronta per un ripristino immediato in caso di attacco ransomware.

Il modulo di ripristino accelerato in seguito ad attacchi ransomware consente di eseguire il ripristino in tutta sicurezza, garantendo l'integrità dei dati di ripristino. È possibile eseguire la scansione delle snapshot alla ricerca di malware e IOC tramite il rilevamento antivirus integrato o la Threat Intelligence dalle indagini forensi o dai feed di Threat Intel. La scansione delle snapshot prima del ripristino elimina il rischio di reinfezione.