Giornata mondiale del backup: Quattro best practice per la data protection da conoscere

Stare al passo con l'evoluzione delle minacce informatiche non è facile, neanche nelle organizzazioni più grandi e ben finanziate. Secondo il sondaggio di PwC del 2024 sulla fiducia digitale globale, solo il 2% delle aziende sta ottimizzando e migliorando continuamente le nove best practice di resilienza informatica. Inoltre, solo il 3% delle aziende aggiorna continuamente i piani di gestione del rischio. La parte di sicurezza che "mantiene il passo" è più simile a quella che viene eseguita in sede (a malapena).

Il panorama delle minacce continuerà a diventare sempre più sofisticato. Infatti, lo scorso anno abbiamo osservato un maggior numero di casi di "cyber-espionage"

in cui gli hacktivisti abbattono i sistemi di infrastruttura critici o espongono i dati pubblicamente, e di “crittografia intermittente”, in cui gli hacker criptano solo bundle di dati alternativi per sfuggire al rilevamento.

Man mano che il valore dei dati aziendali continua a salire e la creatività e la sofisticatezza degli hacker raggiunge nuovi livelli, è assolutamente fondamentale adottare un approccio solido al backup, sia nell’infrastruttura che nella cultura. Ma come puoi ottenerlo? Ecco alcune best practice da prendere in considerazione quando si implementa una solida strategia di data protection:

1. Concentrarsi sulla gestione proattiva delle minacce e delle vulnerabilità

Con qualsiasi evento di sicurezza, c’è un prima, un durante e un dopo.Prima di un attacco, gli avversari stanno facendo i loro compiti. Stanno imparando a conoscere la tua organizzazione per capire le dimensioni e l’ambito della loro opportunità, spesso cercando di scoprire i limiti dell’assicurazione sulla sicurezza informatica, le operazioni critiche eseguite dalla tua organizzazione e dove e a chi vengono forniti i servizi. Armato di queste informazioni, l’autore dell’attacco può tracciare un percorso per tentare di forzare il pagamento di un riscatto. Ecco perché è fondamentale che anche le organizzazioni svolgano i propri compiti.

Tieniti aggiornato sugli eventi informatici che stanno rivoluzionando diverse aree geografiche, settori e gruppi, nonché sui tipi di attacchi che più probabilmente avranno un impatto sulla tua azienda. Grazie a questo, prepara i tuoi team di gestione delle minacce informatiche interni o esterni e informa i tuoi dipendenti su cosa cercare.

Nell’ambito di un approccio proattivo, consiglio di implementare:

- Autenticazione multifattore e vaulting delle credenziali amministrative
- Una piattaforma di analytics rapida per i dati di registro che consente di eseguire ricerche rapide ed eventi di correlazione per identificare i segnali di potenziali autori di minacce nell’ambiente prima che colpiscano

- Accesso coerente tra gli ambienti per rafforzare le difese
- Una buona igiene dei sistemi con un programma di gestione delle patch attivo e ben definito

2. Implementare un'architettura di data protection multilivello

Quando si tratta di sicurezza informatica, la prevenzione degli attacchi è solo la metà della battaglia. Le strategie di data protection non possono riguardare solo il periodo precedente a un evento, ma devono soddisfare anche le aspettative dopo un evento.

L'implementazione di un'architettura di data protection e resilienza multilivello è un modo eccellente per integrare resilienza e durata in una strategia di ripristino. Le architetture di backup a più livelli utilizzano posizioni logiche e geografiche diverse per soddisfare le diverse esigenze di backup e ripristino. Inoltre, contribuiscono a garantire il raggiungimento degli obiettivi di tempo di ripristino appropriati, offrendo una serie di funzionalità che aiutano l'azienda a tornare in funzione il più rapidamente possibile dopo un attacco. Adotta un'architettura di backup a più livelli utilizzando posizioni logiche e geografiche diverse per soddisfare le diverse esigenze di backup e ripristino.

A tale scopo, consiglio anche un ambiente di ripristino isolato sicuro (SIRE), un ambiente speciale per l'archiviazione e la protezione di backup puliti dei dati. A differenza dei backup tipici, i SIRE sono intenzionalmente memorizzati lontano dalla rete principale in modo che i dati non possano essere infettati o eliminati in caso di incidente informatico o altro disastro. Un SIRE non è solo un altro backup, ma è anche a prova di guasto quando si verifica il peggio, offrendoti un ripristino dei punti garantito per ripristinare le operazioni critiche in modo rapido, pulito e sicuro.

3. Tratta i dati come cittadini di prima classe con visibilità e resilienza dei dati migliorate

Dai priorità a una migliore visibilità dei dati e implementa sistemi di backup e ripristino a prova di guasto. Per proteggere dataset e processi preziosi, le organizzazioni hanno bisogno di visibilità sui dati e di sistemi a prova di guasto che consentano di continuare a lavorare anche se gli autori degli attacchi non riescono a mettersi in gioco. In precedenza ho spiegato come una piattaforma di analytics rapida per i dati di registro può eseguire ricerche rapide e correlare gli eventi per identificare i segnali di potenziali autori di minacce nel tuo ambiente prima che colpiscano. Il data storage ad alte performance come Pure Storage può acquisire e analizzare le anomalie in tempo reale, consentendo ai team di ricerca delle minacce di individuare gli intrusi che si intrudono nella rete prima che il danno venga danneggiato.

4. Adotta soluzioni di backup super immutabili

Senza immutabilità, i dati di backup diventano vulnerabili alle infezioni quanto il dataset primario. Ransomware si sono evoluti per colpire specificamente i sistemi di backup, rendendo inefficaci le strategie di protezione tradizionali. Questi moderni attacchi ransomware neutralizzano deliberatamente i backup prima di lanciare l'attacco principale, garantendo alle vittime l'assenza di opzioni di ripristino, se non il pagamento del riscatto.

I backup immutabili costituiscono una formidabile barriera contro gli attacchi ransomware, le eliminazioni accidentali e persino le minacce interne dannose con privilegi elevati. È sufficiente eseguire il restore da queste copie non manomesse senza pagare riscatti, riducendo al minimo i downtime e le perdite finanziarie.

A differenza di altre soluzioni, **le snapshot SafeMode™** sono davvero immutabili e non possono essere eliminate (eliminate), modificate o crittografate da ransomware o malintenzionati. Sono protetti con l'autenticazione multifattore e richiedono un rigoroso processo di verifica multifase che coinvolga il team di supporto di Pure Storage per apportare modifiche. SafeMode genera

automaticamente snapshot immutabili a intervalli personalizzabili, garantendoti sempre versioni aggiornate e inalterate dei tuoi dati. Le solide policy configurabili per la frequenza, la conservazione e la replica delle snapshot in varie destinazioni impediscono agli autori degli attacchi di compromettere l'intera strategia di backup e SafeMode può completare i restore da 10 a 20 volte più velocemente rispetto alle soluzioni della concorrenza.

Questa combinazione di protezione ironclad e funzionalità di ripristino rapido rende i backup immutabili un componente essenziale di qualsiasi strategia di resilienza informatica moderna.

La chiave del successo organizzativo è la resilienza e l'agilità

Questa Giornata mondiale del backup è un promemoria tempestivo per le organizzazioni che desiderano rivalutare il proprio approccio e gli strumenti di sicurezza. Ma l'impatto positivo della resilienza e della protezione dei dati va ben oltre una semplice giornata. La creazione di resilienza e agilità in tutta l'organizzazione è cruciale non solo per i dati, ma anche per il successo complessivo del business. Le organizzazioni che proteggono efficacemente i dati delle applicazioni garantiranno la business continuity anche di fronte a minacce sofisticate.