Domande frequenti sul ripristino a seguito di ransomware

Il termine “immutabilità” è diventato particolarmente di moda nel settore come la soluzione per gli attacchi ransomware e magari ti stai chiedendo come si pone Cove Data Protection™ in merito.

In realtà, per un ripristino efficace a seguito di un attacco ransomware è necessaria un’architettura di sicurezza più completa. Sono tre gli aspetti chiave di tale approccio: isolare copie di backup, ridurre la superficie di attacco e impedire il più possibile agli utenti diversi dagli amministratori autorizzati di accedere ai backup.

D. In che modo Cove supporta l’isolamento?

Cove è stato concepito per il cloud, il che significa che ogni backup viene inviato off-site e isolato nel nostro cloud privato per impostazione predefinita, senza la necessità di un’appliance locale che funga da intermediaria. In questo modo, i tuoi backup vengono archiviati all’esterno della rete locale, al sicuro da ransomware.

Cove sottopone a crittografia i backup in loco, con crittografia AES a 256 bit, quindi li trasferisce al data center remoto tramite connessioni unidirezionali TLS 1.2. I backup vengono memorizzati e crittografati nei nostri data center. I data center globali di N-able sono stati concepiti per garantire la sicurezza e ti permettono di conservare i backup nella tua area geografica.

Un approccio basato su cloud non è affatto limitativo: se vuoi, puoi tenere una copia facoltativa dei backup in locale per il ripristino alla velocità della LAN, utilizzando una condivisione di rete esistente o l’hardware che preferisci e la funzionalità LocalSpeedVault. Se subisci un attacco ransomware che distrugge la copia in locale, il backup principale resterà al sicuro.

D. Qual è la differenza rispetto alle soluzioni della concorrenza?

I tradizionali prodotti che prevedono il backup a livello di immagine sono concepiti per essere utilizzati in locale e poi si affidano a meccanismi aggiuntivi per inviare tali backup a uno spazio di archiviazione off-site. Questo approccio fa lievitare i costi e il livello di complessità e spesso richiede licenze aggiuntive, oltre che la configurazione manuale. Alcuni fornitori offrono lo storage cloud, altri impongono al cliente di trovare un servizio adeguato, di acquistarlo, configurarlo e gestirlo.

Per ridurre la superficie di attacco dell’infrastruttura di backup on-premise, i fornitori tradizionali usano spesso tecnologie quali il blocco WORM, che spesso fa riferimento alla possibilità di creare copie immutabili, che si dimostrano protezioni adeguate in caso di attacchi informatici distruttivi. Se da un lato questo approccio reattivo non risolve il problema più ampio delle copie di backup archiviate sulla stessa rete dei criminali informatici, esso aggiunge complessità di gestione circa conservazione, scadenza, controllo dei file da cestinare e così via.

D. In che modo Cove riduce le dimensioni della superficie di attacco?

I criminali informatici generalmente operano sferrando un attacco ad applicazioni e dati necessari per l’azienda, cercando anche le copie di backup e l’infrastruttura utilizzata per ripristinare tali backup, vale a dire l’applicazione per la protezione dei dati. Cove sposta due di questi tre elementi critici all’esterno della rete locale, in modo che siano inattaccabili.

Come abbiamo già illustrato, il metodo di backup basato su cloud di Cove archivia i dati di backup in una sede cloud remota e rende inaccessibili tali elementi a chiunque riesca ad accedere alla tua rete locale.

E poiché Cove è un'applicazione SaaS completamente in hosting, anche il tuo meccanismo di ripristino è lontano dalla rete locale. Con Cove, i file di backup e l'infrastruttura per il disaster recovery restano esterni alla rete, il che riduce significativamente la superficie di attacco in caso di malware e semplifica le cose in caso di ripristino.

D. In che modo Cove risolve il problema del controllo degli accessi?

A differenza di altri prodotti, Cove impone e applica l'autenticazione a due fattori che aumenta la protezione dagli hacker in grado di rubare le tue credenziali, aggiungendo un ulteriore livello di sicurezza.

Inoltre, l'accesso a funzionalità specifiche è limitato in base ai diversi ruoli, il che ti permette di concedere l'accesso granulare ad attività limitate affidate all'help desk o agli utenti finali, senza concedere a tali utenti livelli di accesso non necessari. Ad esempio, puoi delegare solo il ripristino dei file a determinati dispositivi o domini, senza concedere l'accesso completo.

D. Che livello di accesso è necessario per apportare modifiche alle selezioni, alle esclusioni o alle pianificazioni dei backup?

È richiesto l'accesso come amministratore locale per accedere al client della gestione backup o alle funzioni amministrative della riga di comando. È inoltre possibile limitare le modifiche a selezioni, esclusioni e pianificazioni dal client della gestione backup utilizzando i profili di backup. È possibile configurare una password per l'interfaccia utente grafica per uno o più dispositivi tramite comando remoto per limitare l'accesso all'interfaccia del client della gestione backup locale e all'API client.

Inoltre, come già sottolineato, Cove richiede l'autenticazione a due fattori, per un ulteriore livello di sicurezza. Le modifiche a selezioni, esclusioni, pianificazioni, filtri di backup o altre modifiche alle configurazioni effettuate nella gestione backup locale o nella riga di comando non influiranno sulle precedenti sessioni di backup.

D. Che cosa succede se l'agent della gestione backup locale di Cove viene eliminato da un dispositivo?

La disinstallazione del client locale di gestione backup non elimina le sessioni di backup precedenti archiviate sulla LocalSpeedVault (LSV) o nello storage cloud di N-able.

D. Che succede ai backup con Cove se i dati di produzione vengono eliminati, danneggiati o sottoposti a crittografia?

L'eliminazione, il danneggiamento o la crittografia dei file sul sistema di produzione non ha alcun impatto sulle precedenti sessioni di backup già memorizzate sulla LSV o nello storage cloud di N-able.

D. Quali sono le considerazioni da fare circa la sicurezza quando si configura una LocalSpeedVault?

Si consiglia di configurare la LocalSpeedVault facoltativa perché punti a un dispositivo NAS con sicurezza a livello di gruppo di lavoro e credenziali univoche inserite solo nella gestione backup, senza condivisioni esterne né unità mappate. La LSV i cui dati non sincronizzati sono stati compromessi o danneggiati non sarà caricata dalla gestione backup nello storage cloud di N-able.

D. Come vengono protetti gli archivi?

La pulizia forzata delle singole origini dati può essere avviata dal client di gestione backup locale ma richiede l'accesso come amministratore locale e la chiave o passphrase di crittografia del dispositivo e può essere limitata con l'impiego di una password per l'interfaccia grafica.

L'eliminazione di una pianificazione archivio non influisce sulle sessioni precedenti di backup o archiviazione. La pulizia delle sessioni di archiviazione specifiche precedenti rispetto alle impostazioni predefinite di conservazione è eseguibile dalla gestione backup locale ma richiede l'accesso come amministratore locale ed è limitata con l'utilizzo di una password per l'interfaccia grafica.

Misure di sicurezza aggiuntive:

1. L'accesso alla console di gestione dei backup è limitato tramite l'autenticazione a due fattori e i diversi ruoli utente che offrono differenti livelli di accesso.
2. La possibilità di generare una passphrase è limitata agli addetti alla sicurezza indicati, mentre il codice è valido per un solo uso o per 24 ore.
3. L'eliminazione di un dispositivo di backup dalla console di gestione dei backup è consentita per alcuni ruoli utente e può essere annullata dall'assistenza se richiesto entro 14 giorni.
4. La riduzione dei valori delle impostazioni di conservazione nel prodotto attualmente assegnato o la creazione e l'applicazione di un altro prodotto a un dispositivo è eseguibile da un utente della console di gestione dei backup, il che riduce il numero di giorni disponibili per il ripristino.

Informazioni su N-able

N-able offre ai provider di servizi IT potenti soluzioni software per monitorare, gestire e mettere in sicurezza sistemi, dati e reti dei relativi clienti. Grazie alla piattaforma scalabile su cui si basano i nostri prodotti, offriamo un'infrastruttura sicura e strumenti adeguati per semplificare ecosistemi complessi e le risorse per stare al passo con le esigenze IT in continua evoluzione. Aiutiamo i nostri partner in ogni fase del loro percorso a proteggere i clienti e ad espandere la propria offerta di servizi, grazie a un portafoglio flessibile e in continua crescita di integrazioni fornite dai provider di tecnologie leader del settore.

n-able.com/it