DELL Technologies

Breve panoramica sulla soluzione

PowerProtect Cyber Recovery per Sheltered Harbor

Proteggere i dati critici dei clienti e preservare la fiducia dei consumer nei mercati finanziari statunitensi

CHE COS'È SHELTERED HARBOR?

Creato nel 2015 dal settore finanziario, lo standard Sheltered Harbor incorpora una serie di best practice e di salvaguardie in materia di cyber-resilienza e protezione dei dati per tutelare i dati finanziari statunitensi. Le minacce informatiche, tra cui il ransomware, la distruzione dei dati o i furti, che colpiscono i sistemi di produzione e di backup, mettono a rischio i dati finanziari dei consumatori e delle aziende.

Un attacco informatico riuscito contro una banca, una cooperativa di credito o una società di intermediazione statunitense danneggerebbe la reputazione di tale istituto finanziario, minerebbe la fiducia dei consumer nel sistema finanziario statunitense e potrebbe scatenare una crisi finanziaria globale.

Sheltered Harbor migliora la stabilità finanziaria statunitense e la cyber-resilienza delle istituzioni, isolando i record critici dei conti dei clienti e altri dati immutabili all'interno di un vault digitale. Nel caso in cui i sistemi primari o di backup di un istituto siano compromessi da un attacco informatico come il ransomware o altro, si attiva il ripristino rapido di questi dati critici, agevolando la continuità dei servizi bancari indispensabili rivolti ai clienti e conservando la fiducia del pubblico.

PERCHÉ SCEGLIERE CYBER RECOVERY?

Dell Technologies è il primo Solution Provider nell'ambito dello Sheltered Harbor Alliance Partner Program che ha elaborato una soluzione di data vaulting pronta all'uso per gli istituti finanziari degli Stati Uniti.

PowerProtect Cyber Recovery per Sheltered Harbor è la prima soluzione on-premise e pronta all'uso per il data vaulting ad essere approvata da Sheltered Harbor. Soddisfa tutti i requisiti tecnici di prodotto per i Partecipanti che implementano lo standard Sheltered Harbor.

Vault di dati – L'istituto o il fornitore di servizi partecipante crea i backup notturni dei dati critici nel formato standard Sheltered Harbor. Il vault dei dati è criptato, immutabile e isolato dall'infrastruttura dell'istituto, compresi i sistemi di backup, ripristino di emergenza e altri sistemi di protezione dei dati.

Isolamento e governance – Un ambiente isolato e sicuro, disconnesso dalle reti aziendali, limita l'accesso a tutti gli utenti che non dispongono dell'autorizzazione adeguata. La copia automatizzata dei dati e la gestione air-gapped garantiscono la conservazione dell'integrità, della disponibilità, della sicurezza e della riservatezza dei dati.

Ripristino e correzione – Se si attiva un piano di resilienza Sheltered Harbor, l'istituto partecipante recupera rapidamente i dati dal vault per consentire il più rapido ripristino e la ripresa delle operazioni bancarie.

La sfida: evitare una crisi finanziaria globale a seguito di un attacco informatico al settore dei servizi finanziari

Tutte le organizzazioni si preoccupano dell'impatto paralizzante che un attacco informatico malevolo può avere sul loro business, anche se il 97% delle organizzazioni utilizza dati sensibili nei propri sforzi di Digital Transformation.[1] Lo sblocco del valore dei dati dà grandi soddisfazioni.

Vi è anche un rischio significativo se i dati sensibili cadono nelle mani sbagliate, vengono distrutti o resi pubblici. Malware e ransomware evolvono e gli attacchi proliferano: i ransomware aziendali sono aumentati del 12% nel 2019 e rappresentano l'81% di tutte le infezioni da ransomware secondo l'Internet Security Threat Report di Symantec del 2019.[2] Inoltre, secondo un recente rapporto del Ponemon Institute, nel 2020 il 52% di tutte le violazioni di dati è stato di natura malevola, con un aumento del 30% rispetto a soli cinque anni fa.[3]

Per di più, le tattiche e gli strumenti dei responsabili delle minacce si sono evoluti per rendere sempre più difficile il rilevamento e la prevenzione degli attacchi. Le tattiche di criminalità informatica continuano a evolvere: secondo il Verizon Data Breach Investigations Report del 2020, il 30% degli attacchi informatici segnalati coinvolgono gli addetti ai lavori, in aumento rispetto al 25% di soli tre anni fa.[4]

Il settore finanziario statunitense ha subito negli ultimi tre anni le perdite più elevate a causa della criminalità informatica (secondo il rapporto annuale sui costi del crimine informatico di Accenture del 2019[5]) e queste forze concorrono a creare una tempesta perfetta di minacce che i mercati finanziari globali devono affrontare.

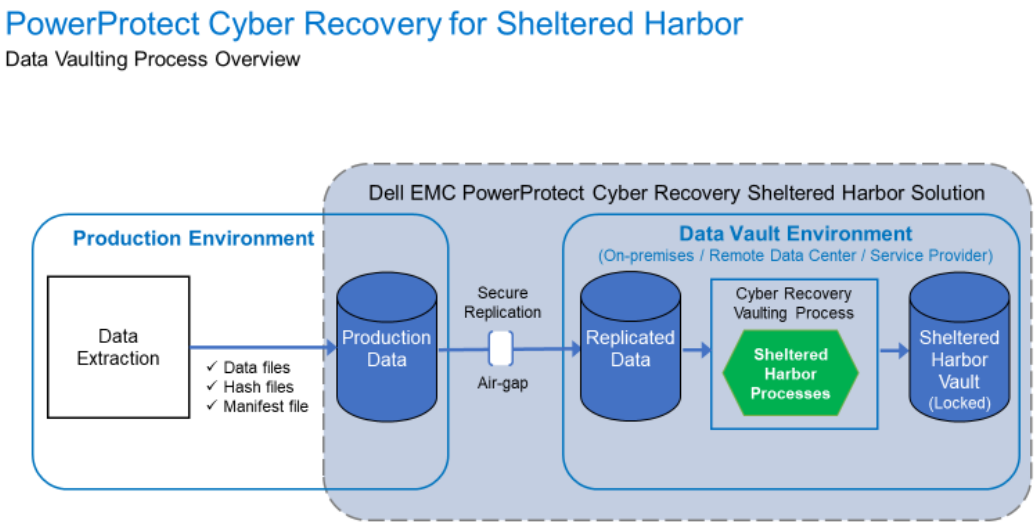
Sheltered Harbor è un'iniziativa senza scopo di lucro, creata nel 2015 e guidata dal settore, che ha lo scopo di orientare le istituzioni finanziarie statunitensi verso la riduzione del rischio di attacchi informatici capaci di compromettere i dati dei clienti e interrompere i normali servizi bancari. L'ecosistema Sheltered Harbor comprende istituzioni partecipanti (banche statunitensi, cooperative di credito, agenzie di intermediazione, gestori patrimoniali), associazioni nazionali di categoria, fornitori di soluzioni e di servizi dedicati al miglioramento della stabilità e della resilienza informatica del settore finanziario.

Il disaster recovery tradizionale e la continuità aziendale sono necessari per ripristinare la piena capacità operativa dopo un evento naturale o causato dall'uomo. A seguito di un attacco informatico mirato e sofisticato, Sheltered Harbor si propone di garantire che i dati necessari per ripristinare le operazioni bancarie di base siano prontamente disponibili e integri, mentre le procedure di recupero completo proseguono.

Dell EMC PowerProtect Cyber Recovery per Sheltered Harbor – Robusta cyber-resilienza per i dati critici delle istituzioni finanziarie

Dell Technologies è il primo fornitore di soluzioni ad aderire al programma per i partner di Sheltered Harbor Alliance. La nostra soluzione approvata per Sheltered Harbor si basa su Dell PowerProtect Cyber Recovery, leader di mercato con quasi cinque anni di esperienza nel proteggere i dati critici delle organizzazioni da attacchi informatici, come il ransomware.

Per conformarsi alla specifica Sheltered Harbor, l'architettura del vault Cyber Recovery è stata estesa al fine di eseguire i processi di generazione di archivi e archiviazione sicura. I dati estratti da Sheltered Harbor sono salvati in produzione, quindi replicati in modo sicuro tramite un collegamento logico, air-gapped e dedicato all'ambiente in vault, dove si eseguono le fasi rimanenti, come il blocco di retention.



Creando un ambiente dedicato, isolato e fisicamente separato dalle reti aziendali e dai sistemi di backup, i set di dati critici, che i Partecipanti Sheltered Harbor sono tenuti a proteggere, sono disponibili in formato standardizzato in modo da poter riprendere rapidamente i servizi bancari di base per i clienti. Il deployment è misurato in settimane, invece che in mesi, e con la certezza della conformità alla specifica Sheltered Harbor.

Riepilogo

Dell EMC PowerProtect Cyber Recovery per Sheltered Harbor fornisce alle istituzioni partecipanti un'alternativa completamente approvata, veloce, economica ed efficiente per ogni istituzione che costruisce un vault proprietario una tantum al fine di ottenere la conformità alla specifica Sheltered Harbor. Le banche, le cooperative di credito e le società di brokeraggio che scelgono di implementare lo standard Sheltered Harbor possono rivolgersi a Dell Technologies per una soluzione di vaulting dei dati pronta all'uso, completamente approvata e supportata.

Con l'ulteriore vantaggio di sfruttare una tecnologia matura basata sul vault, i partecipanti di Sheltered Harbor che scelgono PowerProtect Cyber Recovery per Sheltered Harbor possono soddisfare in tutta sicurezza le esigenze di deployment immediato, oltre a stabilire un punto di riferimento per le future esigenze di vaulting dei dati. Le istituzioni partecipanti dispongono di un percorso di sopravvivenza e la fiducia dell'opinione pubblica nel sistema finanziario statunitense è mantenuta.

Fonti:

1. 2019 Thales Data Threat Report – www.thalessecurity.com/DTR
2. 2019 Symantec Internet Security Threat Report - https://www.symantec.com/security-center/threat-report
3. Report sul costo di una violazione dei dati del 2020, Ponemon Institute, LLC - https://www.ibm.com/it-it/security/data-breach
4. Data Breach Investigations Report di Verizon per il 2020 - https://enterprise.verizon.com/resources/reports/dbir/
5. 2019 Accenture Cost of Cybercrime Report - https://www.accenture.com/us-en/insights/security/cost-cybercrime-study