DELL Technologies

Présentation de la solution

PowerProtect Cyber Recovery pour Sheltered Harbor

Protection des données client stratégiques et maintien de la confiance des consommateurs sur les marchés financiers américains

QU'EST-CE QUE SHELTERED HARBOR ?

Créée en 2015 par le secteur des services financiers, la norme Sheltered Harbor intègre un ensemble de pratiques d'excellence en matière de cyber-résilience et de protection des données. Elle comprend également des mesures de protection des données financières aux États-Unis. Les cyber-menaces, y compris les rançongiciels, la destruction des données ou les vols ciblant les systèmes de production et de sauvegarde, mettent en péril les données financières des particuliers et des entreprises.

Une cyberattaque réussie contre une banque, une coopérative de crédit ou une société de courtage américaine pourrait nuire à la réputation de cette institution financière, saper la confiance des consommateurs du système financier américain, voire même déclencher une crise financière mondiale.

Sheltered Harbor améliore la stabilité financière des États-Unis et la cyber-résilience des institutions en isolant de manière immuable les relevés de compte client stratégiques ainsi que d'autres données dans un coffre-fort numérique. Si les systèmes principaux ou de sauvegarde d'une institution devaient être compromis par une cyberattaque du type rançongiciel ou autre, la récupération rapide de ces données stratégiques serait alors activée. L'objectif est double : préserver la continuité des services bancaires stratégiques proposés directement aux clients et renforcer la confiance du public.

POURQUOI CHOISIR CYBER RECOVERY ?

Dell Technologies est le premier fournisseur de solutions dans le cadre du programme de partenariat de l'alliance Sheltered Harbor à avoir mis au point une solution de mise en coffre-fort des données clé en main Sheltered Harbor pour les établissements financiers américains.

PowerProtect Cyber Recovery pour Sheltered Harbor est la première solution de mise en coffre-fort des données clé en main et sur site à être approuvée par Sheltered Harbor. Elle répond à toutes les exigences techniques relatives aux produits auxquelles les participants doivent se conformer lorsqu'ils appliquent la norme Sheltered Harbor.

Coffre-fort de données : les sauvegardes nocturnes des données stratégiques au format de norme Sheltered Harbor sont créées par l'institution financière participante ou le prestataire de services. Le coffre-fort de données est chiffré, non modifiable et isolé de l'infrastructure de l'institution. Cela comprend les processus de sauvegarde, la reprise après sinistre et d'autres systèmes de protection des données.

Isolement et gouvernance : un environnement isolé et sécurisé déconnecté des réseaux d'entreprise limite l'accès des utilisateurs sans autorisation appropriée. La copie automatisée des données et la gestion de l'isolement physique font que l'intégrité, la disponibilité, la sécurité et la confidentialité des données sont préservées.

Récupération et mesure corrective : si un plan de résilience Sheltered Harbor est activé, l'institution participante peut rapidement récupérer les données du coffre-fort pour que les opérations bancaires soient restaurées et relancées dès que possible.

Pour contrer une crise financière mondiale, relever le défi de la cyberattaque dans le secteur des services financiers

Toutes les organisations sont préoccupées par les conséquences désastreuses que pourrait avoir une cyberattaque malveillante sur leur activité, d'autant plus que 97 % d'entre elles utilisent des données sensibles dans leurs efforts de transformation numérique.[1] En effet, exploiter la valeur des données présente de grands avantages.

Le risque est également important si les données sensibles tombent entre de mauvaises mains, qu'elles sont détruites ou sont divulguées. Les logiciels malveillants et de type rançongiciel sont en constante évolution et les attaques augmentent. Ainsi, selon le rapport de Symantec de 2019 sur les menaces à la sécurité sur Internet, les demandes de rançon auprès des entreprises ont augmenté de 12 % en 2019, soit 81 % de toutes les infections de type rançongiciel.[2] En outre, d'après un récent rapport du Ponemon Institute, 52 % des violations de données en 2020 avaient des intentions malveillantes, soit une hausse de 30 % en l'espace de cinq ans.[3]

Qui plus est, les tactiques et les outils des auteurs de menaces ont évolué rendant la détection presque impossible et entraînant une hausse de la prévention de telles attaques. Les tactiques de cybercriminalité ne cessent d'évoluer. Ainsi, d'après le rapport d'enquêtes Verizon de 2020 sur la violation de données, les cyberattaques de l'intérieur signalées sont passées de 25 % à 30 % en seulement trois ans.[4]

Aux États-Unis, selon le rapport annuel d'Accenture de 2019 sur le coût de la cybercriminalité, le secteur des services financiers a subi au cours des trois dernières années les pertes les plus élevées dues à la cybercriminalité. En outre, ces forces combinées peuvent s'avérer une véritable menace pour les marchés financiers mondiaux.[5]

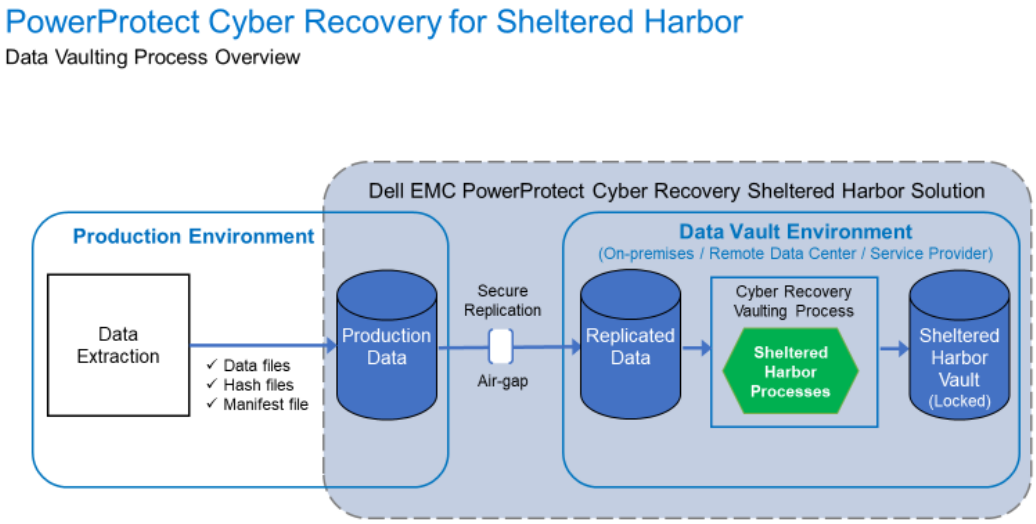
Sheltered Harbor a été créé en 2015 en tant qu'initiative à but non lucratif dirigée par le secteur pour guider les institutions financières américaines à réduire le risque d'une cyberattaque pouvant compromettre les données des clients et interrompre les services bancaires courants. L'écosystème Sheltered Harbor comprend des institutions participantes (banques, coopératives de crédit, sociétés de courtage et gestionnaires de fonds américains), des organisations professionnelles nationales, des fournisseurs de solutions et des prestataires de services dédiés à l'amélioration de la stabilité et de la cyber-résilience du secteur financier.

La reprise après sinistre et la continuité d'activité traditionnelles sont nécessaires pour restaurer la totalité des fonctionnalités opérationnelles suite à un événement d'origine naturelle ou humaine. À la suite d'une cyberattaque ciblée et sophistiquée, Sheltered Harbor a pour objectif que les données nécessaires à la restauration des opérations bancaires de base soient facilement disponibles de manière intègre tandis que les procédures de récupération complète se poursuivent.

Dell EMC PowerProtect Cyber Recovery pour Sheltered Harbor – Cyber-résilience robuste pour les données les plus stratégiques des institutions financières

Dell Technologies est le premier fournisseur de solutions à rejoindre le programme de partenariat de l'alliance Sheltered Harbor. Notre solution approuvée pour Sheltered Harbor est basée sur Dell PowerProtect Cyber Recovery, un leader du marché qui a presque cinq ans d'expérience en matière de protection des données les plus stratégiques des organisations en matière de cyberattaque, telles que les rançongiciels.

Pour se conformer à la spécification Sheltered Harbor, l'architecture de coffre-fort Cyber Recovery a été étendue pour effectuer les processus de génération d'archivage et de référentiel sécurisé. Les données Sheltered Harbor extraites sont sauvegardées en production, puis répliquées de manière sécurisée via une connexion dédiée, isolée physiquement et logique à l'environnement mis en coffre-fort où les étapes restantes, telles que le verrouillage de la conservation, sont effectuées.



En créant un environnement dédié et isolé, physiquement séparé des réseaux d'entreprise et des systèmes de sauvegarde, le format des ensembles de données stratégiques, que les participants à Sheltered Harbor sont tenus de protéger, est standardisé afin que les services bancaires de base accessibles par les clients puissent être rapidement repris. Le déploiement se mesure en quelques semaines au lieu de plusieurs mois, tout en étant conforme avec la spécification Sheltered Harbor.

Synthèse

Afin de se conformer à la spécification Sheltered Harbor, la solution Dell EMC PowerProtect Cyber Recovery pour Sheltered Harbor offre à chaque institution participante créant un coffre-fort propriétaire unique une alternative entièrement approuvée, rapide, rentable et efficace. Les banques, les coopératives de crédit et les sociétés de courtage qui choisissent de mettre en œuvre la norme Sheltered Harbor peuvent se tourner vers Dell Technologies pour bénéficier d'une solution de mise en coffre-fort des données clé en main entièrement approuvée et entièrement prise en charge.

Outre l'avantage de tirer parti d'une technologie de mise en coffre-fort éprouvée, les participants à Sheltered Harbor à la recherche d'une solution PowerProtect Cyber Recovery pour Sheltered Harbor peuvent répondre en toute confiance à leurs besoins de déploiement immédiats, ainsi qu'à la mise en place de leurs besoins futurs en matière de mise en coffre-fort des données. Une institution participante a désormais un moyen de se protéger des cyber-menaces et la confiance du public dans le système financier américain est maintenue.

Sources :

1. Rapport de Thales de 2019 sur les menaces visant les données : www.thalessecurity.com/DTR
2. Rapport de Symantec de 2019 sur les menaces à la sécurité sur Internet : https://www.symantec.com/security-center/threat-report
3. Rapport du Ponemon Institute, LLC de 2020 sur le coût de la violation de données : https://www.ibm.com/security/data-breach
4. Rapport d'enquêtes Verizon de 2020 sur la violation de données : https://enterprise.verizon.com/resources/reports/dbir/
5. Rapport d'Accenture de 2019 sur le coût de la cybercriminalité : https://www.accenture.com/us-en/insights/security/cost-cybercrime-study