DELL Technologies

Lösungsübersicht

PowerProtect Cyber Recovery für Sheltered Harbor

Schutz kritischer Kundendaten und Wahrung des Verbrauchervertrauens in die US-Finanzmärkte

Was ist Sheltered Harbor?

Der 2015 von der Finanzbranche geschaffene Sheltered Harbor-Standard umfasst eine Reihe von Best Practices für die Ausfallsicherheit bei Cyberangriffen und für Data Protection sowie Sicherheitsvorkehrungen zum Schutz von US-Finanzdaten. Cyberbedrohungen wie Ransomware, Datenvernichtung oder Diebstahl, die auf Produktions- und Backupsysteme abzielen, gefährden die Finanzdaten von Verbrauchern und Unternehmen.

Ein erfolgreicher Cyberangriff auf eine US-amerikanische Bank, Kreditgenossenschaft oder Maklerfirma würde den Ruf dieses Finanzinstituts schädigen, das Vertrauen der Verbraucher in das US- Finanzsystem untergraben und möglicherweise eine weltweite Finanzkrise auslösen.

Sheltered Harbor erhöht die Finanzstabilität der USA sowie die Ausfallsicherheit der Institutionen bei Cyberangriffen, indem kritische Kundenkontodaten und andere Daten unverändert in einem digitalen Vault isoliert werden. Für den Fall, dass die Primär- oder Backupsysteme einer Institution durch einen Cyberangriff wie Ransomware oder ein anderes Ereignis infiziert werden, wird eine schnelle Recovery dieser kritischen Daten ermöglicht. Dadurch wird die Kontinuität kritischer kundenbezogener Bankdienstleistungen erleichtert und das Vertrauen der Öffentlichkeit gewahrt.

Gute Gründe für Cyber Recovery

Dell Technologies ist der erste Lösungsanbieter im Partnerprogramm „Sheltered Harbor Alliance“, der eine gebrauchsfertige Daten-Vaulting-Lösung für US- Finanzinstitute entwickelt hat.

PowerProtect Cyber Recovery für Sheltered Harbor ist die erste gebrauchsfertige Daten-Vaulting-Lösung vor Ort, die von Sheltered Harbor unterstützt wird. Sie erfüllt alle technischen Produktanforderungen für Teilnehmer, die den Sheltered-Harbor-Standard umsetzen.

Data Vault – Die teilnehmenden Institutionen oder Serviceanbieter erstellen nächtliche Backups kritischer Daten im Standardformat von Sheltered Harbor. Der Data Vault ist verschlüsselt, unveränderbar und von der Infrastruktur der Institution isoliert, einschließlich Backup, Disaster Recovery und anderer Data-Protection-Systeme.

Isolierung und Governance – Eine isolierte, sichere Umgebung, die von den Unternehmensnetzwerken getrennt ist, schränkt Nutzer ein, die nicht über eine ordnungsgemäße Freigabe verfügen. Automatisiertes Datenkopien- und Air-Gap-Management gewährleisten die Erhaltung der Datenintegrität, -verfügbarkeit, -sicherheit und -vertraulichkeit.

Recovery und Korrektur – Wenn ein Sheltered-Harbor-Plan für die Ausfallsicherheit aktiviert ist, kann die teilnehmende Institution Daten schnell aus dem Vault wiederherstellen, um die schnellste Wiederherstellung und Wiederaufnahme von Bankgeschäften zu ermöglichen.

Die Herausforderung: Ein Cyberangriff auf die Finanzdienstleistungsbranche könnte eine weltweite Finanzkrise auslösen

Alle Unternehmen sind besorgt über die lähmenden Auswirkungen, die ein bösartiger Cyberangriff auf ihr Geschäft haben könnte, auch wenn 97 % der Unternehmen sensible Daten bei ihren Bemühungen zur digitalen Transformation verwenden.[1] Es ist äußerst lohnend, den Wert von Daten nutzbar zu machen.

Es besteht auch ein erhebliches Risiko, wenn sensible Daten in die falschen Hände geraten, vernichtet werden oder an die Öffentlichkeit gelangen. Malware und Ransomware entwickeln sich weiter und die Angriffe nehmen zu – laut dem 2019 Internet Security Threat Report von Symantec[2] stiegen die Ransomware-Angriffe auf Unternehmen im Jahr 2019 um 12 % und machten damit 81 % aller Ransomware-Bedrohungen aus. Darüber hinaus sind 52 % aller Datenschutzverletzungen im Jahr 2020 in bösartiger Absicht erfolgt. Dies stellt einen Anstieg um 30 % im Vergleich zu vor nur fünf Jahren dar, so ein kürzlich veröffentlichter Bericht des Ponemon Institute.[3]

Darüber hinaus haben sich die Taktiken und Tools der Bedrohungsakteure dahingehend weiterentwickelt, dass sie die Erkennung und die Angriffsprävention nahezu unmöglich machen. Die Taktiken der Cyberkriminalität entwickeln sich weiter: Laut dem Verizon Data Breach Investigations Report 2020[4] sind 30 % der gemeldeten Cyberangriffe von Insidern durchgeführt worden, vor nur drei Jahren waren es noch 25 %.

Die US- Finanzbranche hat laut dem 2019 Annual Cost of Cybercrime Report von Accenture[5] in den letzten drei Jahren die höchsten Verluste aufgrund von Cyberkriminalität erlitten, und diese Kräfte vereinen sich zu einem perfekten Sturm von Bedrohungen, denen sich die globalen Finanzmärkte stellen müssen.

Sheltered Harbor wurde 2015 als gemeinnützige, von der Branche geführte Initiative gegründet, um US- Finanzinstitutionen dabei zu unterstützen, das Risiko eines Cyberangriffs zu verringern, bei dem Kundendaten gefährdet und normale Bankdienstleistungen gestört werden. Die Sheltered-Harbor-Umgebung umfasst teilnehmende Institutionen (US-amerikanische Banken, Kreditgenossenschaften, Maklerfirmen, Vermögensverwalter), nationale Handelsverbände, Lösungsanbieter und Serviceanbieter, die sich für die Verbesserung der Stabilität und Ausfallsicherheit des Finanzsektors bei Cyberangriffen einsetzen.

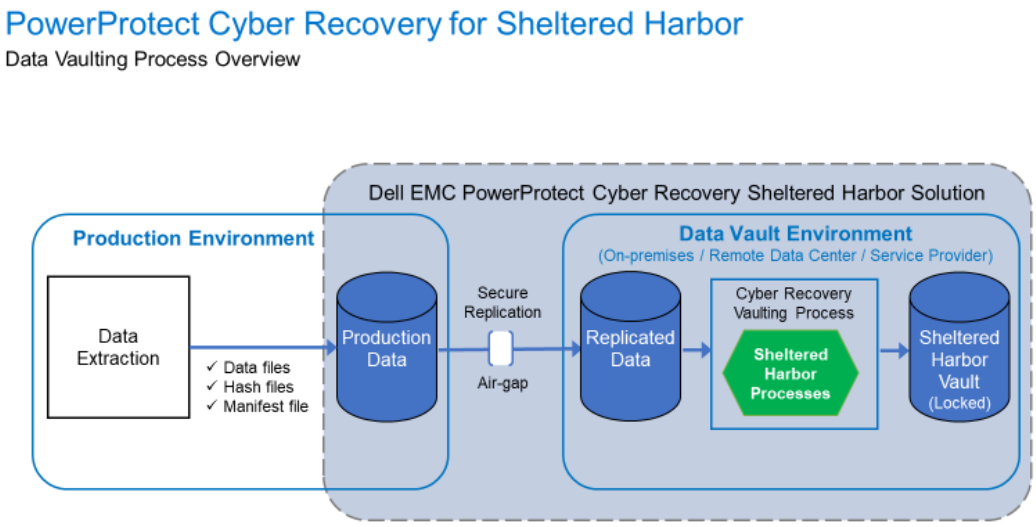
Herkömmliche Disaster Recovery und Business Continuity sind notwendig, um nach einem Natur- oder von Menschen verursachten Ereignis wieder voll einsatzfähig zu sein. Im Zuge eines gezielten, ausgeklügelten Cyberangriffs will Sheltered Harbor sicherstellen, dass die Daten, die zur Wiederherstellung grundlegender Bankgeschäfte erforderlich sind, sofort und integer verfügbar sind, während die Verfahren zur vollständigen Recovery fortgesetzt werden.

© 2020 Dell Technologies oder deren Tochtergesellschaften. Alle Rechte vorbehalten. Dell, EMC und andere Marken sind Marken von Dell Inc. oder Tochtergesellschaften. Andere Marken sind möglicherweise Marken der jeweiligen Inhaber. Referenznummer: H18199

Dell EMC PowerProtect Cyber Recovery für Sheltered Harbor – robuste Ausfallsicherheit bei Cyberangriffen für die kritischsten Daten von Finanzinstituten

Dell Technologies ist der erste Lösungsanbieter, der sich dem Partnerprogramm „Sheltered Harbor Alliance“ anschließt. Unsere empfohlene Lösung für Sheltered Harbor basiert auf Dell PowerProtect Cyber Recovery, einem Marktführer, der seit fast fünf Jahren die kritischsten Daten von Unternehmen vor Cyberangriffen wie z. B. Ransomware schützt.

Um der Sheltered-Harbor-Spezifikation zu entsprechen, wurde die Architektur des Cyber Recovery Vault erweitert, um die Prozesse der Archivgenerierung und des sicheren Repositorys durchzuführen. Die extrahierten Sheltered-Harbor-Daten werden in der Produktion gespeichert und dann über eine logische, dedizierte Air-Gap-Verbindung zur Vault-Umgebung sicher repliziert, wo die restlichen Schritte, wie z. B. die Sperrung der Aufbewahrung, durchgeführt werden.



Durch die Schaffung einer dedizierten, isolierten Umgebung, die physisch von Unternehmensnetzwerken und Backupsystemen getrennt ist, stehen kritische Datensätze, die die Sheltered-Harbor-Teilnehmer schützen müssen, in einem standardisierten Format zur Verfügung, sodass grundlegende Bankdienstleistungen für Kunden schnell wieder aufgenommen werden können. Die Bereitstellung wird in Wochen statt in Monaten gemessen und es besteht die Gewissheit, dass die Spezifikationen von Sheltered Harbor eingehalten werden.

Zusammenfassung

Dell EMC PowerProtect Cyber Recovery für Sheltered Harbor bietet den teilnehmenden Institutionen eine voll unterstützte, schnelle, kostengünstige und effiziente Alternative zum Aufbau eines einmaligen, proprietären Vaults durch jede Institution, um die Einhaltung der Sheltered-Harbor-Spezifikationen zu erreichen. Banken, Kreditgenossenschaften und Maklerfirmen, die den Sheltered-Harbor-Standard implementieren, können sich an Dell Technologies wenden, um eine vollständig unterstützte, gebrauchsfertige Daten-Vaulting-Lösung zu erhalten.

Mit dem zusätzlichen Vorteil der Nutzung einer ausgereiften, Vault-basierten Technologie können Sheltered-Harbor-Teilnehmer, die sich für PowerProtect Cyber Recovery für Sheltered Harbor entscheiden, ihre unmittelbaren Bereitstellungsanforderungen sicher erfüllen und gleichzeitig eine Basis für ihre zukünftigen Anforderungen an das Daten-Vaulting schaffen. Eine teilnehmende Institution verfügt über einen Weg zum Weiterbestehen und das Vertrauen der Öffentlichkeit in das US- Finanzsystem wird aufrechterhalten.

Quellen:

1. 2019 Thales Data Threat Report – www.thalessecurity.com/DTR
2. 2019 Symantec Internet Security Threat Report – https://www.broadcom.com/support/security-center
3. Bericht „Kosten einer Datenschutzverletzung“, 2020, Ponemon Institute, LLC – https://www.ibm.com/de-de/security/data-breach
4. Verizon Data Breach Investigations Report 2020 – https://enterprise.verizon.com/de-de/resources/reports/dbir/
5. 2019 Accenture Cost of Cybercrime report – https://www.accenture.com/us-en/insights/security/cost-cybercrime-study