DELL Technologies

Resumo da solução

PowerProtect Cyber Recovery para o Sheltered Harbor

Proteção de dados essenciais do cliente e preservação da confiança dos consumidores nos mercados financeiros dos Estados Unidos

O QUE É SHELTERED HARBOR?

Criado em 2015 pelo setor financeiro, o Sheltered Harbor padrão incorpora um conjunto de práticas recomendadas e medidas de segurança de resiliência cibernética e proteção de dados para proteger os dados financeiros dos Estados Unidos. As ameaças cibernéticas, incluindo ransomware, destruição de dados ou roubo que visam sistemas de produção e backup, colocam os dados financeiros de consumidores e corporativos em risco.

Um ataque cibernético bem-sucedido a um banco, empresa de crédito ou de corretagem nos Estados Unidos prejudicaria a reputação da instituição financeira, prejudicando a confiança dos consumidores no sistema financeiro dos Estados Unidos e, possivelmente, desencadearia uma crise financeira global.

O Sheltered Harbor aprimora a resiliência cibernética das instituições e a estabilidade financeira nos Estados Unidos ao isolar registros essenciais da conta do cliente e outros dados imutáveis em um cofre digital. Caso os sistemas de backup ou principal de uma instituição sejam comprometidos por um ataque cibernético, como ransomware ou outro evento, a recuperação rápida desses dados essenciais é ativada, facilitando a continuidade dos serviços bancários essenciais voltados para o cliente, garantindo que a confiança pública seja mantida.

POR QUE ESCOLHER O CYBER RECOVERY?

A Dell Technologies é o primeiro Solution Provider do programa de parceria Sheltered Harbor Alliance, que desenvolveu uma solução de armazenamento em cofre de dados turnkey com proteção para as instituições financeiras nos Estados Unidos.

O PowerProtect Cyber Recovery para o Sheltered Harbor é a primeira solução de armazenamento em cofre de dados turnkey no local pronta para ser endossada pelo Sheltered Harbor. Ela atende a todos os requisitos técnicos do produto para que os participantes implementem o Sheltered Harbor padrão.

Cofre de dados – backups noturnos de dados essenciais no formato padrão do Sheltered Harbor são criados pela instituição participante ou pelo provedor de serviços. O cofre de dados é criptografado, inalterado e isolado da infraestrutura da instituição, incluindo backup, recuperação de desastres e outros sistemas de proteção de dados.

Isolamento e governança – um ambiente isolado e seguro desconectado das redes corporativas restringe os usuários que não aqueles com autorização adequada. A cópia de dados automatizada e o gerenciamento de lacunas de ar garantem a preservação da integridade, disponibilidade, segurança e confidencialidade dos dados.

Recuperação e correção – se um plano de resiliência do Sheltered Harbor for ativado, a instituição participante poderá recuperar rapidamente os dados do cofre para possibilitar a restauração e o reinício mais rápidos das operações bancárias.

O desafio: o ataque cibernético ao setor de serviços financeiros pode provocar uma crise financeira global

Todas as organizações ficam preocupadas com o impacto incapacitante que um ataque cibernético mal-intencionado pode ter nos negócios delas, mesmo que 97% das organizações usem dados confidenciais em suas iniciativas de transformação digital.[1] Há uma grande recompensa ao desbloquear o valor dos dados.

Há também um risco significativo se dados confidenciais caírem nas mãos erradas, serem destruídos ou revelados para o público. O malware e o ransomware estão em evolução e os ataques estão em ascensão. Os ataques de ransomware empresarial aumentaram 12% em 2019, sendo 81% de todas as infecções de ransomware de acordo com o relatório de ameaças de segurança da Internet da Symantec de 2019.[2] Além disso, 52% de todas as violações de dados são mal-intencionadas em 2020, acima dos 30% de apenas cinco anos atrás, de acordo com um relatório recente do Ponemon Institute.[3]

Além disso, as táticas e as ferramentas dos atores de ameaças evoluíram para tornar a detecção e a prevenção contra ataques quase impossíveis cada vez mais. As táticas de cibercrime continuam a evoluir, com 30% dos ataques cibernéticos relatados envolvendo insiders, acima dos 25% de apenas três anos atrás, de acordo com o relatório de investigações sobre violação de dados de 2020 da Verizon.[4]

O setor financeiro dos Estados Unidos sofreu as maiores perdas devido à cibercriminalidade nos últimos três anos, de acordo com o relatório do custo anual do cibercrime de 2019 da Accenture[5], e essas forças se combinam em uma verdadeira tempestade de ameaças com que os mercados financeiros globais precisam lidar.

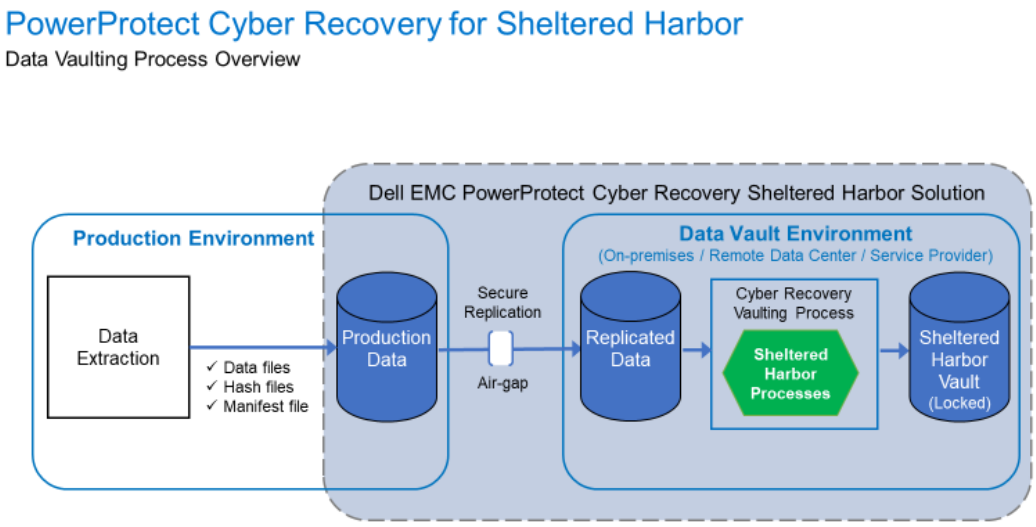
O Sheltered Harbor foi criado em 2015 como uma iniciativa sem fins lucrativos liderada pelo setor para orientar as instituições financeiras dos Estados Unidos e reduzir o risco de ataques cibernéticos que comprometam os dados do cliente e interrompam os serviços bancários normais. O ecossistema do Sheltered Harbor abrange as instituições participantes (bancos, sindicatos de crédito, corretores, gerentes de ativos dos Estados Unidos), associações de comércio nacional, provedores de soluções e provedores de serviços dedicados a aprimorar a estabilidade e a resiliência cibernética do setor financeiro.

A recuperação de desastres tradicional e a continuidade dos negócios são necessárias para ajudar a restaurar os recursos operacionais completos após um evento natural ou feito pelo homem. Após um ataque cibernético sofisticado e direcionado, o Sheltered Harbor visa garantir que os dados necessários para restaurar operações bancárias básicas estejam prontamente disponíveis com integridade, enquanto os procedimentos de recuperação completos continuam.

Dell EMC PowerProtect Cyber Recovery para o Sheltered Harbor – Resiliência cibernética eficiente para dados mais essenciais das instituições financeiras

A Dell Technologies é o primeiro Solution Provider a ingressar no programa de parceria Sheltered Harbor Alliance. Nossa solução endossada para o Sheltered Harbor se baseia na Dell PowerProtect Cyber Recovery, uma líder de mercado com um histórico de quase cinco anos de proteção dos dados mais essenciais das organizações contra ataques cibernéticos, como ransomware.

Para estar em conformidade com a especificação do Sheltered Harbor, a arquitetura do cofre do Cyber Recovery foi estendida para realizar a geração de arquivamento e os processos de repositório seguro. Os dados do Sheltered Harbor extraídos são salvos em produção e, em seguida, replicados de maneira segura por meio de uma conexão lógica, com lacuna e dedicada ao ambiente do cofre, onde as etapas restantes, como o bloqueio de retenção, são executadas.



Ao criar um ambiente isolado e dedicado, fisicamente separado das redes corporativas e dos sistemas de backup, os conjuntos de dados essenciais, que são necessários para proteger os participantes do Sheltered Harbor, estão disponíveis em formato padronizado para que os serviços bancários básicos possam ser rapidamente retomados para os clientes. A implementação é medida em semanas, em vez de meses, e com uma certeza de conformidade com a especificação do Sheltered Harbor.

Resumo

A Dell EMC PowerProtect Cyber Recovery para o Sheltered Harbor oferece às instituições participantes uma alternativa totalmente endossada, rápida, econômica e eficiente para cada instituição que constrói um cofre exclusivo único para alcançar a conformidade com a especificação do Sheltered Harbor. Bancos, sindicatos de crédito e empresas de corretagem que optarem pela implementação do padrão Sheltered Harbor podem usar a Dell Technologies como solução de armazenamento de dados em cofre turnkey totalmente endossada e compatível.

Com o benefício adicional de aproveitar uma tecnologia madura com base no cofre, os participantes do Sheltered Harbor que optarem pelo PowerProtect Cyber Recovery para o Sheltered Harbor podem atender às necessidades imediatas de implementação deles com confiança, bem como estabelecer uma posição de apoio para os futuros requisitos armazenamento de dados em cofre. Uma instituição participante tem um caminho para a sobrevivência e a confiança pública no sistema financeiro dos Estados Unidos é mantida.

Fontes:

1. 2019 relatório de ameaças de dados da Thales – www.thalessecurity.com/DTR
2. 2019 relatório de ameaças de segurança da Internet da Symantec- https://www.symantec.com/security-center/threat-report
3. Custo do relatório de violação de dados 2020, Ponemon Institute, LLC - https://www.ibm.com/security/data-breach
4. Relatório de investigações sobre violação de dados da Verizon 2020 - https://enterprise.verizon.com/resources/reports/dbir/
5. Relatório sobre o custo do cibercrime da Accenture2019 - https://www.accenture.com/us-en/insights/security/cost-cybercrime-study