DELL Technologies

Lösungsübersicht

Dell PowerProtect Cyber Recovery

Moderner und ausfallsicherer Schutz kritischer Daten vor Ransomware und destruktiven Cyberangriffen

Gute Gründe für Cyber Recovery

Cyberangriffe sind auf die Zerstörung, den Diebstahl oder eine anderweitige Kompromittierung Ihrer wertvollen Daten und auch Ihrer Backups ausgelegt. Der Schutz Ihrer kritischen Daten und eine Wiederherstellung mit sichergestellter Integrität ist nach einem Angriff der Schlüssel zur Rückkehr zu einem normalen Geschäftsbetrieb. Könnte Ihr Unternehmen dies überleben? Im Folgenden sind die Komponenten einer cybersicheren Lösung aufgeführt:

Datenisolierung und Data Governance
Eine isolierte Rechenzentrumsumgebung ist von Unternehmens- und Backupnetzwerken getrennt und ein Zugriff ist nur für NutzerInnen mit angemessener Berechtigung möglich.

Automatisierte Datenkopie und Air Gap
Erstellen Sie unveränderliche Datenkopien in einem sicheren digitalen Vault und Prozesse, die zu einem betrieblichen Air Gap zwischen der Produktions-/Backupumgebung und dem Vault führen.

Intelligente Analysen und Tools Innerhalb des sicheren Vaults sind maschinelles Lernen und vollständige Inhaltsindexierung mit leistungsfähigen Analysen verfügbar. Automatisierte Integritätsprüfungen stellen fest, ob Daten durch Malware beeinträchtigt wurden, und Tools unterstützen bei einer möglicherweise notwendigen Korrektur.

Recovery und Korrektur Nach einem Incident wird mittels Workflows und Tools und unter Verwendung dynamischer Wiederherstellungsprozesse sowie bestehender Disaster-Recovery-Verfahren eine Recovery durchgeführt.

Lösungsplanung und -design
Kompetente Beratung bei der Auswahl kritischer Datenvolumen, Anwendungen und anderer wichtiger Ressourcen zur Ermittlung von RTOs und RPOs und zur Optimierung der Recovery.

Die Herausforderung: Cyberangriffe sind der Feind datengestützter Unternehmen

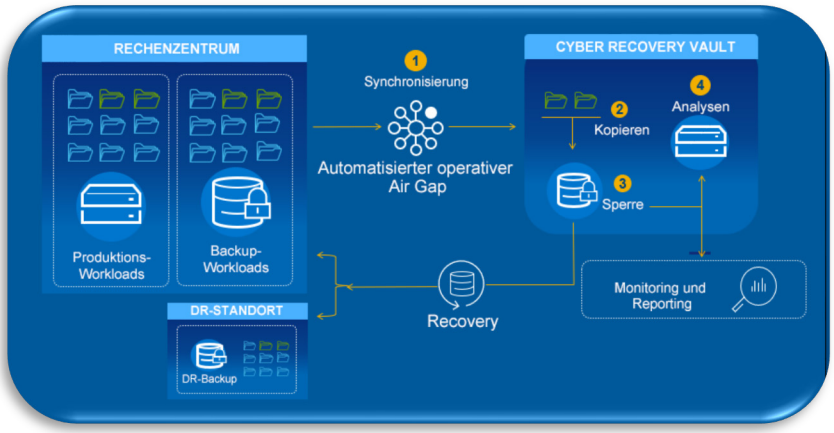
Daten sind die Währung der Internetwirtschaft. Sie stellen eine kritische Ressource dar, weshalb ihr Schutz, ihre Vertraulichkeit und ihre sofortige Verfügbarkeit sichergestellt sein müssen. Der heutige internationale Markt hängt von einem konstanten Datenfluss in miteinander verbundenen Netzwerken ab, und durch die digitale Transformation sind mehr sensible Daten gefährdet als früher.

Dadurch sind Unternehmensdaten für Cyberkriminelle ein attraktives und lukratives Angriffsziel. Unabhängig von der Branche oder der Unternehmensgröße sind Unternehmen und Behörden durch Cyberangriffe stets dem Risiko von infizierten Daten, Umsatzausfällen durch Ausfallzeiten, Rufschäden und teuren Ordnungsstrafen ausgesetzt.

Eine Strategie für die Ausfallsicherheit bei Cyberangriffen ist zu einem Muss für Führungskräfte in Unternehmen und Behörden geworden, doch vielen Unternehmen fehlt das Vertrauen in ihre Data-Protection-Lösungen. Laut dem Global Data Protection Index befürchten 79 % der IT-EntscheidungsträgerInnen, dass es in den nächsten 12 Monaten zu einer Unterbrechung Ihrer Geschäftstätigkeit kommen wird. 75 % befürchten, dass die vorhandenen Data-Protection-Maßnahmen ihres Unternehmens nicht ausreichen, um mit Malware- und Ransomwarebedrohungen umzugehen.[1]

Wie können Sie also Ihr Unternehmen und seine wertvollen Daten sowie Ihre KundInnen und MitarbeiterInnen schützen?

Die Lösung: Dell PowerProtect Cyber Recovery



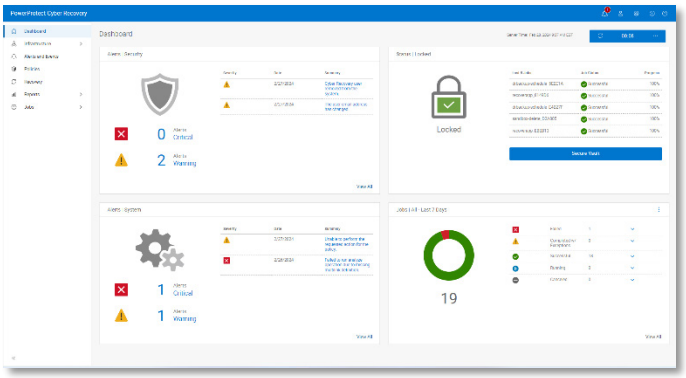
Zur Verringerung der Geschäftsrisiken durch Cyberangriffe und für eine Data Protection mit verstärkter Ausfallsicherheit bei Cyberangriffen können Sie Ihre Recovery- und Business-Continuity-Strategien modernisieren und automatisieren. Gleichzeitig können Sie zur Entdeckung und Abwehr von Cyberbedrohungen die neuesten intelligenten Tools nutzen.

Dell PowerProtect Cyber Recovery bietet einen bewährten, modernen, ausfallsicheren und intelligenten Schutz zur Isolierung kritischer Daten, der Erkennung verdächtiger Aktivitäten und einer beschleunigten Daten-Recovery, sodass Sie schnell wieder Ihren gewohnten Geschäftsbetrieb aufnehmen können.

PowerProtect Cyber Recovery – Unveränderbarkeit, Isolierung und Intelligenz

Cyber Recovery Vault

Der Vault von PowerProtect Cyber Recovery bietet einen mehrschichtigen Schutz und sorgt damit selbst bei Cyberangriffen durch InsiderInnen für Ausfallsicherheit. Kritische Daten werden von der Angriffsfläche entfernt und innerhalb eines geschützten Bereichs des Rechenzentrums isoliert. Für einen Zugriff sind separate Zugangsdaten und eine Multi-Faktor-Authentifizierung notwendig. Zusätzliche Sicherheitsvorkehrungen beinhalten einen automatisierten betrieblichen Air Gap zur Netzwerkisolierung. Infizierbare Managementschnittstellen wurden eliminiert. PowerProtect Cyber Recovery automatisiert die Datensynchronisation zwischen Produktionssystemen, einschließlich Open Systems und Mainframes, und dem Vault. Dabei werden unveränderliche Kopien mit gesperrten Aufbewahrungsrichtlinien erstellt. Bei einem Cyberangriff können Sie rasch eine saubere Datenkopie auswählen, Ihre kritischen Systeme wiederherstellen und Ihr Unternehmen wieder in Gang bringen.



CyberSense

PowerProtect Cyber Recovery ist die erste Lösung mit einer vollständigen Integration von CyberSense. Falls ein Angriff bis ins Rechenzentrum vordringt, bietet CyberSense eine zusätzliche Schutzschicht zur Identifizierung beschädigter Daten. Dieser innovative Ansatz beinhaltet eine vollständige Inhaltsindexierung und nutzt KI-basiertes maschinelles Lernen (ML) zur Analyse von über 200 inhaltsbasierten Statistiken. Dadurch werden Anzeichen durch Ransomware beschädigter Daten erkannt. CyberSense findet beschädigte Daten mit einem Konfidenzniveau von bis zu 99,5 %. Damit hilft es Ihnen bei der Identifizierung von Bedrohungen und der Diagnose von Angriffsvektoren, während gleichzeitig Ihre geschäftskritischen Inhalte geschützt werden – all dies innerhalb des sicheren Vaults.

Recovery und Korrektur

PowerProtect Cyber Recovery bietet automatisierte Wiederherstellungs- und Recovery-Verfahren, sodass geschäftskritische Systeme rasch und verlässlich wieder online gebracht werden können. Die Recovery ist in Ihren Incident-Response-Prozess integriert. Nach einem Ereignis analysiert das Incident-Response-Team die Produktionsumgebung, um die Ursache des Ereignisses zu ermitteln. CyberSense bietet außerdem forensische Berichte nach einem Angriff, um die Reichweite und den Umfang des Angriffs zu verstehen. Die Lösung stellt auch eine Liste der letzten fehlerfreien Backupsätze vor der Beschädigung bereit. Wenn die Produktion dann für die Recovery bereit ist, stellt Cyber Recovery Managementtools und die Technologie zur Verfügung, mit denen die tatsächliche Daten-Recovery durchgeführt wird. Die Lösung automatisiert die Erstellung der Wiederherstellungspunkte, die für Recovery oder die Sicherheitsanalysen verwendet werden.

Lösungsplanung und -design

Optionale Dell Advisory Services helfen Ihnen bei der Ermittlung, welche geschäftskritischen Systeme geschützt werden sollen. Anwendungs- und Serviceabhängigkeiten können dargestellt werden und die notwendige Infrastruktur zu ihrer Wiederherstellung wird ermittelt. Der Service formuliert auch Wiederherstellungsvoraussetzungen sowie Designalternativen und identifiziert Technologien zur Analyse, dem Hosting und dem Schutz Ihrer Daten zusammen mit einem Business Case und einer Zeitskala für die Implementierung.

Für den Schutz Ihrer wichtigen Daten vor Cyberangriffen sind bewährte, moderne und ausfallsichere Lösungen notwendig. PowerProtect Cyber Recovery verschafft Ihnen die Zuversicht, dass Sie nach einem Cyberangriff zweifelsfrei funktionierende Daten schnell identifizieren und wiederherstellen und zum normalen Geschäftsbetrieb zurückkehren können.

[1] Basierend auf einer von Dell Technologies in Auftrag gegebenen Studie von Vanson Bourne, „Global Data Protection Index 2023 Snapshot“, Oktober 2023.

Weitere Informationen zu Dell PowerProtect Cyber Recovery

Kontakt zum Dell Technologies Expertenteam

Weitere Ressourcen anzeigen

Reden Sie mit: #PowerProtect