

Dell EMC PowerProtect Cyber Recovery

Bewährter und moderner 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? Eine bewährte und moderne Cyber-Recovery-Lösung setzt sich aus fünf Komponenten zusammen:

Datenisolierung und Data Governance

Eine isolierte Rechenzentrums-umgebung 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.

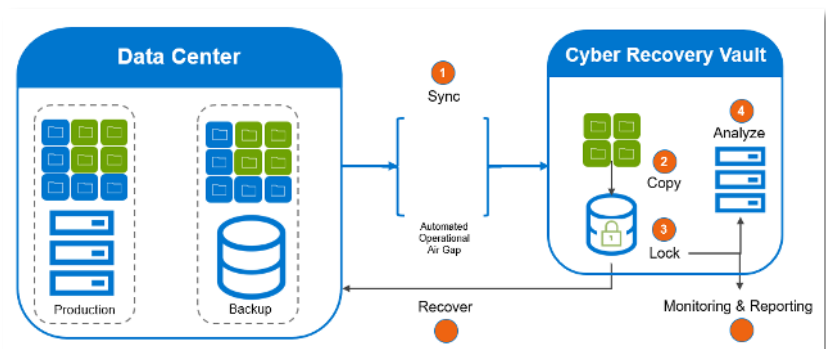
Cyberkriminalität wurde als der größte Wohlstandstransfer der Geschichte bezeichnet. Bei alledem geht es nur um Daten. Accenture schätzt, dass in den nächsten fünf Jahren Daten im Wert von 5,2 Bio. US-Dollar durch Cyberkriminalität gefährdet sind.ⁱ

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. Durchschnittlich erlitten Unternehmen im Jahr 2018 jährliche Kosten durch Cyberkriminalität von 13 Mio. US-Dollar. Dies entspricht einem Anstieg um 72 % während der letzten fünf Jahre.ⁱⁱ

Für Führungskräfte in Unternehmen und Behörden ist es inzwischen eine Pflicht, über eine Cyber-Recovery-Strategie zu verfügen. Laut einer Studie des Jahres 2019 von Marsh und Microsoft bezeichnen 79 % aller globalen Führungskräfte Cyberangriffe als eine ihrer höchsten Prioritäten im Risikomanagement.ⁱⁱⁱ

Wie können Sie also Ihr Unternehmen und seine wertvollen Daten schützen?

Die Lösung: 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 sowie automatisieren. Gleichzeitig können Sie zur Entdeckung und Abwehr von Cyberbedrohungen die neuesten intelligenten Tools nutzen.

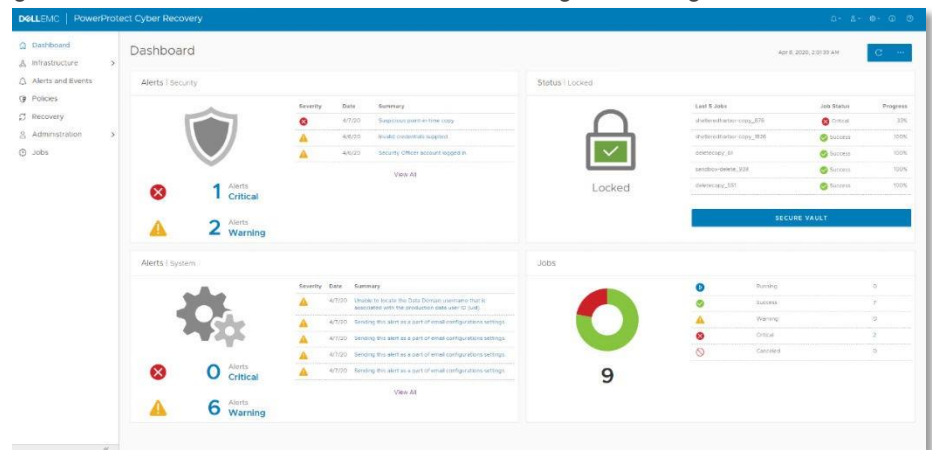
Dell EMC PowerProtect Cyber Recovery bietet einen bewährten, modernen und intelligenten Schutz zur Isolierung kritischer Daten, einer Erkennung verdächtiger Aktivitäten und einer beschleunigten Data Recovery, sodass Sie schnell wieder Ihren gewohnten Geschäftsbetrieb aufnehmen können.

PowerProtect Cyber Recovery – bewährter, moderner und intelligenter Schutz zur Verringerung von Geschäftsrisiken aus Cyberbedrohungen

- **Cyber Recovery Vault** – Der PowerProtect Cyber Recovery Vault bietet mehrere Schutzebenen, um die Ausfallsicherheit gegen Cyberangriffe selbst bei einer Insider-Bedrohung zu gewährleisten. 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.

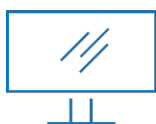
Zusätzliche Sicherheitsvorkehrungen umfassen einen automatisierten betrieblichen Air Gap, der die Netzwerkisolierung gewährleistet und die Managementschnittstellen eliminiert, die infiziert werden könnten.

PowerProtect Cyber Recovery automatisiert die Datensynchronisation zwischen Produktionssystemen und dem Vault. Dabei werden unveränderliche Kopien mit gesperrten Aufbewahrungsrichtlinien erstellt. Im Falle eines Cyberangriffs 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 maschinelles Lernen zur Analyse von über 100 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, um geschäftskritische Systeme schnell und zuverlässig wieder online zu bringen. Als Bestandteil von PowerProtect Data Manager und für Kunden mit Dell EMC NetWorker ermöglicht Cyber Recovery eine automatisierte Recovery aus dem Vault. Dell EMC und das Partnernetz bieten eine umfassende Datenschutzmethodik, bewerten Schäden und führen forensische Untersuchungen durch. Dadurch werden entweder eine Wiederherstellung Ihrer Systeme oder eine Korrektur und Entfernung der Malware angestrebt.
- **Lösungsplanung und -design** – Optionale Dell EMC 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 und moderne Lösungen notwendig. PowerProtect Cyber Recovery verschafft Ihnen die Zuversicht, dass Sie nach einem Cyberangriff bekanntermaßen gute Daten rasch identifizieren, wiederherstellen und zum normalen Geschäftsbetrieb zurückkehren können



[Weitere Informationen](#) zu
Dell EMC PowerProtect
Cyber Recovery



[Kontakt](#) zu einem Dell EMC
Experten

[Quelle: Accenture Die Kosten der Cyberkriminalität Studie 2019]

[Quelle: Accenture Die Kosten der Cyberkriminalität Studie 2019]

[Quelle: Marsh & Microsoft, Global Cyber Risk Perception Study 2019]