DELL Technologies

Serviceübersicht

CYBER RECOVERY SERVICES

Entwickeln Sie Ihre Cyber-Recovery-Strategie und implementieren Sie Ihr Recovery-Programm.

Wesentliche Merkmale

Dell Technologies Cyber Recovery Services:

- Erstellung einer Minimum Viable Company im Cyber-Recovery-Vault, dem die Wiederherstellung der Kerngeschäftsfunktionen nach einem Cyberangriff zugetraut wird
- Beratung zu Ihrer Recovery-Strategie und Ihren Integrationspunkten mit unternehmensweiten Incident-Response-Plänen
- Integration einer am NIST Cybersecurity Framework ausgerichtete Recovery-Lösung, die für eine Vielzahl von Bedrohungsvektoren plant
- Entwicklung und Test von Recovery-Plänen und -Verfahren

Die geschäftliche Herausforderung

Cyberangriffe sind heute allgegenwärtig. Sie können zu verlängerten Ausfallzeiten führen und den Geschäftsbetrieb tage- und sogar wochenlang zum Stillstand bringen – und das kostet Millionen. Abgesehen von der Sorge um die Offenlegung vertraulicher Informationen oder geschützter Daten, kommt es immer häufiger vor, dass viele Cyberangriffe speziell auf die Datenzerstörung oder die Verschlüsselung von Daten und deren Lösegeldforderung ausgerichtet sind. Viele aktuelle Ransomware-Angriffe waren besonders schädlich für Fertigungssysteme, Krankenhausinformationssysteme, Bankingsysteme und lokale Behörden. Diese Angriffe können herkömmliche Sicherheitskontrollen am Perimeter umgehen, so dass der Angreifer über Monate oder manchmal sogar Jahre hinweg unentdeckt bleiben kann, so viele Systeme wie möglich in Mitleidenschaft zieht und das Unternehmen noch weniger auf eine Recovery vorbereitet ist. Zusätzlich zu schädlichen Akteuren außerhalb Ihres Unternehmens ist es leider so, dass zunehmend Insider in Cyberangriffe verwickelt sind, und die Unternehmensführung muss darauf vorbereitet sein, ihr Unternehmen gegen alle Arten von Bedrohungen zu schützen. Diese Faktoren haben dazu geführt, dass Führungskräfte in allen Branchen sicherstellen müssen, dass im Fall eines Cyberangriffs eine Wiederherstellung möglich ist.

Da Cyberangriffe immer ausgefeilter und verheerender werden, müssen Unternehmen neue Anwendungsbeispiele für Data Protection und Cybersicherheit in Betracht ziehen, die eine „letzte Abwehrlinie“ darstellen, um sicherzustellen, dass das Unternehmen einen vernichtenden Cyberangriff überstehen kann.

Servicebeschreibung

Der neueste Ansatz sieht die Aufbewahrung einer vom Produktionsnetzwerk und Produktionsbackupsystemen isolierten Kopie Ihrer kritischsten Daten vor (beispielsweise zentrale Anwendungen, Daten und geistiges Eigentum). Wenn keine direkte Netzwerkverbindung besteht und mehrere Rollbackpunkte verfügbar sind, ist sichergestellt, dass eine unversehrte „Goldkopie“ für die Recovery vorhanden ist.

Dell EMC PowerProtect Cyber Recovery unterstützt Sie bei der Realisierung eines Data-Protection-Vault mit Airgap und beschleunigt in Verbindung mit Dell Technologies Services die Einführung der Technologie und Prozesse, um das Vertrauen in Ihre Fähigkeit zur Wiederherstellung nach einem Cyberangriff zu erhöhen. Unsere Services konzentrieren sich auf zwei Hauptbereiche: Beratung und Implementierung.

Der Schwerpunkt der Beratungsphase liegt auf der Bereitstellung von Empfehlungen für die Integration und Optimierung der Cyber Recovery in Ihrer Data-Protection-Umgebung. Dies wird durch die Analyse Ihres aktuellen und zukünftigen Status erreicht, um eine maßgeschneiderte Strategie für die Cyber-Recovery-Vorbereitung zu erstellen, die eine enge Abstimmung mit den Geschäftsanforderungen für Schutz und Recovery gewährleistet.

Eine Kernkomponente der Beratungsphase ist ein Workshop und eine Informationssitzung, um Daten über Ihre Anwendungen zu sammeln und deren Kritikalität für den normalen Geschäftsbetrieb zu verstehen. Diese Überlegungen helfen bei der Erstellung von Empfehlungen, was durch den Cyber-Recovery-Vault geschützt werden sollte und Ihre Minimum Viable Company ausmacht – eine Erfassung Ihrer kritischsten Daten und Anwendungen, die dazu verwendet werden können, zuerst die Kernfunktionen wiederherzustellen und den Geschäftsbetrieb wieder aufzunehmen.

In der Implementierungsphase wird die Cyber-Recovery-Lösung in Ihre Data-Protection-Umgebung integriert. In dieser Phase können die in der Beratungsphase gesammelten Informationen verwendet werden, um die Lösung an Ihre exakten Anforderungen anzupassen. Außerdem können wir zusätzliche Technologien und Funktionen in Ihre Cyber-Recovery-Umgebung integrieren, darunter:

- Bereitstellung der Vault-Infrastruktur
- Bereitstellung von CyberSense-Analysen zur Analyse von Daten und zur Identifizierung von Frühindikatoren für eine Gefährdung
- Änderung von Produktionsbackups zur Unterstützung von Cyber-Recovery-Vault-Anforderungen
- Verstärkung der zusätzlichen Produktionsinfrastruktur von Dell Technologies
- Integration von Cyber-Recovery-Vault und Funktionen in Mainframe-Umgebungen
- Erstellung eines Cyber-Recovery-Vault, um mehrere Plattformen, heterogene Technologien, Aufbewahrungs-Policies und Anwendungen einzubeziehen
- Entwicklung detaillierter Betriebsverfahren (Recovery Runbooks) zur Durchführung einer Recovery aus dem Vault
- Support bei der Erstellung von erweiterten Recovery Runbooks und zusätzlichen Testszenarien

Zusammenfassung der Vorteile

Aufgrund der starken Zunahme von Cyberangriffen ist es heute eine Frage des Wann und nicht des Ob, ob ein Unternehmen betroffen ist. Jedes Unternehmen hat seine eigenen Ziele und IT-Anforderungen, die von seinen Strategien zur Antwort auf Cyber-Incidents und zur Cyber Recovery erfüllt werden müssen. Unsere BeratungsexpertInnen arbeiten mit Ihnen an der Entwicklung von Prozessen und Verfahren, mit denen Sie Ihr Unternehmen im Fall eines verheerenden Cyberangriffs schützen und wiederherstellen können.

Dell Technologies Services bietet Folgendes:

- Eine Cyber-Recovery-Vault-Lösung mit Airgap und Empfehlungen, um Ihre Minimum Viable Company im Vault zu erstellen und eine Recovery im Falle eines Cyberangriffs zu ermöglichen.
- Wir helfen Ihnen, Ihre Compliance-Ziele bei immer strenger werdenden gesetzlichen Auflagen zu erreichen, indem Sie die Recovery-Funktionen bestimmter Kernanwendungen schützen und nachweisen.
- Einbindung einer am NIST Cybersecurity Framework ausgerichteten Recovery-Strategie in ihre Vorbereitungen zur Reaktion auf Incidents