Datentresor gegen Ransomware-Erpresser

DELL Technologies
TITANIUM PARTNER

Ransomware-Attacken verursachen weltweit jedes Jahr Schäden in Milliardenhöhe. Dell hat seine PowerProtect DD-Serie (Data-Domain) um einen speziellen Schutz erweitert.

Ransomware ist in den vergangenen Jahren zur größten Malware-Bedrohung für Unternehmen geworden. Die Software verschlüsselt die internen Daten einer Organisation oder verwehrt den Usern den Zugriff darauf. Erst nach Zahlung der geforderten Summe geben die Erpresser die Daten wieder frei. Oder auch nicht: Oft kommt es vor, dass die Täter mit dem Geld untertauchen, ohne sich noch einmal zu melden. Doch egal, ob ein Unternehmen der Forderung nachkommt oder nicht: Der Schaden ist auf jeden Fall immens und erreicht teilweise dreistellige Millionenbeträge. Die Methoden der Ransomware-Programmierer sind in den letzten Jahren immer raffinierter geworden und damit auch immer schwerer abzuwehren. Da Backups einen gewissen Schutz versprechen, greift die Schadsoftware mittlerweile oftmals gezielt die Sicherungssysteme des Unternehmens an, löscht sämtliche vorhandenen Daten und führt eine Neuinitialisierung der Systeme durch. Es sind daher neue Konzepte für den Schutz der Daten erforderlich.

Wie sich Unternehmen schützen können

Das amerikanische National Institute of Standards and Technology (NIST) empfiehlt Unternehmen einen mehrstufigen Schutz ihrer Daten. Er umfasst zum einen die klassischen Daten-Backups, wie sie heute glücklicherweise von praktisch allen Firmen vorgenommen werden. Hinzu kommen unter anderem regelmäßige Sicherungen der Daten auf einem speziell dafür ausgelegten Backup-Server, Berechtigungen für den Zugriff auf die Backups und die Definition dedizierter Backup-User sowie in der Praxis bewährte Konzepte wie die 3-2-1-Regel: Drei Kopien der Daten liegen auf zwei Medien, von denen eine Kopie extern gelagert wird.

Für Backups, die höchsten Ansprüchen an Sicherheit genügen, bietet Dell die Modelle der PowerProtect DD-Reihe an. Die Maschinen speichern die Unternehmensdaten auf Disk, wobei es sich in erster Linie um Festplatten handelt, einige Modelle verfügen auch über SSDs. Um den vorhandenen Platz bestmöglich zu nutzen, werden die Daten von der PowerProtect DD per Hardware dedupliziert. Die Maschinen eignen sich daher sowohl für die Aufnahme regelmäßiger Backups wie auch für die längerfristige Archivierung. Sie wurden zudem von vornherein auf höchste Sicherheit getrimmt und bieten dazu beispielsweise einen Retention Lock: Die Funktion sorgt dafür, dass die gesicherten Daten für einen einstellbaren Zeitraum weder verändert noch gelöscht werden können. Dabei unterstützt die PowerProtect DD zwei unterschiedlich strenge Level: In der Governance-Variante lässt sich der Retention Lock bei Bedarf aufheben.

concat AG
IT SOLUTIONS

We unlock the Promise of Technology

Ist jedoch die Variante Compliance eingestellt, funktioniert das nicht mehr, die Sperre ist dann bis zum Ende des eingestellten Zeitraums fest. Wählt der Anwender diese Option, erfüllt die PowerProtect DD die Vorgaben der staatlichen Behörden für die sichere Aufbewahrung von Daten. Der Retention Lock der PowerProtect DD wird unterstützt von den Backup-Anwendungen Dell PowerProtect Data Manager und NetWorker sowie einigen Produkten anderer Hersteller. Ein zusätzliches Sicherheits-Feature der PowerProtect DD nennt sich DDBoost. Dabei handelt es sich um ein von Dell entwickeltes Protokoll, das es ermöglicht, die Maschinen direkt in Backup-Anwendungen zu integrieren. In diesem Fall lässt sich die Deduplikation der Daten bereits auf dem Backup-Server beziehungsweise dem -Client durchführen. Dadurch reduziert sich die benötigte Netzwerkbandbreite und die Zeit für die Datenübertragung sinkt.

Erweiterter Schutz gegen Ransomware-Attacken

Aufgrund der steigenden Bedrohung durch Ransomware-Angriffe hat Dell eine Schutz-Software entwickelt, die in ihrem Konzept und den Möglichkeiten derzeit einmalig ist. Cyber Recovery setzt auf die bewährte PowerProtect DD-Technologie auf und erweitert diese um einen Schutz der Backupdaten vor Angriffen durch Ransomware.
Sobald es einem Angreifer gelingt, die Backup-Umgebung unter seine Kontrolle zu bekommen, ist es dem Unternehmen ohne diese letzte Verteidigungslinie nicht mehr möglich, Restores seiner Produktivumgebung durchzuführen. Ausgehend von der Beobachtung, dass moderne Ransomware zunehmend auf die Backup-Systeme in den Unternehmen abzielt und danach trachtet, sie zu deaktivieren oder zu kontrollieren, entstand bei Dell das Konzept für einen Vault, also einen Tresor, der für Angreifer absolut unzugänglich ist. Dieser Cyber Recovery Vault (CR Vault) speichert eine Art Goldkopie der Unternehmensdaten, sodass sich der vorherige Datenstand jederzeit wiederherstellen lässt. Mehr noch: Der Cyber Recovery Vault kann auch den Backup-Server selbst aufnehmen und auf diese Weise die Funktionsfähigkeit der Wiederherstellungsroutinen sicherstellen. Bei den Backup-Lösungen Dell Networker und Data Manager lässt sich dieser Vorgang sogar automatisieren, bei anderen Sicherungsprodukten muss der Administrator den Server manuell aufsetzen. Dann ist es möglich, nicht nur die von der Malware blockierten Datensätze, sondern auch den fertig konfigurierten Server zurückzuspielen und auf diese Weise innerhalb kürzester Zeit wieder eine saubere und funktionierende Produktionsumgebung herzustellen.
Die Basis für Dell Cyber Recovery bilden zwei Power-Protect DD-Systeme. Die eine Maschine ist in die Produktivumgebung eingebunden, üblicherweise als Backup-Target. Sie repliziert ihre Daten auf die zweite PowerProtect DD, den Cyber Recovery Vault. Dieser Vault steht in einem eigenen, abgeschlossenen Raum, zu dem nur ein ausgesuchter Personenkreis Zutritt hat – laut Statistik erfolgen die meisten Datendiebstähle in den Unternehmen durch interne Mitarbeiter. Er ist nicht an ein Netzwerk angeschlossen, sondern durch ein virtuelles Air Gap von allen anderen Systemen separiert. Damit im Rahmen der Replikation überhaupt eine Datenübertragung erfolgen kann, öffnet die Cyber-Recovery-Software auf der PowerProtect DD-Maschine im Vault über eine Policy den physischen Replikations-Port und überträgt die Daten vom Backup-Server zum Vault.

Wichtige strategische Überlegungen im Vorfeld eines Cyber-Recovery-Projektes

Bestimmung der kritischen Daten

Unternehmen müssen evaluieren, welche die entscheidenden Daten sind, um nach einem Cyber-Angriff den Geschäftsbetrieb wieder aufnehmen zu können.

Bewertung der Datenmenge

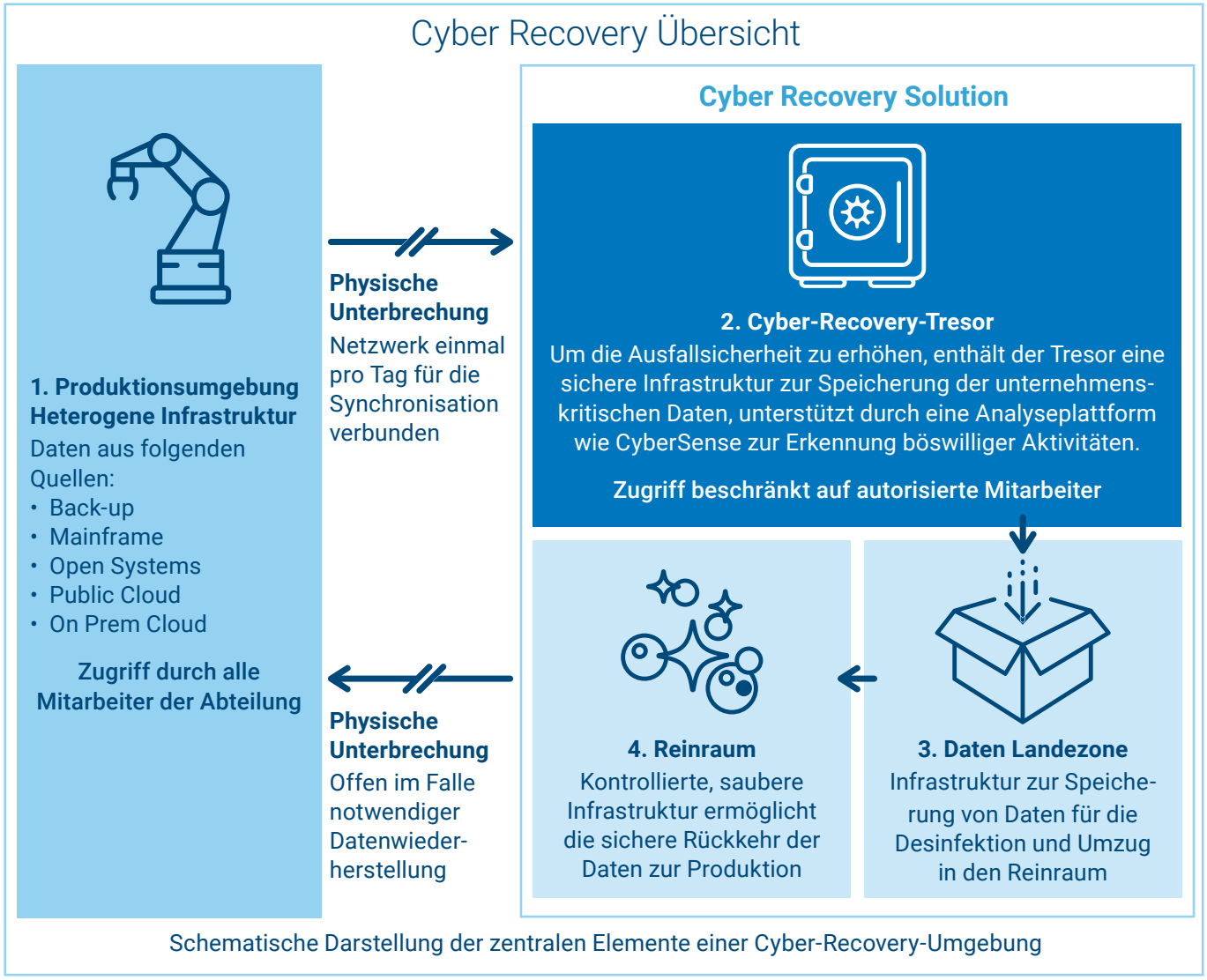
Kritische Daten machen durchschnittlich zwischen 10 und 15 % der Gesamtdaten eines Kunden aus. Im Falle eines Angriffs führt der Tresor die kritischsten Daten des Unternehmens wieder in die Produktion zurück.

Definition des Zeitrahmens für die Wiederherstellung

Das Unternehmen muss definieren, wie der Zeitplan für die Wiederherstellung nach einem katastrophalen Angriff aussehen soll.

Berücksichtigung der Cloud-Strategie

Klärung der Fragen, welche Datensätze bzw. Dienste sich in der Cloud befinden, wie diese geschützt werden können und ob sie im Falle eines Cyber-Angriffs dringend benötigt werden.



Schematische Darstellung der zentralen Elemente einer Cyber-Recovery-Umgebung

Sobald sämtliche Daten ihr Ziel erreicht haben, wird die Verbindung von der Software wieder geschlossen. Als zusätzliche Schutzfunktion ist im Cyber Recovery Vault ein Dateisystem eingerichtet, das jegliche Veränderung der Daten ausschließt (Write Once Read Many – WORM). So sind sie nicht nur vor Bearbeitungen geschützt, sondern gleichzeitig auch vor böswilligen Crypto-Verschlüsselungen, wie sie oft bei Ransomware-Angriffen eingesetzt werden.

Zusätzliche Analyse auf Malware-Befall

Ein großes Problem bei herkömmlichen Backup-Systemen ist, dass die Daten, die im Rahmen eines Recovery zurückgespielt werden sollen, ebenfalls bereits von einer Malware befallen sind. Antiviren-Software kann diese Gefahr minimieren, gänzlich ausschließen lässt sie sich jedoch nicht. Bei der Goldkopie der Daten eines Unternehmens wäre es besonders fatal, wenn sie aufgrund der Aktivitäten einer Malware unvollständig oder manipuliert oder sogar selbst befallen wäre. Da der Cyber Recovery Vault jedoch die meiste Zeit keine Verbindung mit der Außenwelt hat, ist es nicht möglich, dort eine Antiviren-Lösung einzurichten, die ständig aktuell mit Malware-Definitionen versorgt wird.
Um eine Veränderung oder Verunreinigung der Goldkopie so weit wie möglich auszuschließen, ist Dell EMC eine Partnerschaft mit dem US-Unternehmen Index Engines eingegangen, Hersteller der Security-Software CyberSense. Diese optional lizenzierbare Anwendung analysiert Backupdaten auf Merkmale und Veränderungen, die auf eine Malware-Infektion hinweisen. Dabei wendet sie sowohl heuristische Methoden wie auch Methoden des Machine Learning an und vergleicht zudem die auf dem Vault eingehenden Backup-Daten mit bereits bestehenden, älteren Datenbeständen.
Die Software überwacht kontinuierlich die ankommenden Daten und sucht beispielsweise nach Auffälligkeiten in der Bit-Struktur und Hinweisen auf Verschlüsselungen. Außerdem achtet sie auf den Anteil von veränderten Daten in den eingehenden Backup-Sätzen – wenn sich dieser Prozentsatz plötzlich deutlich verändert, schlägt sie sofort Alarm. Die Benachrichtigung des zuständigen Administrators erfolgt dann per E-Mail. Auf diese Weise lassen sich Verunreinigungen in der Goldkopie direkt feststellen. So gewährleistet CyberSense den Restore aus sauberen Backupdaten und schließt die Gefahr einer erneuten Verschlüsselung nahezu aus.

Wirksamer Schutz vor Erpressung

Die Kombination aus PowerProtect DD-Maschinen, Backup-Software, Dell Cyber Recovery und CyberSense ist nicht fest, sondern lässt sich flexibel an Budget und Anforderungen des jeweiligen Unternehmens anpassen. Management und IT-Abteilung haben mehrere Optionen, beispielsweise ob die komplette Produktionsumgebung in der Vault gesichert werden soll oder ob es genügt, die wichtigsten Unternehmensdaten vor dem Zugriff von Kriminellen zu schützen. Das ist nicht nur eine Kostenfrage, sondern auch eine Frage der Recovery-Geschwindigkeit: Das zusätzliche Backup der Produktionsumgebung erfordert zwar ein größeres Speichervolumen, erspart jedoch ein Neuaufsetzen des gesamten Systems und verkürzt damit die Zeit, bis die IT wieder zur Verfügung steht.
Dell Cyber Recovery stellt derzeit den wohl wirksamsten Schutz gegen den Versuch der Erpressung durch das Einschleusen von Ransomware dar. Die Software erfordert jedoch eine gründliche Analyse der Situation beim Kunden und eine eingehende Beratung.

Die Concat AG unterstützt Sie mit entsprechenden Consulting Services. Sie umfassen unter anderem Workshops vor Ort beim Kunden, Analysen des derzeitigen und des gewünschten, zukünftigen Status, die Entwicklung einer Strategie zusammen mit dem Kunden sowie die Integration der angepassten Lösung in die Data-Protection-Umgebung des jeweiligen Unternehmens. Unternehmen bekommen so auf diesem Weg genau die Cyber-Recovery-Lösung, nach der sie verlangen und die sie benötigen.

Sie möchten aus Gründen des Datenschutzes (z. B. DSGVO) und der IT-Sicherheit Ihre Daten in eine andere Domain außerhalb des Unternehmens replizieren? Dann sind wir der richtige Dienstleister für Sie. Mit unserem gemanagten Service haben Sie die Gewissheit, dass Ihre Backups sicher und DSGVO-konform in der Concat-Cloud aufbewahrt werden.

Unsere Experten beantworten gerne Ihre Fragen zu Cyber Recovery. Schreiben Sie per E-Mail an:
info@concat.de

Weitere Informationen auf:
www.concat.de/partner/dell/dell-cyber-recovery

Concat AG IT Solutions
Seit 1990 realisieren wir maßgeschneiderte IT-Infrastrukturen. Auf Wunsch erbringt unsere Managed-Service-Organisation dafür Support- und Betriebsleistungen (24×7). Darüber hinaus bieten wir Private-Cloud-Enterprise-Lösungen und schlanke, voll gemanagte Dienste im Hybrid- und Public-Cloud-Bereich. Alle Daten liegen verschlüsselt in deutschen Rechenzentren (zertifiziert nach ISO 9001 und ISO 27001).

concat AG
IT SOLUTIONS
A Meridian Group International Company

Concat AG
Berliner Ring 127–129
64625 Bensheim

Telefon: 06251 7026-0
E-Mail: info@concat.de
www.concat.de