DELL Technologies
TITANIUM PARTNER

GLOBAL INFORMATION DISTRIBUTION

Quellle: IT-Business, Dr. Stefan Riedl, Ransomware muss draußen bleiben, Ausgabe 19/2024.

RANSOMWARE MUSS DRAUßEN BLEIBEN!

Der Angstgegner der IT-Verantwortlichen heißt Ransomware. Das Systemhaus GID sorgt bei Kunden als Dell-Partner produktseitig mit dem „Cyber Vault“ vor und setzt finanzierungsseitig auf die Möglichkeiten der Dell-eigenen Bank „Dell Financial Services‘ (DFS).

Die Entwicklung zum Ransomware-Bekämpfer

Der Weg zum Ransomware-Bekämpfer mit Dell-Technologie erscheint rückblickend wie vorgezeichnet: Mit der Digitalisierung haben sich ab 2008 sukzessive neue Schwerpunkte ergeben, nämlich Backup und Deduplizierung mit der DataDomain-Appliance von EMC als Ersatz für Tape-Libraries. Beim Thema VMware-basierte Lösungen für Hyperconverged Infrastructure (HCI) wurde sich mit VxRail von EMC positioniert. Im Jahr 2016 hat Dell Technologies die Firma EMC gekauft und so wurde GID Dell-Partner, inzwischen mit dem Partner-Status „Titanium“.

Ein typisches Projekt startet bei GID immer mit einer „Live-Optics-Analyse“. Das Tool analysiert die bestehende IT-Infrastruktur hinsichtlich Kapazität, Memory, Auslastung, Peaks, Virtuelle Maschinen et cetera. Damit wird in die Diskussion mit dem Kunden gegangen und abgeglichen, ob er seinen Ist-Zustand so bestätigen kann. Gemeinsam wird dann für einen Lösungsvorschlag überlegt, welche Entwicklungen und Anforderungen in den kommenden drei bis fünf Jahren im Raum stehen und wie dem begegnet werden kann.

Die Grundlage der Projekte

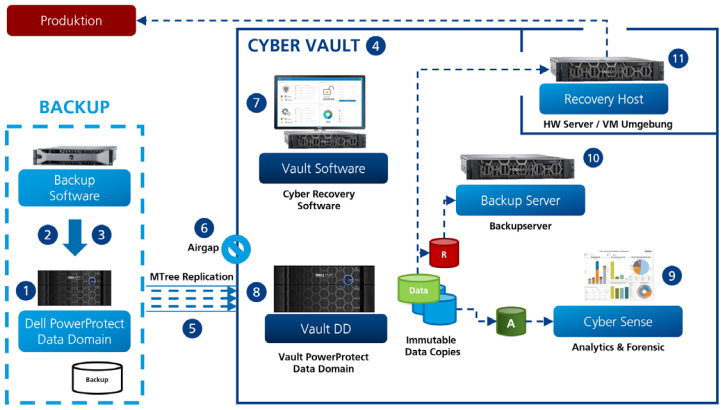
Viele der Projekte basieren dieser Tage auf der Cyber-Vault-Lösung von Dell, bestehend aus Backup Software und einer Backup-Appliance. Damit sollen mehrere Möglichkeiten umgesetzt werden können, in Ransomware-Zeiten das Backup dahingehend zu schützen, dass es unkompromittiert bleibt und die Produktivsysteme wieder hochgefahren werden können. Friedrich Förster beschreibt: „Die Daten werden im WORM-Modus gesichert, also Write Once - Read Many. Die Lösung speichert hinter einer Firewall und nutzt dabei Air-Gap*-Technologie. Die Software CyberSense, die zwar nicht von Dell ist, aber im Paket mit vertrieben wird, scannt die zu sichernden Daten auf Inhaltsebene, sodass vermieden wird, dass das Backup kompromittiert wird.“ All das sei vom Gedanken getragen, dass es keine Frage des „ob“, sondern des „wann? ist, dass man von Ransomware verschlüsselt wird.

* **Air Gap** (englisch für „Luftspalt“) meint einen Prozess, der zwei IT-Systeme physisch und logisch voneinander trennt, aber dennoch die Übertragung von Daten zulässt.

Das Konzept des Cyber-Vaults

Die 3-2-1-Backup-Regel fordert eine räumlich getrennte Kopie. Dies kann über S3-bjektspeicher in einem Hyperscaler-Rechenzentrum vorgenommen werden, allerdings würden viele Kunden, insbesondere die öffentliche Hand, nicht auf die Hyperscaler setzen wollen. Dann werden Lösungen umgesetzt, bei denen die Kopie über den Cyber Vault an einem zweiten und gegebenenfalls auch dritten eigenen Standort intern gesichert wird. Früher fehlte für solch umfassende Lösungen vielerorts schlichtweg das Budget, „aber Ransomware hat hier Tatsachen geschaffen und die Kunden sind bereit, entsprechend in ihr System zu investieren", verrät der GID-Chef.

Das Konzept des Cyber-Vaults bietet eine mehrschichtige Sicherheitslösung für den Schutz und die Wiederherstellung von Daten. Durch die Kombination aus unveränderlichen Datenkopien, Air Gap, Cyber-Recovery-Software und forensischen Analysen soll sichergestellt werden, dass Unternehmen im Falle eines Angriffs wieder auf ihre Daten zugreifen können.



1. Dell PowerProtect Data Domain (DD)
2. DD Boost-Protokoll
3. Funktion "Retention Lock" (WORM)
4. Aufbau Cyber Vault
5. Firewall
6. Air Gap
7. Dell Cyber Recovery Software
8. Dell PowerProtect DD im Vault
9. Cyber Sense Software
10. Backup Server
11. Recovery Host

1. **Dell PowerProtect Data Domain (DD):** Das primäre Backup-Speichergerät in der Produktionsumgebung. Hier werden die Daten initial dedupliziert und gesichert.
2. **DD Boost-Protokoll:** Dieses Protokoll ermöglicht die effiziente Datenübertragung vom Backup-Server zur Data Domain, reduziert die Datenmenge und beschleunigt den Backup-Prozess. DD-Boost wurde, anders als CIFS oder NFS, bisher nicht angegriffen.
3. **Retention Lock-Funktion (WORM)**: Hierbei handelt es sich um eine Funktion, die die gesicherten Daten vor Manipulation schützt, indem sie in einem „Write Once, Read Many"-Format (WORM) gespeichert werden. Dies sorgt für unveränderliche Datenkopien.
4. **Aufbau des Cyber Vault:** Der Cyber Vault ist eine isolierte Umgebung, die von der Produktionsumgebung getrennt ist. Er ist durch eine Firewall (5) geschützt.
5. **MTree-Replikation:** Die gesicherten Daten werden über MTree von der primären Data Domain zur Data Domain im Vault repliziert.
6. **Air Gap:** Dies ist eine physische oder logische Trennung zwischen der Backup-Umgebung und dem Cyber Vault. Diese Isolation verhindert, dass im Falle eines Angriffs auf die Produktionsumgebung auch der Cyber Vault kompromittiert wird .Über die Air Gap-Funktion wird gesteuert, dass die Vault DD in der Nacht nur wenige Stunden, nämlich während der benötigten Zeit für die Datenübertragung, erreichbar ist.
7. **Dell Cyber Recovery Software:** Diese Software verwaltet die Cyber Vault-Infrastruktur und die Wiederherstellungsvorgänge. Sie überprüft und orchestriert die Schritte zur Datenwiederherstellung im Falle eines Cyberangriffs.
8. **Vault PowerProtect Data Domain:** Diese Data Domain im Cyber Vault speichert die replizierten, unveränderlichen Datenkopien und dient als zweites Backup-System.
9. **Cyber Sense Software:** Die Software führt Analysen und forensische Untersuchungen der gesicherten Daten durch, um verdächtige Aktivitäten oder Manipulationen zu erkennen. Sie bietet Einblicke in potenzielle Cyberangriffe, indem sie die Datenintegrität überprüft.
10. **Backup Server im Vault:** Dies ist der Backup-Server innerhalb des Vaults, der im Notfall zur Wiederherstellung der Daten verwendet wird.
11. **Recovery Host:** Ein spezieller Server oder eine virtuelle Maschine, auf der die wiederhergestellten Daten in einer isolierten Umgebung getestet und für die Rückkehr in die Produktionsumgebung vorbereitet werden.

Der Faktor Mensch im Ransomware-Schutz

Abseits der Technik sei ein wichtiger Baustein beim Schutz vor Ransomware die ‚Awareness der Mitarbeiter, die beispielsweise wissen müssen, dass man einen auf dem Firmenparkplatz gefundenen USB-Stick eben nicht einfach einstöpseln soll. Und auch ein kritischer Umgang mit QR-Codes und Links sei unabdingbar. „Wir sind Teil eines Systemhausverbundes, der Medialine Group, die in diesem Zusammenhang in Sachen Awareness, Workshops sowie Schulungen und Aufklärung sehr engagiert sind", sagt der Manager.

Finanzielle Flexibilität durch Dell Financial Services

Als Dell-Partner spielt die Zusammenarbeit mit der konzerneigenen Dell Financial Services (DFS), die über eine eigene Bank-Lizenz verfügen, eine wichtige Rolle, denn die Zeiten, in denen IT-Anschaffungen und -Dienstleistungen einfach in bar bezahlt werden, neigen sich dem Ende. DFS ermögliche es, „Lösungen zur Miete oder in einem Leasingmodell oder einem wie auch immer gearteten APEX-Modell bereitzustellen wie beispielsweise Storage-Dienste mit einem Grundbetrag und einer nutzungsabhängigen Komponente." Für GID als Systemhaus hat die Abwicklung über DFS eigentlich nur Vorteile, so Friedrich Förster und begründet: „Bei einem Leasing-Geschäft schicken wir beispielsweise unsere Rechnung einfach an DFS und die regelt den Rest mit dem Kunden." Auch sehr nützlich sei die Bonitätsprüfung des Kunden durch die DFS, wenn diese involviert ist - das minimiere Zahlungsausfälle.

Der Partner GID

Die Global Information Distribution GmbH (GID) als Systemhaus und -integrator berät und bietet Lösungen in den Bereichen Infrastruktur, Hyperconverged Infrastructure (HCI), Storage, Backup und Recovery an. Langjährige Erfahrung und bei namhaften Partnern zertifizierte Spezialisten in Vertrieb und Technik setzen die Projekte um und halten so die IT ihrer Kunden auf Erfolgskurs.

GID wurde 1994 in Köln gegründet und ist ein deutschlandweit agierendes Systemhaus. Neben dem Hauptsitz in Köln gibt es Niederlassungen in Form von Vertriebs- und Servicestandorten in Augsburg, Berlin, Halle (Saale), Frankfurt und Stuttgart, in denen derzeit 35 Mitarbeiterinnen und Mitarbeiter beschäftigt sind. Weitere Informationen zu den Produkten und Services der GID GmbH finden Sie unter https://www.gid-it.de oder folgen Sie uns auf LinkedIn, XING und Facebook.

Global Information Distribution GmbH.
Wissen bewahren - Zukunft sichern.

GLOBAL INFORMATION DISTRIBUTION

MEDIALINE GROUP

DELL Technologies TITANIUM PARTNER

Global Information Distribution GmbH
Headquarter
Brügelmannstr. 5
50679 Köln

Telefon: +49 (0) 221 837902-0
Telefax: +49 (0) 221 837902-30
E-Mail: info@gid-it.de
Web: https://www.gid-it.de

GID in Ihrer Nähe
Standort Augsburg
Morellstr. 33, 86159 Augsburg
Telefon: +49 (0) 821 25849-0
E-Mail: augsburg@gid-it.de

Weitere Vertriebsstandorte
Berlin berlin@gid-it.de
Halle halle@gid-it.de
Frankfurt frankfurt@gid-it.de
Stuttgart stuttgart@gid-it.de