DELL Technologies
TITANIUM PARTNER

GLOBAL INFORMATION DISTRIBUTION

RANSOMWARE IST DER ANGST-GEGNER NUMMER 1

GID und Dell Technologies treffen Vorsorgemaßnahmen für ihre Kunden mit der Schutz-Software „Cyber Recovery“

Unsere Erfahrungen mit Ransomware

Die Anzahl der Ransomware Angriffe steigt dramatisch. Die Frage ist nicht, ob der Kunde angegriffen und verschlüsselt wird, sondern eher wann dieser Fall eintritt. Durch die vielen Fälle, die täglich in den Medien zu hören oder zu lesen sind, steigt die Sensibilität. Waren die Kunden vor zwei bis drei Jahren oberflächlich interessiert, so kann man heute eine intensive Diskussion mit den IT-Verantwortlichen führen. Budgets werden geplant und erste Projekte erfolgreich umgesetzt.

Das Strickmuster ist unterschiedlich. Oftmals werden die Kunden zunächst im Backup verschlüsselt und dann geht der Angreifer systematisch auf die Primärsysteme über. Je nachdem, wann der Kunde die Attacke bemerkt, kann er retten, was zu retten ist: Stecker ziehen, Notfallhandbuch, Schaden feststellen, Equipment beschaffen, System neu aufbauen, usw.. Vielfach muss eine Meldung an das BSI (Bundesamt für Sicherheit in der Informationstechnik) erfolgen, die dann dazu führt, dass die betroffenen Systeme zwecks Täterermittlung zunächst untersucht werden müssen und bis zum Abschluss nicht genutzt werden dürfen. Das kann mitunter mehrere Tage dauern, wie folgendes Beispiel aus der Praxis zeigt:

In einem konkreten Fall bei einem unserer Kunden, wurde ebenfalls das komplette Produktivsystem verschlüsselt. Das Backup befand sich auf zwei Data Domain-Systemen, die von der Verschlüsselung aber nicht betroffen waren. Dank des Boost-Protokolls war der Backupspeicher für die Angreifer nicht zugänglich. Durch Auswertung der Datenmenge der Roh- und Nettodaten konnte ermittelt werden, ab wann die Daten auch im Backup verschlüsselt waren. Die gesicherten Daten vor diesem Zeitpunkt waren nicht betroffen und konnten zurückgesichert werden. Insgesamt war der Kunde nach sieben Tagen wieder voll operabel. In einem vergleichbaren Fall bei einem anderen Unternehmen, bei dem aber Tape als Backupmedium eingesetzt wurde, hat diese Wiederherstellung der Operabilität sechs Monate gedauert!

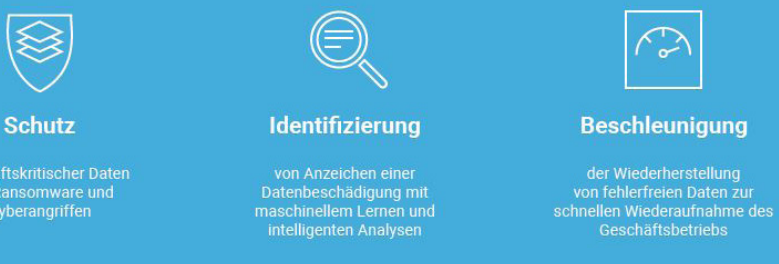
Die Software „Cyber Recovery“ von Dell Technologies

Die Erfahrungen mit Cyber Recovery von Dell Technologies sind sehr positiv. Kunden, die die Lösung bestehend aus Dell PowerProtect Data Domain bis hin zu einem Cyber Vault einsetzen, hatten eine große Chance, sehr schnell wieder online zu sein. Nutzen Kunden in einer ersten Ausbaustufe eine Data Domain als Zielspeicher für das Backup, so konnten diese zwei Vorteile nutzen, die es dem Angreifer erschwert, die Systeme zu verschlüsseln. Das eine ist das sogenannte BOOST-Protokoll, das bisher nicht angegriffen werden konnte, das zweite ist die Funktion „Retention Lock“, bei der die Daten in einem „WORM-Modus“ (write once read many) weggeschrieben werden und damit nicht verschlüsselt werden können. Noch besser sind jene Unternehmen geschützt, die eine zweite oder dritte Data Domain in einen Cyber Vault stellen, der hinter einer weiteren Firewall steht und nur über ein Air Gap* zu erreichen ist. In der maximalen Ausbaustufe steht auch ein Backup-Server hinter dieser Firewall und kann unmittelbar für eine Recovery/Wiederherstellung der nicht verschlüsselten Daten genutzt werden, wenn die Primärsysteme nicht mehr nutzbar sind.

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

Aufgrund der steigenden Bedrohung durch Ransomware-Angriffe hat Dell Technologies eine Schutz-Software entwickelt, die in ihrem Konzept und den Möglichkeiten derzeit einmalig ist. Cyber Recovery gehört zum Lieferumfang der neueren Data-Domain-Systeme und bildet eine Art letzter Verteidigungslinie gegen Malware- Angriffe aller Art. Retention Lock kann als Governance- oder Compliance-Modus angewendet werden. Für den in der Aufbewahrungssperre festgelegten Zeitraum können diese Daten nicht geändert, überschrieben oder gelöscht werden. Der Compliance-Modus wird für strenge regulatorische Standards des Unternehmens verwendet und sichert das Data-Domain-System über einen Security Officer gegen innere und äußere Angriffe ab. Wenn der Security Officer einmal angelegt ist, haben alle weiteren Benutzer nur noch operative Rechte und können weder Benutzer ausschließen, Daten löschen, verändern oder verschlüsseln.

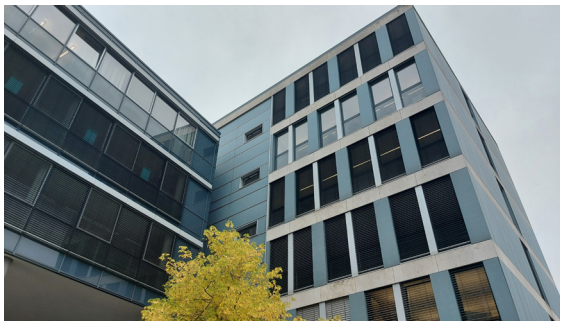
Ausgehend von der Beobachtung, dass moderne Ransomware zunehmend auf die Backup-Systeme in den Unternehmen abzielt und danach trachtet, sie zu deaktivieren oder zu kontrollieren, entstand bei Dell Technologies das Konzept für einen Vault, also einen Tresor, der für Angreifer absolut unzugänglich ist. 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.



Erste Schritte in einem Cyber Recovery-Projekt

Die Backup- und Recovery-Projekte sind abhängig von dem Volumen der zu sichernden Daten, der Schutzbedürftigkeit der Daten und der Ausbaustufe der o.g. Konfigurationen, von PowerProtect Data Domain bis zum Cyber Vault. Gerne besprechen wir die Details in einem persönlichen Gespräch. Die Lösung erfordert eine gründliche Analyse der Situation beim Kunden und eine eingehende Beratung. Die GID GmbH bietet daher entsprechende Consulting Services an. 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 auf diesem Weg genau die Cyber-Recovery-Lösung, nach der sie verlangen und die sie benötigen.

Der Partner GID GmbH



Die Global Information Distribution GmbH (GID) als Systemintegrator 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, Stuttgart und Frankfurt, 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