ESG SHOWCASE

# Ausfallsicherheit bei Cyberangriffen – für erfolgskritischen Storage unerlässlich

**Datum:** Oktober 2022 **AutorInnen:** Scott Sinclair, Practice Director, und Monya Keane, Senior Research Analyst

**ZUSAMMENFASSUNG:** Die IT-Landschaft hat sich verändert. Da Daten heutzutage eine so wertvolle Ressource darstellen, sind auch Cyberbedrohungen allgegenwärtig geworden. Daher muss die Ausfallsicherheit bei Cyberangriffen ein zentraler Aspekt bei der Wahl von erfolgskritischem Storage sein. Bei PowerMax hat Dell Technologies wesentliche Funktionen für Ausfallsicherheit bei Cyberangriffen entwickelt und direkt in die Systeme integriert. So konnte das Unternehmen sich noch stärker als Vorreiter in Sachen erfolgskritischer Storage etablieren.

## Übersicht

Daten sind eine wichtige und äußerst wertvolle Unternehmensressource. Eine ESG-Studie zeigt, dass 59 % der befragten Unternehmen Daten im Prinzip als ihr Geschäft identifizieren, und dieser Prozentsatz soll in zwei Jahren voraussichtlich auf 81 % steigen.[1] Die Rolle einer erfolgskritischen Storage-Infrastruktur besteht darin, Daten zu erhalten, zu schützen und bereitzustellen, die Workloads und Anwendungen zugrunde liegen, die einfach niemals ausfallen dürfen.

Über Jahrzehnte hinweg war die Bereitstellung von „erfolgskritischem Storage“ gleichbedeutend mit der Bereitstellung der erforderlichen Leistung und Skalierbarkeit, bei gleichzeitiger Gewährleistung ununterbrochener Verfügbarkeit zum Schutz vor Komponentenausfällen, Systemausfällen am Standort, Nutzerfehlern und Naturkatastrophen. Jetzt nimmt die Verbreitung bösartiger Angriffe zu. Die zentralen Aspekte von erfolgskritischem Storage müssen daher über diese herkömmlichen Funktionen hinausgehen, um auch die Cyberresilienz eines Unternehmens zu verbessern.

Dell Technologies, ein führender Anbieter von Enterprise Storage, entwickelt seine Vorzeige-Storage-Plattform PowerMax beständig weiter, um die erfolgskritischen Anforderungen der anspruchsvollsten IT-Umgebungen zu erfüllen. Die jüngsten Innovationen von Dell konzentrierten sich darauf, die PowerMax-Produktreihe um robuste Funktionen zur Verbesserung der Cyberresilienz jedes Unternehmens zu ergänzen, das seine Daten und wichtigen Anwendungen besser schützen, seinen Markenruf wahren und langfristigen Erfolg erzielen möchte.

## Das Zeitalter allgegenwärtiger Cyberbedrohungen für Daten

Neben der Zunahme von Cyberbedrohungen hat sich auch die IT-Komplexität erhöht. Fast die Hälfte (46 %) der TeilnehmerInnen an der ESG-Umfrage sagt, dass die IT heute komplexer ist als vor zwei Jahren. Die rasante Entwicklung der Cybersicherheitslandschaft (von 37 % erwähnt) und die Bemühungen zur Einhaltung neuer Datensicherheits- und Datenschutzbestimmungen (laut 32 % der Befragten) waren zwei der am häufigsten genannten Faktoren für die Erhöhung der IT-Komplexität.[2]

Leider haben Unternehmen derzeit Schwierigkeiten, genügend qualifizierte Cybersicherheitstalente einzustellen, um diese Komplexität bewältigen zu können. 48 % der befragten Unternehmen gaben an, dass sie derzeit nicht über genügend CybersicherheitsexpertInnen verfügen. Dies ist derzeit der am häufigsten genannte Bereich, wenn es um den Kompetenzmangel in der Unternehmens-IT geht.[3]

[1] Quelle: ESG Research Report, *Data Infrastructure Trends*, November 2021.
[2] Quelle: ESG Complete Survey Results, *2022 Technology Spending Intentions Survey*, November 2021.
[3] Ebd.

Dieser ESG Showcase wurde von Dell Technologies in Auftrag gegeben. Seine Verbreitung erfolgt mit Genehmigung von TechTarget, Inc.

© 2022 TechTarget, Inc. Alle Rechte vorbehalten.

### Ransomware und Malware sind weitverbreitet

Unter den zahlreichen Bedrohungen, denen Unternehmen ausgesetzt sind, sind externe Ransomware- und Malwareangriffe praktisch unausweichlich geworden. In einer kürzlich durchgeführten ESG-Umfrage unter IT- und CybersicherheitsexpertInnen, die Technologien und Prozesse in Zusammenhang mit dem Schutz ihrer Unternehmen vor Ransomware beaufsichtigen, gaben 79 % an, dass sie in den letzten 12 Monaten einen versuchten Ransomwareangriff erlebt haben. Und 30 % dieser Befragten gaben an, dass diese Angriffe wöchentlich oder sogar häufiger auftreten.[4]

Unter den Unternehmen, die einen Angriffsversuch erlebt haben, war bei 73 % mindestens einer der Angriffsversuche erfolgreich. Unter diesen Umständen ist die Zahlung eines Lösegelds jedoch keine optimale oder auch nur einigermaßen intelligente Strategie. 56 % der Unternehmen, die Opfer eines erfolgreichen Angriffs wurden, haben bezahlt. Doch bei denjenigen, die das geforderte Lösegeld bezahlt haben, ist Folgendes geschehen:

- **87 %** von ihnen erlebten dann zusätzliche Erpressungsversuche für mehr Geld. Tatsächlich zahlten 61 % derjenigen, die anfangs bezahlt haben, letztendlich später noch mehr.[5]
- Nur **14 %** haben 100 % ihrer Daten zurückerhalten, selbst nachdem das Lösegeld überwiesen wurde.
- Und **61 %** haben nach der Zahlung nur 75 % ihrer Daten oder weniger zurückerhalten.

Umfassender Ransomwareschutz erfordert ganz klar eine facettenreichere Strategie – eine Strategie, die mehrere Technologien und Tools mit Fokus auf Erkennung, Prävention und Recovery beinhaltet.

Viele Unternehmen modellieren jetzt ihre Strategien für Ausfallsicherheit bei Cyberangriffen basierend auf den Angaben des NIST Cybersecurity Framework, das Unternehmen empfiehlt, kritische Ressourcen zu identifizieren, diese Ressourcen zu schützen, Fehler und Sicherheitsverletzungen aufzuspüren und die Reaktion und Recovery nach Cyber-Incidents zu planen. Eine weitere Komponente des NIST-Frameworks, die Unternehmen häufig nutzen, ist die Zero- Trust-Architektur, mit der das Konzept eines schützenden Netzwerk-Edge durch den Grundsatz „Niemals vertrauen, immer überprüfen“ ersetzt wird. In diesem Modell muss die Sicherheitskonfiguration von NutzerInnen (selbst Personen, die innerhalb des Unternehmens arbeiten) wiederholt und regelmäßig validiert werden, bevor diese NutzerInnen auf Anwendungen/Daten zugreifen können.

Storage-Systeme müssen definitiv Teil dieses Cybersicherheitsansatzes sein. Schließlich ist ESG-Untersuchungen zufolge die Storage-Hardware die Infrastrukturkomponente, auf die Ransomwareangriffe am häufigsten abzielen. Es war die häufigste Antwort: Ganze 40 % der Befragten haben sie genannt.

## Wie erfolgskritischer Storage die Ransomwareresilienz verbessert

Bei Ransomwareangriffen liegt der Fokus darauf, auf wichtige Unternehmensdaten zuzugreifen und diese dann zu verschlüsseln. Viele Strategien für Ausfallsicherheit bei Cyberangriffen basieren auf Tools und Technologien, bei denen der Fokus auf der **Prävention** durch Fernhalten von Bedrohungen und auf der frühzeitigen **Erkennung** von Angriffen liegt, die sich durchsetzen konnten. Bei Ransomware ist es jedoch wichtig, sich auch auf eine **beschleunigte Recovery** zu konzentrieren.

Erfolgskritische Storage-Systeme befinden sich an einer Stelle im Datenpfad, die sich ideal für die schnelle Daten-Recovery nach einem Angriff eignet. In Anbetracht der zunehmenden erfolgreichen Ransomwareangriffe konnten einige Storage-Systeme beispielsweise die in sie integrierten Funktionen nutzen, um eine schnelle Recovery durch sichere Aufbewahrung und anschließende Bereitstellung sicherer und unveränderbarer Datenvolume-Kopien zu unterstützen.

[4] Quelle: ESG Research Report, *The Long Road Ahead to Ransomware Preparedness*, Juni 2022. Sofern nicht anders angegeben, stammen alle ESG-Forschungsreferenzen im vorliegenden Showcase aus diesem Forschungsbericht.
[5] Quelle: ESG Complete Survey Results, *The Long Road Ahead to Ransomware Preparedness*, Juni 2022.

© 2022 TechTarget, Inc. Alle Rechte vorbehalten.

Diese Art von Unterstützung ist unglaublich hilfreich, um die Recovery zu beschleunigen. Snapshots können schnell als „zweifellos fehlerfreie" Volumes identifiziert und von der IT schnell wiederhergestellt werden, um Datenvolumen so makellos wiederherzustellen, wie sie zuvor waren. Für erfolgskritische Anwendungsumgebungen *muss die Storage-Technologie jedoch noch mehr leisten*.

## Dell PowerMax kann die Ausfallsicherheit bei Cyberangriffen für Unternehmen verbessern

Produktnamen haben sich geändert und die Funktionen wurden im Laufe der Jahrzehnte erweitert, aber die erfolgskritischen Infrastruktur-Storage-Systeme von Dell Technologies sind in diesem Bereich bereits führend, seitdem Enterprise Storage Ende der 1980er-Jahre von EMC als separate IT-Kategorie eingeführt wurde. Heute bietet Dell PowerMax zahlreiche Funktionen, die darauf ausgelegt sind, die anspruchsvollen Anforderungen erfolgskritischer Workloads zu erfüllen, darunter:

- Eine All-NVMe-Scale-out-Architektur mit mehreren Controllern für außerordentliche, konsistente Leistung im großen Maßstab.
- Massive Workload-Konsolidierung mit Unterstützung für vielfältige Block- und Dateianwendungsumgebungen, die Mainframe-Workloads, Bare-Metal-Systeme, VMs, Container und mehr umfassen.
- Höchste Sicherheit, Verfügbarkeit und Ausfallsicherheit. PowerMax bietet eine Verfügbarkeit von 99,9999 % mit End-to-End-Datenverschlüsselung von Hosts zu PowerMax, Data-at-Rest-Verschlüsselung und sicheren Snapshots – laut Dell werden bis zu *64 Mio. Snapshots pro Array* unterstützt. Darüber hinaus nutzt die SRDF-Disaster-Recovery-Software (Symmetrix Remote Data Facility) von Dell erweiterte Topologien und Automatisierungsfunktionen, um eine solide Grundlage für Ausfallsicherheit zu schaffen. Mit SRDF können Unternehmen sogar einen Air-Gap-Vault erstellen. In diesem Vault werden die Daten isoliert und die Verbindung zum Vault ist intermittierend und stark eingeschränkt.

### Dell hat PowerMax für Resilienz entwickelt

In letzter Zeit hat sich Dell darauf konzentriert, noch mehr Sicherheitsfunktionen zu entwickeln und in PowerMax zu integrieren. PowerMax ist beispielsweise jetzt für Zero-Trust-Sicherheitsumgebungen konzipiert, die auf den sieben Grundpfeilern von Dell für Zero Trust basieren. Dazu gehört auch die intrinsische Sicherheit/der Schutz des Systems selbst vor Angriffen durch:

- Funktionen für eine unveränderliche Hardware-Root-of-Trust: Diese Funktionen authentifizieren Hardware- und Softwareänderungen über Nodes, Datenträgergehäuse und die Control Station hinweg. Eingebettete, unveränderbare kryptografische Schlüssel auf Komponentenebene werden von der Dell Fertigung im Arbeitsspeicher verankert.
- Funktionen für Secure-Boot-Vertrauensketten: Diese Funktionen erstellen eine Firmware-„Vertrauenskette" gegen bösartige Start-, Kernel- und Treiber-Rootkits und erweitern sie. Bei der Secure-Boot-Vertrauenskette kommt eine kryptografische Authentifizierung für nachfolgende Firmwareladevorgänge/Bootloader auf Basis von Dell Signaturen zum Einsatz.
- Digital signierte Firmwareupdates: PowerMax nutzt außerdem die Authentifizierung mittels digitaler Signatur von Dell, um sich vor unerlaubten Firmwareupdates zu schützen. PowerMax führt Scans von Node-, Datenträger- und Control-Station-Komponenten mithilfe von kryptografischen Authentifizierungsschlüsseln aus.

Zusätzlich zu diesem vertrauenswürdigen Design bietet PowerMax noch weitere Funktionen zur Verbesserung der Prävention, Erkennung und Recovery nach Ransomwareangriffen und anderen Cybersicherheitsbedrohungen.

© 2022 TechTarget, Inc. Alle Rechte vorbehalten.

Für die **Prävention** bietet PowerMax nicht nur integrierte Hardwaresicherheit, sondern auch erweiterte Sicherheit zur Vermeidung unbefugter Nutzerzugriffe, sodass Angriffe abgewehrt werden können. Außerdem punktet die Lösung mit Common Criteria-, STIG Hardening/APL- und FIPS 140-Sicherheitszertifizierungen sowie Unterstützung für Mechanismen zur Kontrolle von Administratorzugriffen wie:

- SecurID-Multi-Faktor-Authentifizierung zur Überprüfung der Identität von AdministratorInnen
- CAC-/PIV-Smartcard-Unterstützung mit einem Zertifikat/privaten Schlüssel für den Zugriff auf Onlineressourcen innerhalb von US- Bundesbehörden
- Rollenbasierte Zugriffskontrollen (Role-Based Access Controls, RBAC), LDAP-Unterstützung und zDP 2 Actor (erfordert zwei Personen, um bestimmte zDP-Befehle auszuführen), sodass nur autorisierte NutzerInnen bestimmte Vorgänge wie die Bereitstellung von Storage durchführen können

Für die **Erkennung** bieten sowohl die PowerMax-Hardware als auch Dell CloudIQ-KI-Software Funktionen zur Erkennung von Malwareanomalien. Hierbei handelt es sich um Compliancewarnmeldungen auf Basis von Cybersicherheitswarnprotokollen, gepaart mit sicheren Syslog-Warnmeldungen und -Exporten. Zu schnellen Erkennung von Cyberangriffen setzt CloudIQ insbesondere auf die Überwachung ungewöhnlicher PowerMax-Speicherauslastung und verdächtiger Aktivitätsmetriken. Anschließend werden AdministratorInnen auf drastische Veränderungen aufgrund einer möglichen Verschlüsselung aufmerksam gemacht. Außerdem kann die Storage-Infrastruktur kontinuierlich überwacht werden, um Cybersicherheitsrisiken aufgrund falsch konfigurierter Systemeinstellungen automatisch zu identifizieren und dann detaillierte Empfehlungen zur Behebung dieser Probleme bereitzustellen.

Und für die **Recovery** bietet die sichere Snapshot-Technologie von PowerMax Datensicherheit und Data Protection auf neuem Niveau. Je nach Service-Level-Zielen des Unternehmens kann die IT bis zu 64 Mio. Snapshot-Kopien auf jedem PowerMax konfigurieren (siehe Abbildung 1).

**Abbildung 1: Wie PowerMax die schnelle Cyber Recovery unterstützt**


*Quelle: Dell Technologies*

Diese Funktion ermöglicht es PowerMax, Recovery Point Objectives (RPOs) von nur wenigen Minuten vor einem erfolgreichen Angriff zu unterstützen. Und durch die Unterstützung für so viele Snapshots verfügt die IT über ausreichend Kopien, um selbst große, konsolidierte erfolgskritische Storage-Umgebungen praktisch minutenaktuell zu schützen. So kann eine beinahe sofortige Recovery erfolgskritischer Anwendungen erreicht werden. Dieses Maß an Schutzflexibilität ist bahnbrechend für groß angelegte Produktionsumgebungen. Laut Dell ermöglicht PowerMax die detaillierteste Cyber Recovery im großen Maßstab zur Optimierung der RPO.

© 2022 TechTarget, Inc. Alle Rechte vorbehalten.

Dell kann auch eine PowerMax-Cyber-Recovery-Vault-Option für Unternehmen hinzufügen, die eine Remote-Vault-Air-Gap-Recovery-Option (SRDF) benötigen – mit orchestriertem/r Vaulting/Recovery sowohl für Open Systems als auch für Mainframe-Storage Das PowerMax-Cyber-Recovery-Vault-Angebot wird im Laufe dieses Monats allgemein verfügbar sein und nutzt die SRDF-Remotereplikation zur Air-Gap-Erstellung. Diese Lösung wurde für Kunden entwickelt, die eine Datenkopie außerhalb ihres Produktionsnetzwerks mit schneller Recovery (RTO) benötigen. Während PowerMax-Kunden diese Konfiguration schon eine Weile manuell bereitstellen, umfasst die Ankündigung in diesem Monat die Automatisierung der Bereitstellungsorchestrierung und Dell Professional Services zur Rationalisierung der Installation.

## Das Gesamtbild

Dell ist in der Regel nicht der erste Name, der einem einfällt, wenn man über Sicherheitsanbieter nachdenkt. Diese Wahrnehmung muss sich ändern. Böswillige AngreiferInnen werden organisierter und ihre Bedrohungen sind ausgefeilter. Dell hat viel in die Bekämpfung dieser Bedrohungen, den Schutz von Daten und die Vereinfachung des gesamten Managements der Sicherheit und Resilienz investiert und tut dies auch weiterhin.

Daten sind die wichtigste Ressource eines Unternehmens. Sie müssen geschützt und immer verfügbar sein. Die neueste Bedrohung für diese Verfügbarkeit sind Ransomware, Malware und andere Cyberangriffe. Ja, PowerMax blickt auf eine lange Erfolgsgeschichte in Sachen Unterstützung erfolgskritischer High-End-Workloads zurück. Dell verfolgt diesen Ansatz schon seit Jahren, aber die neuen Funktionen von PowerMax sind für so gut wie alle Storage-KäuferInnen von heute besonders passend. Jeder macht sich Sorgen wegen Ransomware, Malware und der Gefahr, in den nächsten Schlagzeilen zu landen.

Und es geht nicht darum, Diebe zu bekämpfen, die versuchen, sich zu bereichern. Diese HackerInnen können genauso gut für eine fremde Regierung arbeiten und geistiges Eigentum stehlen, um ihre eigene nationale Sicherheit oder militärische Stärke zu erhöhen. Wenn sie Ihre Daten nicht nur für Sie unzugänglich machen, sondern darüber hinaus noch verschlüsseln können, kann keiner sagen, was sie sonst noch damit tun können.

Wenn Sie Unternehmensinformationen haben, die auf keinen Fall in die Hände von AngreiferInnen gelangen dürfen, sollten Sie mit Dell darüber sprechen, wie eine Storage-Infrastruktur richtig geschützt werden kann.

Alle Produktnamen, Logos und Marken sind das Eigentum ihrer jeweiligen Inhaber. Die in dieser Veröffentlichung enthaltenen Informationen stammen aus Quellen, die TechTarget, Inc. als zuverlässig betrachtet. TechTarget, Inc. übernimmt aber keinerlei Gewähr dafür. Diese Publikation kann Meinungen von TechTarget, Inc. enthalten, die sich ändern können. Diese Veröffentlichung kann Prognosen, Vorhersagen und andere vorausschauende Aussagen enthalten, die die Annahmen und Erwartungen von TechTarget, Inc. auf der Basis von derzeit verfügbaren Informationen darstellen. Diese Prognosen basieren auf Branchentrends und beinhalten Variablen und Unsicherheiten. Folglich übernimmt TechTarget, Inc. keine Gewährleistung für die Genauigkeit bestimmter hierin enthaltener Prognosen, Vorhersagen oder vorausschauender Aussagen.

Das Urheberrecht für diese Publikation liegt bei TechTarget, Inc. Die komplette oder teilweise Vervielfältigung und/oder Verbreitung dieser Publikation in gedruckter, elektronischer oder sonstiger Form für bzw. an nicht berechtigte Personen ohne ausdrückliche Zustimmung von TechTarget, Inc stellt einen Verstoß gegen die Urheberrechtsgesetze der USA dar und wird mit zivilrechtlichen Klagen geahndet, gegebenenfalls auch strafrechtlich verfolgt. Sollten Sie Fragen haben, wenden Sie sich bitte an Client Relations unter cr@esg-global.com.

Die **Enterprise Strategy Group** ist ein integriertes Technologieanalyse-, -forschungs- und -strategieunternehmen, das Marktinformationen, verwertbare Erkenntnisse und Go-to-Market-Contentservices für die globale IT-Community bereitstellt.

www.esg-global.com contact@esg-global.com +1 508 482 0188

© 2022 TechTarget, Inc. Alle Rechte vorbehalten.