EnTec
IT Systems GmbH

Modern Data Protection

Wie Sie Ihre wertvollen Daten optimal
schützen und aufbewahren

Inhalt

01
DATENWACHSTUM HOCH ZEHN 4

02
DATEN IM VISIER DER CYBERKRIMINELLEN 6

03
WICHTIGE MERKMALE EINER MODERNEN DATA PROTECTION-LÖSUNG 8

04
TRENDS IN MODERN DATA PROTECTION 9

05
IBM MODERN DATA PROTECTION 10

5.1. IBM Spectrum Protect
5.2. IBM Spectrum Protect Plus
5.3. IBM Spectrum Copy Data Management

06
CYBER VAULT UND SAFE GUARDED COPY MACHEN IBM SPEICHERSYSTEME ZUM DATENTRESOR 13

07
FLEXIBEL MIT IBM SPECTRUM STORAGE BLEIBEN 17

08
DIE ÄLTESTE SPEICHER-TECHNOLOGIE IST WIEDER GEFRAGT 18

09
HANDLUNGS-EMPFEHLUNGEN 21

Ob ERP, Big Data und vernetzte Maschinen oder autonomes Fahren und intelligente persönliche Assistenten – Daten sind das Herzstück heutiger und zukünftiger geschäftskritischer Anwendungen. Sie geben Entscheidern in der Wirtschaft die Möglichkeit, bestehende Prozesse zu optimieren und neue innovative Geschäftsmodelle zu entwickeln. Daten haben Öl als die weltweit wertvollste Ressource abgelöst.

Um das damit verbundene rasante Datenwachstum zu bewältigen, benötigen Unternehmen eine Strategie für die Datensicherung und das Disaster Recovery. IT- und Business-Entscheider stellen sich die Frage: Wie lassen sich die erfassten und genutzten Daten effizient speichern, langfristig sichern und bei Bedarf schnell wiederherstellen?

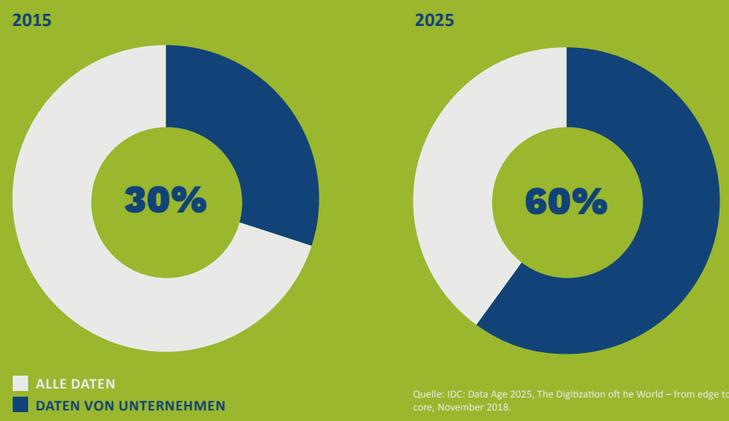
01 Datenwachstum hoch zehn

Laut den Marktanalysten von IDC werden im Jahr 2025 weltweit rund 175 Zettabyte (das ist eine 175 mit 21 Nullen) an Daten erzeugt.

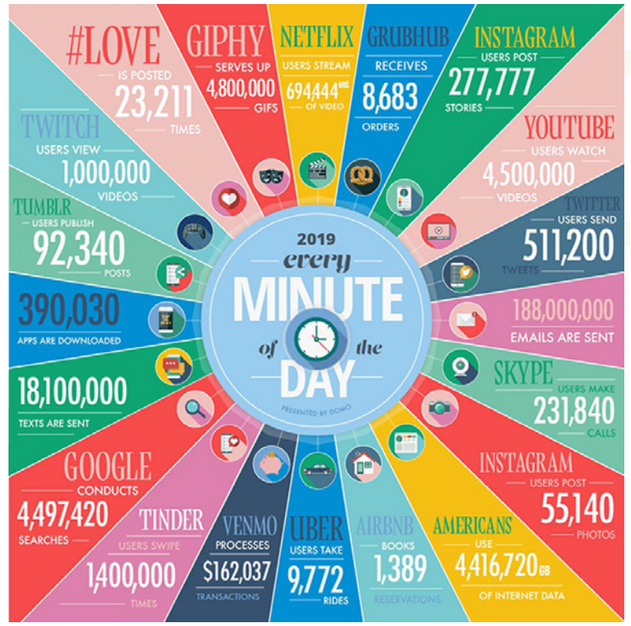
Das ist mehr als das zehnfache an Daten im Vergleich zum Jahr 2016 (16 Zettabyte). Diese Datenmenge auf DVDs abgespeichert und übereinandergestapelt, entspricht der Entfernung von der Erde zum Mond – und das knapp 100 Millionen Mal.

Das Datenwachstum verlagert sich in den nächsten Jahren vom Endverbraucher hin zum Unternehmenssektor. Firmen werden im Jahr 2025 knapp 60 Prozent der globalen Datenmenge erzeugen.

Entwicklung des Datenwachstums von Unternehmen



Quelle: IDC: Data Age 2025, The Digitization oft he World – from edge to core, November 2018.



Quelle: Data Never Sleeps 7.0/www.domo.com

Die IDC-Analysten erwarten, dass bis 2025 knapp 20 Prozent der weltweit verfügbaren Daten für den Privatalltag und Unternehmensprozesse lebenskritisch sein werden, die Hälfte davon sogar hyperkritisch.

Bis zu diesem Zeitpunkt wird jeder Mensch auf der Welt mit Internetzugang im Schnitt 4.800 Mal pro Tag mit vernetzten Geräten agieren, das bedeutet eine Interaktion alle 18 Sekunden. Und über ein Viertel der erzeugten Daten sind Echtzeit-Daten, die zu 95 Prozent aus dem Internet of Things (IoT) stammen.

Mit der Entwicklung hin zum produktivitäts- und innovationsgetriebenen Datenwachstum rückt die Datensicherheit immer mehr in den Mittelpunkt.

02 Daten im Visier von Cyberkriminellen

Es ist die größte Lösegeldsumme, die von Cyberkriminellen bisher gefordert wurde: 70 Millionen US-Dollar fordert die Hackergruppe Revil von weltweit namhaften Unternehmen, ansonsten bleiben deren IT-Systeme verschlüsselt.

Dass dieser Angriff kein Einzelfall ist, zeigt eine aktuelle Studie des Digitalverbands Bitkom. Demnach sind 3 von 4 Unternehmen in den vergangenen Jahren Opfer eines Cyberangriffs geworden.

Weitere 13 Prozent waren vermutlich betroffen. Zu den häufigsten Delikten gehörten der Diebstahl von sensiblen digitalen Daten und Informationen sowie die digitale Sabotage von Informations- und Produktionsabläufen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ermittelte für 2020 117,4 Millionen neue Schadprogramm-Varianten in Deutschland, das sind durchschnittlich 322.000 pro Tag! Automatisierte Schadprogramme – sogenannte Bots – infizieren täglich bis zu 20.000 deutsche Systeme.

Im Trend liegen dabei sogenannte „Ransomware-Attacken“ wie das aktuelle Beispiel der Datenkidnapper von Revil zeigt. Bei solchen Angriffen werden Unternehmensdaten durch die eigenschleuste Software oder App verschlüsselt und erst wieder durch die Zahlung eines Lösegelds entschlüsselt.

Immer öfters konzentrieren sich die Cyberattacken gezielt auf die Backup-Daten. Danach geraten die Primär- und Sekundärdaten ins Visier der Angreifer. Durch diese perfide Strategie werden die Backup-Daten nutzlos, weil sie bereits infiziert, verschlüsselt oder zerstört sind. Der Erpresser hat seine Opfer völlig in der Hand!

Mittlerweile haben sich Ransomware-Angriffe als Geschäftsmodell etabliert: als Ransomware- as-a-Service (RaaS). Es wird davon ausgegangen, dass die Revil-Cyberkriminellen ihre Schadsoftware über das Darknet an Affiliate-Kunden vermietet haben.

Der Gesamtschaden durch Spionage, Sabotage oder Datendiebstahl hat sich laut Bitkom in den letzten Jahren verdoppelt und beträgt aktuell zirka 100 Milliarden Euro pro Jahr.

Weniger häufig vorkommend, aber dafür umso wirkungsmächtiger sind Naturkatastrophen. Sie legten in der Vergangenheit ganze IT-Infrastrukturen und Rechenzentren lahm. Stromausfälle brachten komplette Produktionsprozesse zum Stillstand. Vorsorge-Maßnahmen sind deshalb ein wichtiger Bestandteil eines verantwortungsvollen Disaster-Managements.

Vor dem Hintergrund der beschriebenen Entwicklungen gewinnen Datenschutz und Datensicherheit an großer Bedeutung. Beide Bereiche müssen modernisiert und auf den neuesten organisatorischen und technischen Stand gebracht werden. Erst dann lassen sich alle eingesetzten IT-Umgebungen optimal schützen und es wird möglich, das rapide Datenwachstum und die zunehmende Datenkomplexität zu bewältigen.

Unternehmen stehen vor folgenden Fragestellungen:

- Wie können Daten in unterschiedlichen IT-Umgebungen geschützt werden?
- Wie lassen sich wertvolle und persönliche Daten und Kopien optimal absichern?
- Auf welche Weise können Datenschutz SLA’s (Service Level Agreements) sichergestellt werden?
- Wie ist ein sicherer, kontrollierter Datenzugriff für alle Unternehmensbereiche (zum Beispiel DevOps) umsetzbar?
- Wie lassen sich die Kosten für die Backup-/Speicher-Komponenten (Software und Hardware) begrenzen?

03 Wichtige Merkmale einer modernen Data Protection-Lösung

Vereinfachtes Management für die Wiederverwendung von Daten

Daten müssen aus dem Backup schnell wiederverwendbar sein, weil sie zum Beispiel für Analytics oder für DevOps benötigt werden. Beim Zugriff von Entwicklern oder Datenbank-Administratoren muss eine kontrollierte Verwaltung der Datenkopien vorhanden sein. Zu den benötigten Funktionalitäten gehören eine rollenbasierte Zugriffssteuerung (RBAC – Role Based Access Control), REST-APIs, SLA-basierte Richtlinien und ein Drilldown-Dashboard.

Kontrolle der Speicherkosten

Das enorme Datenwachstum und die Notwendigkeit der Datenaufbewahrung erhöhen die Speicherkosten. Integrierte Datenreduktionstechnologien wie Kompression und Daten-Deduplizierung sowie ein kosteneffizienter Speicher für die Auslagerung von Daten sind heute wichtiger denn je. Offline-Datenträger wie Tapes spielen hier eine maßgebliche Rolle.

Minimierung der Risiken und Sicherstellung der Daten-Compliance

Daten sind vor Cyberattacken und Ransomware-Angriffen umfassend zu schützen. Zudem müssen die Richtlinien für die Datenaufbewahrung den regulatorischen Vorgaben und den branchenspezifischen Vorschriften entsprechen. Auch hierbei sind Offline-Datenträger wie Tapes ein Teil der gesuchten Lösung, zumal das Medium Tape sowohl überschreibbare Kassetten als auch zertifizierte WORM-Datenträger (Write Once Read Many) umfasst. Sind diese in einem Tresorraum aufbewahrt, können Cyberbedrohungen praktisch ausgeschlossen werden.

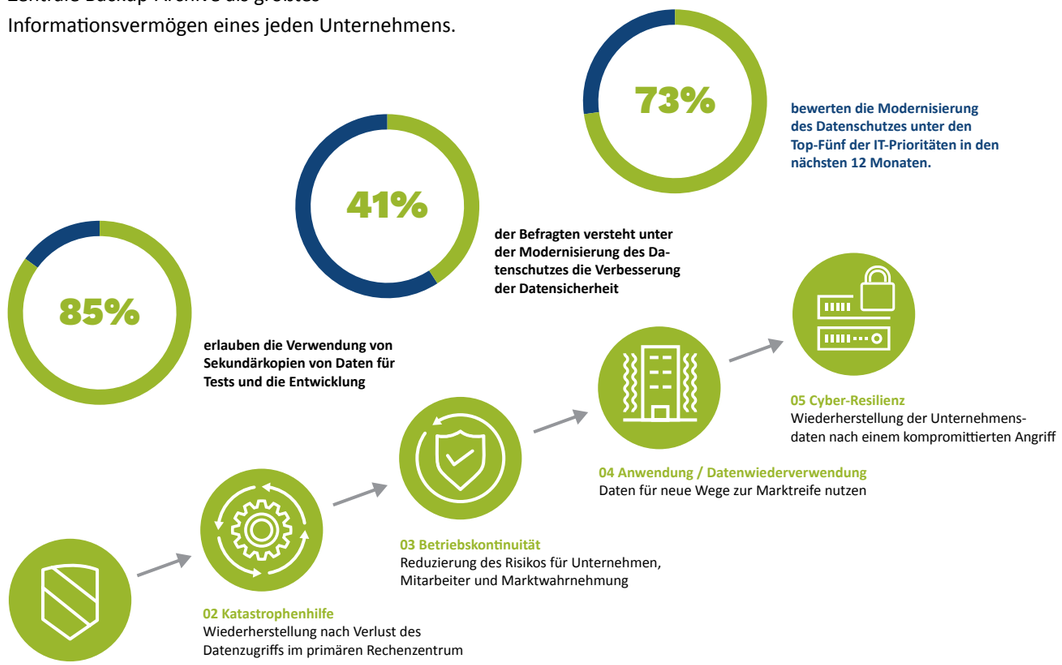
04 Trends in Modern Data Protection

Ein aktuelles Forschungspapier der „Enterprise Strategy Group (ESG)“ informiert über Trends bei der Datenschutz-Modernisierung. Es kann kostenlos auf der IBM Webseite heruntergeladen werden und lässt sich einfach über Google finden (den Titel „Trends in Modern Data Protection“ in das Google-Suchfeld eingeben). 73 Prozent der befragten IT-Entscheider betrachten die Modernisierung der unternehmenseigenen Datensicherheit als eine der Top-5 Prioritäten für die Zukunft. Den größten Nutzen sehen die IT-Entscheider bei der Security und der Widerstandsfähigkeit gegen Cyberattacken (65 Prozent), bei den Speicherkosten und der Infrastruktur-Skalierbarkeit (49 Prozent) sowie bei der Datenmigration und im operativen Backup- und Recovery-Bereich.

Welcher Hersteller ist am besten positioniert, um Organisationen bei der Modernisierung von Datensicherheitslösungen zu helfen? Diese Frage wurde von den IT-Entscheidern eindeutig beantwortet. Fast die Hälfte nannten IBM, gefolgt von Amazon, Oracle und EMC.

Die wichtigsten Datensicherheitstrends von heute

Zentrale Backup-Archive als größtes Informationsvermögen eines jeden Unternehmens.



Quelle: Research conducted by ESG on behalf of IBM 2019

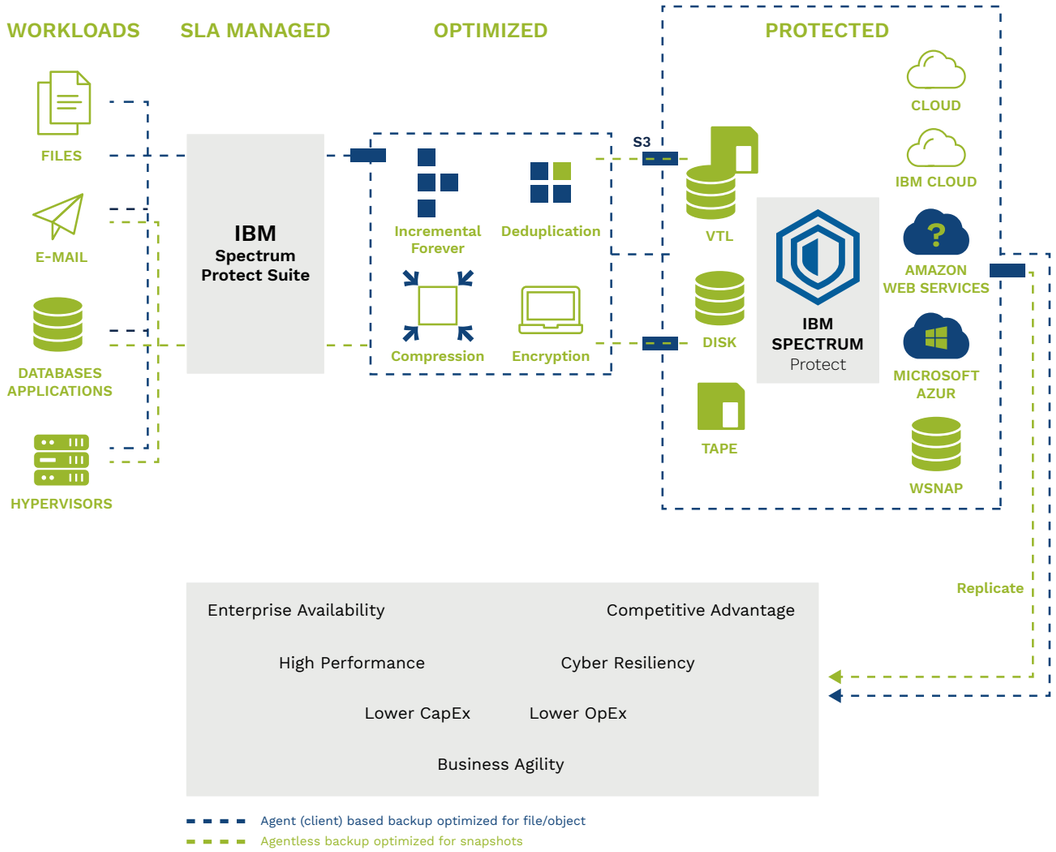
05 IBM Modern Data Protection

IBM Modern Data Protection ist für die höchsten Anforderungen heutiger moderner Datensicherheitslösungen konzipiert. Die Plattform stellt sicher, dass sich Daten sofort wiederherstellen und wiederverwenden lassen.

Der direkte Datenzugriff als „Self-Service“ steigert die Produktivität. Ein SLA- basierendes Management vereinfacht und automatisiert die Operationen. Dabei wird den unterschiedlichen Datenschutz-Zielen für Kosten, Leistung und Security flexibel Rechnung getragen. Leistungsstarke Funktionalitäten ermöglichen ein schnelles Recovery der Daten als Folge eines Cyber-Angriffs.

Das IBM Modern Data Protection-Portfolio umfasst IBM Spectrum Protect, IBM Spectrum Protect Plus und IBM Spectrum Copy Data Management.

IBM Spectrum Protect Portfolio – Intelligent Data Protection / Reuse



Das IBM Modern Data Protection-Portfolio umfasst IBM Spectrum Protect, IBM Spectrum Protect Plus und IBM Spectrum Copy Data Management.

5.1. IBM Spectrum Protect

IBM Spectrum Protect vereinfacht den Datenschutz, unabhängig davon, ob die Daten in physischen, virtuellen, softwaredefinierten oder Cloud-/Multi-Cloud-Umgebungen gehostet werden. Dabei können die Kosten für die Backup-Infrastruktur um über 50 % gesenkt werden. Dies geschieht mit Funktionen wie Kompression, Deduplizierung, inkrementelle „Forever“-Sicherung und eine richtlinienbasierte Verwaltung. IBM Spectrum Protect bietet dabei eine extrem hohe Leistungsfähigkeit, skaliert bis in den multiplen Petabyte-Bereich und stellt zusätzlich eine hohe Flexibilität bei der Auswahl der passenden Speicherlösungen zur Verfügung.

5.2. IBM Spectrum Protect Plus

IBM Spectrum Protect Plus ist eine Lösung für die schnelle Wiederherstellung und Wiederverwendung von Daten in virtuellen- und Datenbank-Umgebungen. Der direkte Zugriff auf das Backup ermöglicht ein sofortiges Recovery der Daten. Die Software unterstützt verschiedene Benutzer-Gruppen mit rollenbasiertem Zugriff und mit benutzerfreundlichen Portalen für die Datensicherung und -wiederherstellung.

5.3. IBM Spectrum Copy Data Management

IBM Spectrum Copy Data Management stellt Datennutzern Datenkopien bereit, wann und wo immer sie benötigt werden. Dies geschieht, ohne dass unnötige Kopien erstellt oder wertvoller Speicherplatz durch nicht genutzte Kopien verschwendet werden. Die Lösung katalogisiert Datenkopien aus einer Vor-Ort-, Hybrid-Cloud- und externen Cloud-Infrastruktur, erkennt Duplikate und vergleicht Kopieranforderungen mit vorhandenen Kopien.

Um die benötigten Kopien zu erstellen, können Datennutzer das Self-Service-Portal verwenden.Zudem lassen sich Kopierprozesse und -abläufe automatisieren. Das Ergebnis: eine höhere Flexibilität und Konsistenz sowie eine verringerte Komplexität. Die Lösung kann als virtuelle Maschine innerhalb von Sekunden oder im Minutenbereich eingesetzt werden und das Senden zum Beispiel von Daten an AWS S3 koordinieren.

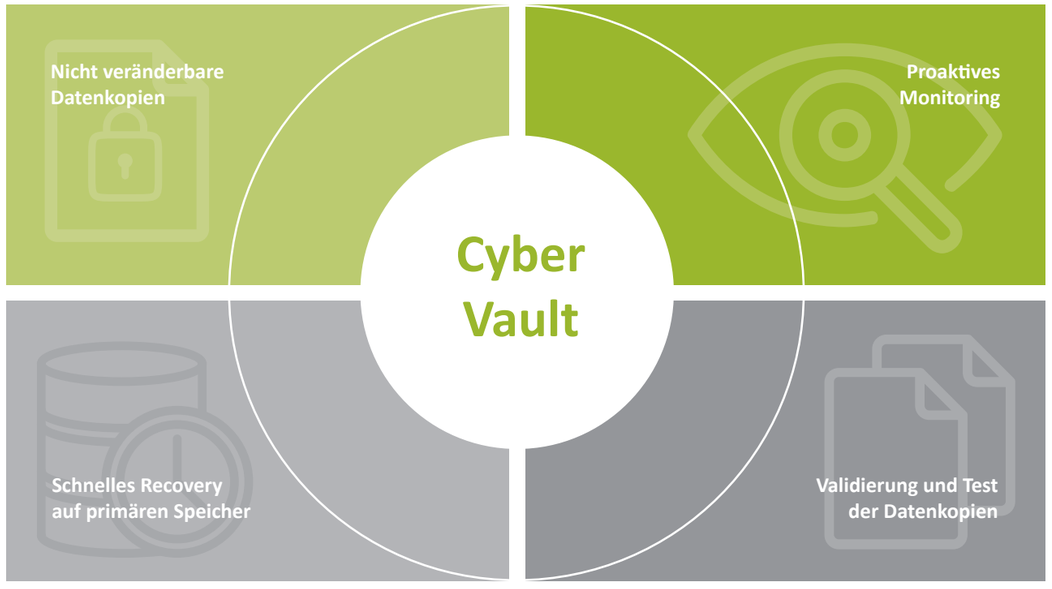
IBM Modern Data Protection

06 Cyber Vault und Safe Guarded Copy machen IBM Speichersysteme zum Datentresor

Mit der Funktionalität IBM Safeguarded Copy und dem IBM Cyber Vault Framework für DS8000-Systeme im Mainframe-Umfeld, IBM Flash-Systeme und den SAN Volume Controller SV3 wird nicht nur ein extrem hoher Schutz vor Cyberangriffen, Ransomware-Attacken, Trojanern oder Eavesdropping bereitgestellt, sondern auch vor allen anderen böswilligen Aktivitäten – extern und intern.

IBM Cyber Vault ist ein Framework für IT Cyber Resiliency und stellt folgende Funktionen zur Verfügung:

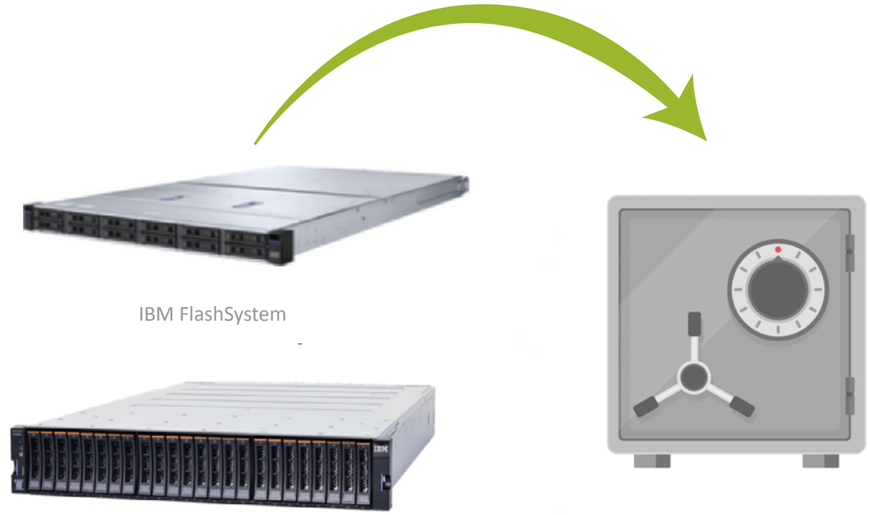
1. **Erzeugen von nicht veränderbaren Datenkopien**
2. **Proaktives Monitoring mit Warnhinweisen**
3. **Validieren und Testen der erzeugten Datenkopien**
4. **Schnelles Recovery**



Erzeugen von nicht veränderbaren Datenkopien

Die Softwarefunktion Safeguarded Copy, die DS8000-Speicher- systemen und mit IBM Spectrum Virtualize kostenlos für alle NVMe-basierten Flash-Systeme und den SAN Volume Controller SV3 zur Verfügung steht, erstellt automatisch Point-in-Time-Kopien (PiT) in einem Daten-safe in dedizierten Storage-Pools innerhalb der Speichersysteme.

Dort werden die Daten wie ein WORM-(Write Once Read Many)-Backup behandelt. Sie können also nicht überschrieben, verändert oder gelesen werden, sondern stehen ausschließlich für Recovery-Zwecke zur Verfügung. Anwendungen erhalten keinen Zugriff.



Um den schlimmen Folgen von Cyberangriffen vorzubeugen, ist es sinnvoll, Safeguarded Copy periodisch aufzusetzen, damit beispiels-weise alle paar Stunden Flash-Kopien erzeugt werden. Tritt der Ernstfall ein, kann man auf die Kopie zurückgreifen, die einen konsis-tenten Datenbestand wiederspiegelt. Dadurch wird es möglich, einen kurzfristigen Restore durchzuführen und schnell wieder online zu gehen. Die Intervalle, in denen Kopien erzeugt werden sollen, lassen sich individuell festlegen. Zudem kann flexibel bestimmt werden, wie lange die Kopien aufbewahrt werden sollen.

Das Zurückspringen beim Recovery von einem Sicherungsstand auf den davorliegenden und die Prüfung, um einen für die Anwendung konsistenten Datenbestand zu finden, kostet Zeit. Diese Spanne wird durch das Validieren der Kopien in Echtzeit mit IBM Cyber Vault mini-miert. Die Wiederherstellung an sich kann dann per Knopfdruck ohne Zeitverlust durchgeführt werden.

Proaktives Monitoring mit Warnhinweisen

Wachsam sein, wenn Angriffe drohen, ist die halbe Miete! Deshalb ist ein proaktives Überwachen der Produktionsumgebungen nötig, um Cyberangriffe schnell zu erkennen. Dies kann beispielsweise mit IBM QRadar, IBM Guardium, IBM Storage Insights und IBM Spectrum Control erfolgen.

IBM Safeguarded Copy ist vollständig in IBM Security QRadar integ-rierbar. QRadar überwacht dabei alle umgebungsrelevanten Aktivi-täten und sucht nach Anzeichen eines Angriffs unterschiedlichster Natur. Dabei werden Login-Versuche außerhalb der regulären Arbeits-zeiten ebenso festgestellt wie Login-Fehlversuche, unbekannte User oder unbekannte IP-Adressen. Im Verdachts- oder Angriffsfall startet QRadar proaktiv Safeguarded Copy, um eine geschützte Backup-Kopie zu erstellen. Dabei steht das Ziel im Fokus, einen sauberen und kon-sistenten Datenbestand zu gewährleisten.

IBM Security Guardium entdeckt und klassifiziert automatisch sensible Daten und stellt ein Real Time Monitoring sicher. IBM Storage Insights und IBM Spectrum Control überwachen den Speicher bezüglich des „normalen“ Verhaltens der I/O-Workloads und gewährleisten damit, dass ein Angriff frühzeitig erkannt wird.

Validieren und Testen der erzeugten Datenkopien

IBM Cyber Vault ergänzt die bestehende Lösung IBM Safeguarded Copy. Dabei werden die Kopien regelmäßig auf ihren sauberen konsistenten Datenstand überprüft.

Cyber Vault ermöglicht ein Echtzeit-Monitoring mit Überprüfung der erzeugten Kopien. Diese Aktionen werden in einer dafür aufgesetzten abgeschirmten Umgebung (Logical Partitions oder VMs) durchgeführt und überwachen die Snapshots von Safeguarded Copy. Mithilfe von standardisierten Datenbank-Tools und anderer Software überprüft Cyber Vault die Snapshots auf Beschädigungen und ihre Datenkonsistenz. Dadurch kann im Angriffsfall sofort entschieden werden, welche Snapshots einen konsistenten sauberen Datenbestand bieten und für den Wiederherstellungsprozess geeignet sind.

Schnelles Recovery

Da sich die Safeguarded Copy-Snapshots auf demselben FlashSystem-Speicher befinden wie die Betriebsdaten, ist die Wiederherstellung mit der gleichen Snapshot-Technologie nahezu ohne Zeitverlust möglich. Die Cyber Vault-Automatisierung verfolgt das Ziel, den Wiederherstellungsprozess schnellstmöglich durchzuführen. So lässt sich das Recovery von mehreren Wochen oder Tagen auf wenige Stunden verkürzen.

Offline-Datenträger zum ultimativen Schutz

Bei Safeguarded Copy handelt es sich um einen Air Gap mit logischer Trennung zwischen Computer und Netzwerk, während beim Offline-Datenträger Tape ein physikalischer Air Gap durch die Auslagerung von Kassetten entsteht. Unternehmen sollten niemals auf ein Tape-Backup verzichten, denn nur Kopien auf einem physisch getrennten Datenträger bieten ultimativen Schutz, wenn nach einem Cyberangriff alle Onlinesysteme zerstört sein sollten.

07 Flexibilität mit IBM Spectrum Storage

IBM Speicherlösungen adressieren sowohl strukturierte als auch unstrukturierte Daten. Sie integrieren Software-basierende Speicher-funktionalitäten und Features in allen Produkten.

Neben den extrem schnellen IBM Flashsystemen (IBM FlashSystem-Familie und IBM DS8880) sorgen die Produkte IBM Spectrum Virtualize, IBM Spectrum Scale und IBM Cloud Object Storage für eine hohe Flexibilität. Denn sie lassen sich sowohl als Hard- und Software als auch als Cloud-Angebot oder in Kombination einsetzen. Dadurch wird der Aufbau bedarfsgerechter maßgeschneiderter Speicherlösungen möglich.

08 Die älteste Speicher-technologie ist wieder gefragt

Old but gold! Anfang der 50er Jahre hielt eine Speicher-technologie Einzug in die Rechenzentren, die heute mit zweistelligen Wachstumsraten gefragter ist denn je. Die Rede ist von Tapes, Bandkassetten. Sie sind als Speichermedium für die IT-Infrastruktur unverzichtbar und bieten dabei eine Vielzahl an Vorteilen:

Ultimativer Schutz vor Cyberangriffen

Bandkassetten können ausgelagert werden und sind daher nicht mehr Bestandteil des Netzwerkes. Sie sind als „Air Gap" – zu Deutsch „Luftspalt" im Einsatz, also gar nicht mit dem Internet verbunden. Cyberangriffe können ihnen nichts anhaben.

Neben den überschreibbaren Kassetten gibt es auch zertifizierte WORM-Kassetten (Write Once Read Many), die eine Datenveränderung oder ein Überschreiben nicht erlauben und damit Compliance-Richtlinien Rechnung tragen. Keine Virensoftware oder andere bösartige Schadprogramme können die Daten auf WORM-Kassetten zerstören.

Compliance-Anforderungen erfüllen

Die Lebensdauer von Tapes unter entsprechenden Lagerbedingungen beträgt mindestens 30 Jahre, während diejenige von Festplatten und anderen optischen Datenträgern deutlich darunter liegen. Damit eignen sich Bandkassetten für viele Branchen, bei denen eine Aufbewahrungsfrist von 10 Jahren und länger vorgeschrieben ist.

Ebenso spielt Tape bei Projekten der Künstlichen Intelligenz wie Machine- und Deep-Learning eine große Rolle. Ist das neuronale Netz einmal trainiert und der trainierte Algorithmus einsetzbar, muss sichergestellt sein, dass die verwendeten Daten zurückverfolgt werden können. Dann lassen sich fehlerhafte Algorithmen leichter auffinden und korrigieren. Ebenso können gesetzliche oder versicherungsrechtliche Auflagen die langfristige Aufbewahrung dieser Daten erfordern.

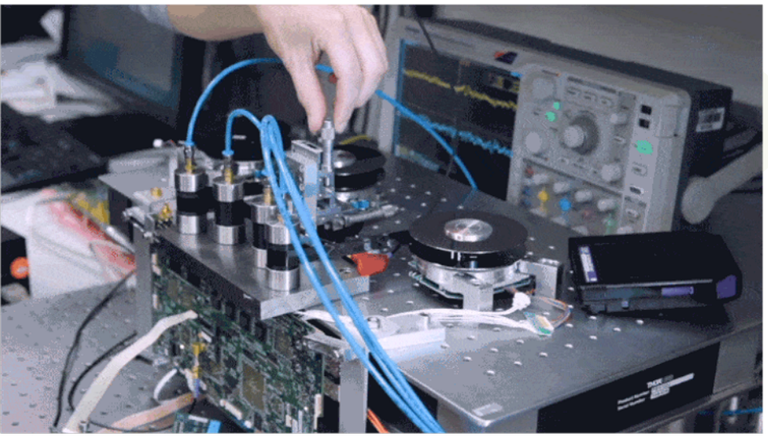
Die Speicherkapazitäten auf Tape sind in den letzten Jahren stetig gestiegen. Die kommende 9. Generation des „Linear Tape Open (LTO)"-Formats wird bis zu 18 Terabyte (TB) an Daten, komprimiert sogar bis zu 45 TB pro Kassette speichern. IBM-Tapes erreichen sogar eine Speicherkapazität von bis zu 20 TB beziehungsweise komprimiert bis zu 60 TB.

Im Vergleich mit optischen Speicherträgern ergibt sich selbst im mittleren Bereich in der Regel eine 10- bis 50-fach höhere Aufnahmekapazität.

Das Kapazitätswachstum wird sich weiter erhöhen, die aktuelle Roadmap des LTO-Konsortiums sieht eine Verdoppelung für die nächste Generation vor. Gleichzeitig erhöhen sich die Schreib- und Lesegeschwindigkeiten. Technologische Grundlage dafür ist die Integration von GMR-Kopftechnik (Giant Magneto- Resistance) in Kombination mit der heute verwendeten Barium/ Eisen-Beschichtung.

Tape Drives	3592 J1A	TS 1120	TS 1120	TS 1130	TS 1140	TS 1150	TS 1155	TS 1160
Release	2003	2005	2006	2008	2011	2014	2017	2018
Capacity	300 GB (JA)	500 GB (JA)	700 GB (JB)	1 TB (JB)	4 TB (JC)	10 TB (JD)	15 TB (JD)	20 TB (JE)
Channels	8	16	16	16	32	32	32	32
Max Data Rate MB/s	40	100	100	160	250	360	360	400

Tape Drives	LTO 1	LTO 2	LTO 3	LTO 4	LTO 5	LTO 6	LTO 7	LTO 8	LTO 9
Release	2000	2002	2004	2007	2010	2012	2015	2017	2021
Capacity	100 GB	200 GB	400 GB	800 GB	1,5 TB	2,5 TB	6 TB	12 TB	18 TB
Channels	8	8	16	16	16	16	32	32	32
FH Data Rate MB/s	15	17 – 35	30 – 80	30 – 120	40 – 140	60 – 160	100 – 300	100 – 360	180 – 400
HH Data Rate MB/s	N/A	N/A	30 – 60	30 – 100	40 – 140	60 – 160	100 – 300	100 – 300	180 – 300



Quelle: IBM

Wie innovativ die Tape-Technologie ist, zeigte sich im Dezember 2020. In diesem Monat wurde Tape-Geschichte geschrieben: IBM und Fujifilm demonstrierten im Rahmen einer Technologie-Demo, wie sich 580 Terabyte auf eine ½ Zoll Kassette schreiben lassen – das sind 317 Gb/in² bei einer Bandlänge und Banddicke wie heute (1255 m Länge und 4,3 µm Dicke). Von der Kapazität her entspricht das 27 x LTO 9 – Bändern.

Möglich wurde dies durch eine neue Beschichtung mit Strontium-Eisen SrFe, deren Partikel als ferro-magnetische Datenträger um den Faktor 4-5 kleiner sind als bei der heutigen Beschichtung mit Barium-Eisen BaFe und nur noch eine Größe von 900 nm³ reflektieren. Dadurch lassen sich die Spurbreiten auf 56.2 nm verkleinern, um – im Vergleich zu heute – das 15 bis 20-fache an Spuren auf dem Band unterzubringen. Das ist Nano-Technologie pur!

Die Versuchsvorrichtung ist auf dem Bild dargestellt. Ein erstes verfügbares Produkt wird in ca. 7 - 8 Jahren erwartet. Dann werden diese hohen Kapazitäten auf Offline-Datenträgern auch dringendst benötigt.

IBM ist heute der führende Entwickler in Sachen Tape-Technologien und inzwischen der größte Tape-Anbieter auf dem Markt. Neben den Bandkassetten und Bandlaufwerken gibt es von IBM intelligente und unterschiedlich große Tape Libraries. Neben der großen und auf dem Markt schnellsten Tape Library IBM TS4500 werden auch kleinere Libraries wie die IBM TS4300 und TS2900 angeboten.

09 Handlungsempfehlungen

Eine effiziente Modern Data Protection-Lösung beruht auf zwei Säulen: Speicherlösungen, mit denen sich Daten schnell wiederherstellen und wiederverwenden lassen, kombiniert mit kostengünstigen Speichertechnologien, die gegen jede Art von Cyberangriffen immun sind.

Zum einen sollte die Lösung ein schnelles operationelles Recovery innerhalb einer Business Continuity Strategie erlauben. Dies wird bei den Produkten im IBM Modern Data Protection-Portfolio durch umfangreiche Funktionalitäten und Snap Shot-Möglichkeiten sichergestellt. Zum anderen sollte immer eine Backup-Kopie auf einem Offline-Datenträger wie Tape vorhanden sein. Google machte dazu vor ein paar Jahren die treffende Aussage: „TAPE is the last line of defense, zu Deutsch: Tape ist die letzte Verteidigungslinie“.

Bei Rückfragen zur IBM Modern Data Protection-Plattform hilft Ihnen unser Ansprechpartner Jan Werner gerne weiter.

Kontaktieren Sie ihn unter:
+49(0) 151.55049912 I Mobil
+49(0) 6181.9984102 I Telefon
E-Mail: jan.werner@entec-systems.de

EnTec
IT Systems GmbH

KONTAKT

EnTec IT Systems GmbH
Platz der Deutschen Einheit 4
98527 Suhl

www.entec-systems.de

Jan Werner
Systemvertrieb Server & Storage – EMEA

+49(0) 151.55049912 I Mobil
+49(0) 6181.9984102 I Telefon
E-Mail: jan.werner@entec-systems.de