EnTec
IT Systems GmbH

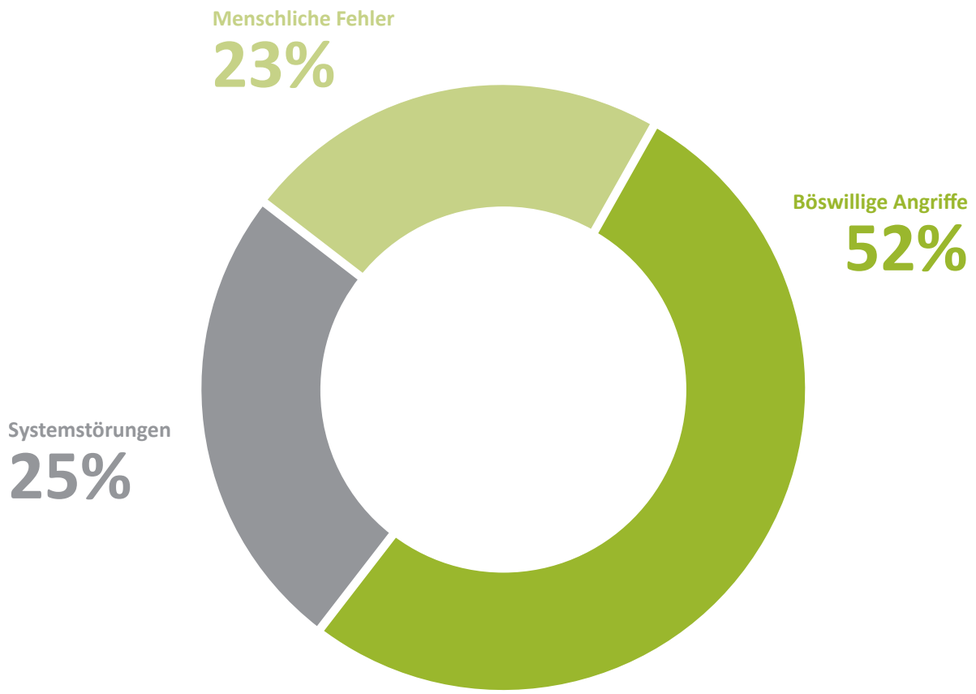
IBM Cyber Vault Technology Guide

Inhalt

01 Cyberangriffe und Ransomware-Attacken

Alle zwei Sekunden wird ein Unternehmen im Jahr 2031 Opfer eines Ransomware-Angriffs, sagt eine aktuelle Studie von Cybersecurity Ventures voraus.

Bereits heute geschieht dies alle elf Sekunden. Dabei entstehen finanzielle Schäden, die seit 2015 um das 57-Fache explodiert sind – auf 20 Milliarden US-Dollar weltweit. Immer häufiger geraten neben Produktivdaten auch Backups ins Visier von Cyberkriminellen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt deshalb, wichtige Daten in einem Offline-Backup zu sichern. Zudem sollte regelmäßig geprüft werden, ob sich die Daten im Notfall schnell wiederherstellen lassen.



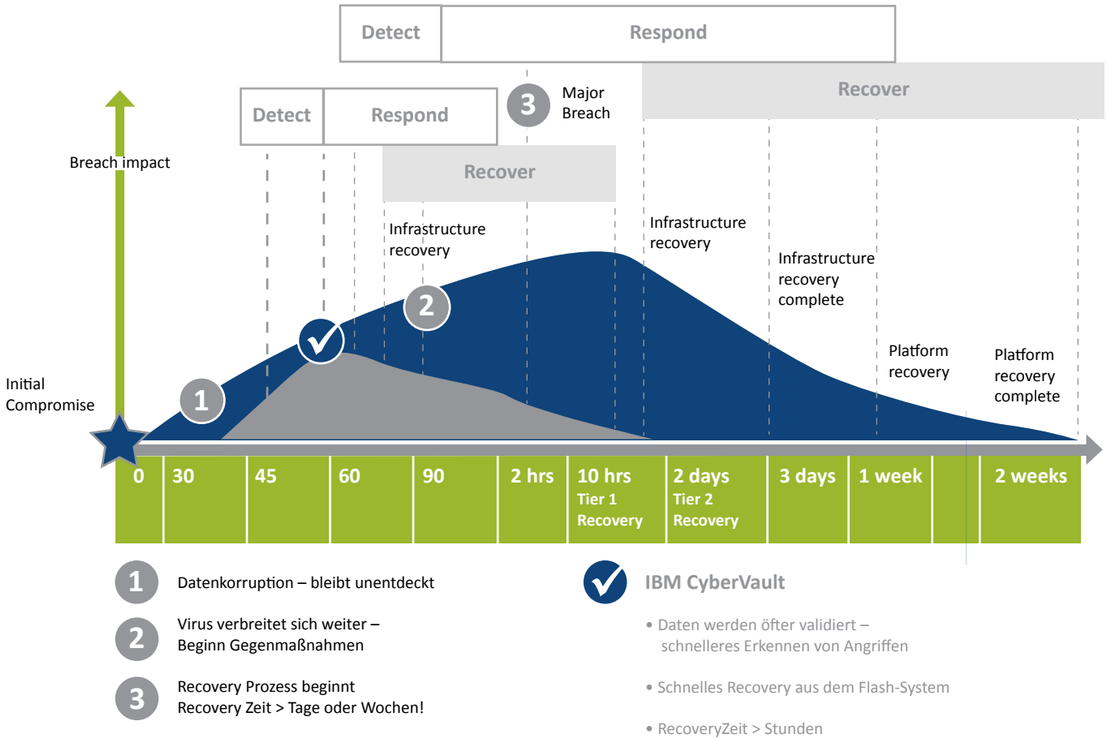
Thaut Images © AdobeStock

02 Kosten durch Cyberangriffe

Laut einem Leifaden des Digitalverbandes Bitkom („Kosten eines Cyber-Schadensfalles“) muss jeder Fall individuell bewertet werden, was die Schadenshöhe angeht. Festhalten lassen sich aber die Kostenarten, die von den jeweiligen Betriebsbeeinträchtigungen oder Unterbrechungen verursacht werden:

- **Kosten für Produktivitätsausfälle**
- **Kosten für Qualitätsbeeinträchtigungen bis hin zum Produktionsausfall**
- **Datensicherung des Fehlerfalls (Festplattendatenbestand inkl. Hauptspeicherzustand) zur Nachstellung in einer Testumgebung**
- **Fehlersuche und -behebung**
- **Kosten für einen möglicherweise notwendigen bzw. erzwungenen System-Shutdown und die damit verbundenen Ausfallzeiten**
- **Gegebenenfalls Neuinstallation des Systems und Aufsetzpunkt der letzten Datensicherung**
- **Einleitung eines Notbetriebsverfahrens für Ersatzprozesse plus Einberufung eines Notfallteams**
- **Herstellung der Betriebsfähigkeit an einem Ausweichstandort, u. a. mit zusätzlichem Personal**
- **Schwenk der IT-Systeme und Anwendungen auf einen Ausweichstandort, u. a. mit zusätzlichem Personal**
- **Einnahmeausfälle, wenn kritische Anwendungen und IT-Systeme nicht mehr zur Verfügung stehen**
- **Ansprüche, Schadensersatzklagen und Vertragsstrafen unterschiedlich**

Zeitprojektionen bei Cyber Angriffen



Nach einer Studie waren 41 Prozent der von Ransomware-Attacken betroffenen Firmen innerhalb eines Monats wieder arbeitsfähig und online. Mehr als die Hälfte (58 Prozent) benötigten für das Recovery mehr als einen Monat. 29 Prozent berichteten, dass die Wiederherstellung über drei Monate dauerte, und bei 9 Prozent waren es sogar fünf bis sechs Monate. Lange Recovery-Zeiten und die damit verbundenen Kosten sind oft die Hauptursache, wenn Unternehmen Insolvenz anmelden müssen. Zeit ist Geld!

Eine Cyber Resiliency-Speicherlösung muss die Fähigkeit besitzen, Schutz vor den unterschiedlichsten Angriffsarten zu bieten.

Zum einen müssen die Daten in Form von speziell geschützten unveränderbaren Kopien logisch oder physisch isoliert werden. Zum anderen ist die kontinuierliche Prüfung auf die Qualität der Daten und deren sauberen Zustand erforderlich. Nur Kopien in einem konsistenten Datenbestand erlauben ein schnelles Recovery auf der Produktionsseite. Parallel dazu muss über Software, Tools und andere Mittel die Möglichkeit geschaffen werden, die Produktionsumgebung konstant auf Unregelmäßigkeiten wie Leistungs- und Kapazitätsverhalten oder Zugriffskontrollen zu überwachen, um Angriffe zu erkennen und einzuschätzen. Nur so lassen sich die optimalen Gegenmaßnahmen etablieren und der richtige Rahmen für schnelle Recovery-Maßnahmen für Files, Datenbanken oder das gesamte System finden und einleiten. IBM Cyber Vault stellt genau diese Mittel zur Verfügung und begrenzt die Recovery-Zeit auf ein Minimum. Dadurch werden für die Wiederherstellung der Produktionsumgebung nicht Wochen oder gar Monate, sondern nur wenige Stunden benötigt.

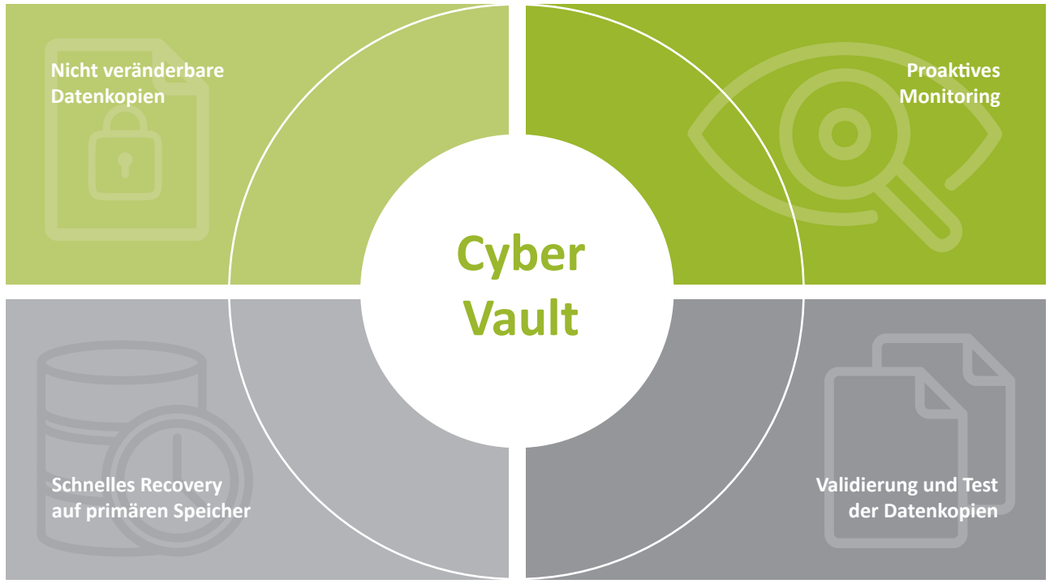
monsitj © AdobeStock

03 Datentresor für IBM Speichersysteme: Safeguarded Copy und Cyber Vault

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**

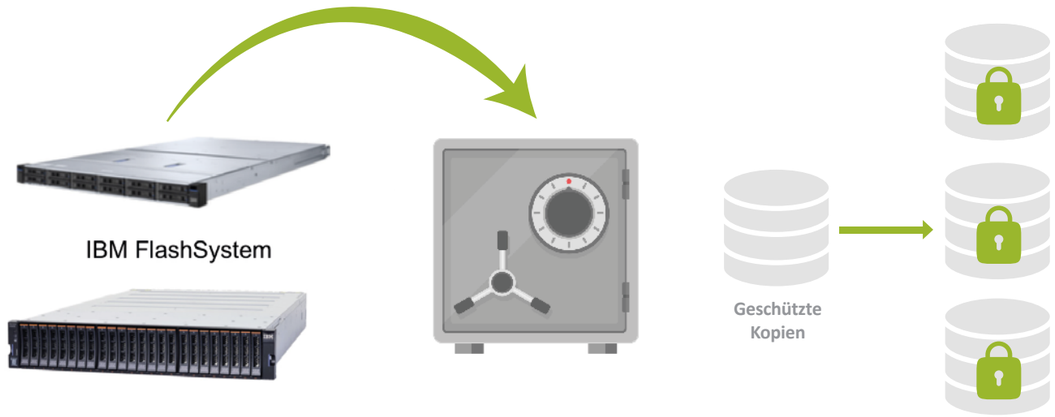


1

04 Erzeugen von nicht veränderbaren Datenkopien

Die Softwarefunktion Safeguarded Copy, die DS8000-Speichersystemen 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 beispielsweise alle paar Stunden Flash-Kopien erzeugt werden. Tritt der Ernstfall ein, kann man auf die Kopie zurückgreifen, die einen konsistenten 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.

Steckbrief: Safeguarded Copy

- **Dedizierte Safeguarded Storage Pools**
- **Erstellen sicherer geschützter Point-in-Time-Kopien (PiT)**
- **Logischer „Air Gap“: Daten sind „offline by Design“**
- **Wie ein WORM (Write Once Read Many)-Backup**
- **Können nicht überschrieben, verändert oder gelesen werden**
- **Können nicht einem Host zugeteilt werden**
- **Anwendungen können nicht auf Daten zugreifen**
- **Nicht autorisierte Benutzer können Daten weder verändern noch löschen**
- **Automatisches Erstellen und Löschen über Scheduler**
- **Stehen ausschließlich für Recovery-Zwecke zur Verfügung**
- **Stellen schnellen Restore im primären Speicher sicher**

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 minimiert. Die Wiederherstellung an sich kann dann per Knopfdruck ohne Zeitverlust durchgeführt werden.

2

05 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 integrierbar. QRadar überwacht dabei alle umgebungsrelevanten Aktivitäten und sucht nach Anzeichen eines Angriffs unterschiedlichster Natur. Dabei werden Login-Versuche außerhalb der regulären Arbeitszeiten 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 konsistenten 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.

Thapana © AdobeStock

3

06 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.

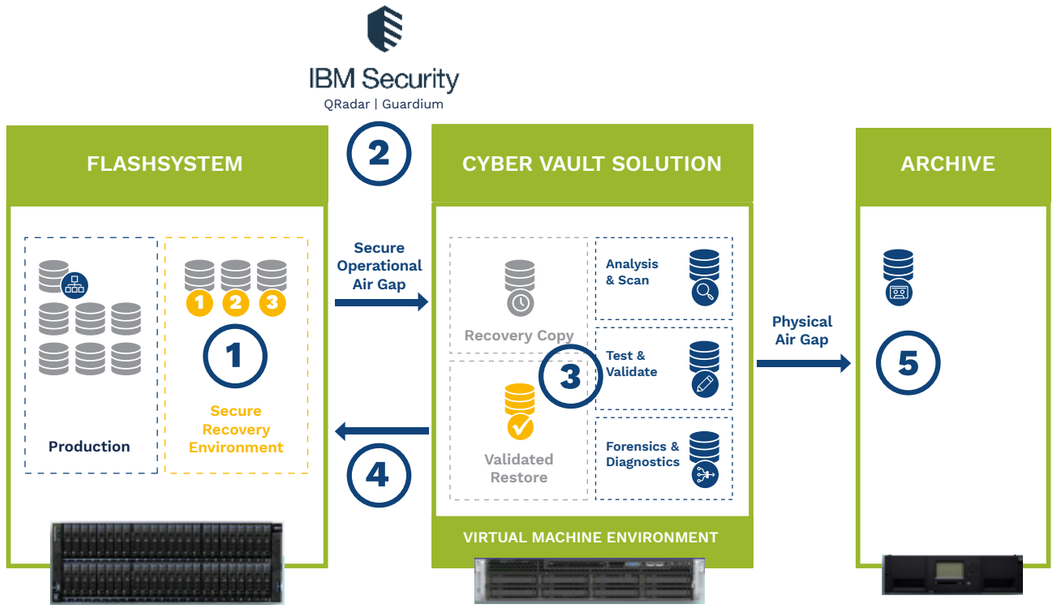
Cyber Vault ermöglicht ein Echtzeit-Monitoring mit Überprüfung der erzeugten Kopien. Diese Aktionen werden in einer dafür aufgesetzten abgeschirmten Umgebung (Logical Partitions oder VMs) durchgeführt und überwachen die Snapshots von Safeguarded Copy. Mithilfe von standardisierten Datenbank-Tools und 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.

4

07 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 CyberVault-Automatisierung verfolgt das Ziel, den Wiederherstellungsprozess schnellstmöglich durchzuführen. So lässt sich das Recovery von mehreren Wochen oder Tagen auf wenige Stunden verkürzen.

IBM Cyber Vault for FlashSystem Framework



1. Erzeugen von nicht veränderbaren Datenkopien
2. Proaktives Monitoring mit Warnhinweisen
3. Validieren und Testen der erzeugten Datenkopien
4. Schnelles Recovery
5. Backup auf Tape als Offline-Datenträger

5

08 Unverzichtbares Tape-Backup

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.

09 Entwickelt für Mainframe-Umgebungen

IBM Cyber Vault und Safeguarded Copy wurden von IBM Lab Services entwickelt und für die DS8000-Speichersysteme in einer Mainframe-Umgebung, die IBM Flash-Systeme und den SAN Volume Controller SV3 eingeführt.

Cyber Vault basiert den Entwicklern zufolge auf einer Lösung, die bereits von mehr als 100 Kunden weltweit mit IBM DS8000-Systemen eingesetzt wird.

Safeguarded Copy ist kostenloser integraler Bestandteil der Software IBM Spectrum Virtualize. SGC und Cyber Vault ergänzen in idealer Weise klassische Sicherheitsverfahren im Onlinebereich wie Spiegelung, Mehrfachspiegelung, Disaster Recovery-Optionen, HyperSwap und Verschlüsselung.

Eine optimale Handhabung der SGC-Funktion bietet die Integration in den IBM Copy Service Manager (CSM). CSM automatisiert Backup und Restores, führt definierte Safe Guarded Copy Policies aus und steuert SGC über mehrere Speichersysteme hinweg. Der IBM Copy Service Manager ist separat in IBM Spectrum Control, IBM Virtual Storage Center (VSC) und in der IBM Spectrum Storage Suite verfügbar. Unterstützt werden die Systeme DS8000, die Flash-Systeme und der SVC.

10 Warum IBM?

IBM bietet ein umfangreiches Portfolio an Hardware, Software und IT-Services, die mit effizienten Lösungen alle Anforderungen im Bereich der Infrastrukturen erfüllen.

Dies beinhaltet die Sicherstellung eines 24 x 7-Betriebs, leistungsstarke und sichere Speichersysteme, maßgeschneiderte Backup-Möglichkeiten und rasches Disaster Recovery im Falle eines Hackerangriffs oder anderer Störungen.

Die IBM Lösungen können flexibel an veränderte Geschäftsanforderungen angepasst werden und decken alle Bereiche der Datenspeicherung ab. Ob im Rechenzentrum, in Cloud- und Multicloud-Umgebungen oder hybriden Infrastrukturen – IBM Storage und IBM Security bieten umfassende und maßgeschneiderte Schutzmöglichkeiten vor Cyberattacken, Werkzeuge zur frühen Erkennung von Angriffen sowie ausgeklügelte, intelligente und schnelle Recovery-Optionen.


Thaut Images © AdobeStock

Platinum
Business
Partner

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