

IBM Safeguarded Copy: Datentresor für Primärspeicher

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

Bereits heute geschieht dies alle 11 Sekunden. Dabei entstehen finanzielle Schäden, die seit 2015 um das 57-fache auf 20 Milliarden US-Dollar weltweit explodiert sind.

Immer mehr geraten nicht nur die Produktiv-Daten ins Visier der Cyberkriminellen, sondern auch die Backup-Daten.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt deshalb, wichtige Daten und Informationen in einem Offline-Backup zu sichern.

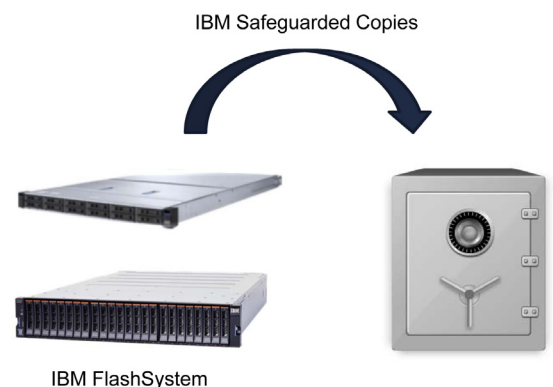
Zudem sollte regelmäßig geprüft werden, ob sich die Daten im Notfall schnell wiederherstellen lassen.

Hierbei hilft IBM Safeguarded Copy:

Die Software-Funktion Safeguarded Copy (SGC) erstellt automatisch Point-in-Time Kopien (PiT) in einem Datensafe innerhalb der IBM Mainframe-Familie DS8000 und der IBM FlashSystem-Modelle.

Dabei werden die PiT-Snapshots in einen dedizierten Storage Pool geschrieben - dort sind sie unveränderlich und unzugänglich, wie bei einem WORM (Write IBM FlashSystem Once Read Many)-Backup (logisches „Air Gap“).

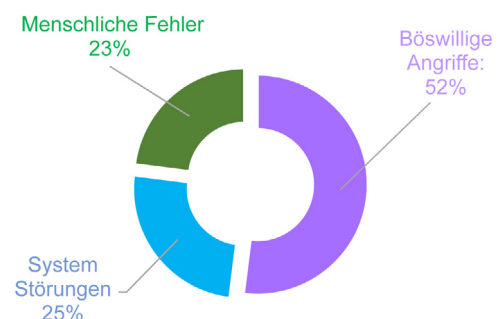
Somit werden Modifikationen oder Löschung von PiT-Kopien durch Benutzer oder Ransomware verhindert.



Safeguarded Copy Schutz

- vor Cyber- und Malware-Attacken
- vor Ransomware Angriffen
- vor vorsätzlichen Fremdverschlüsselungen
- vor anderen bössartigen Aktivitäten
- vor internen arglistigen Attacken

Im Gegensatz zu anderen Snapshot-Lösungen ermöglicht IBM SGC den Anwendern, die PiT-Kopien auf der Basis regelbasierter Backups selbst zu konfigurieren, ohne dass der Hersteller eingeschaltet werden muss.



Ihr Ansprechpartner:

Jörg Fricke
Vertriebsleitung

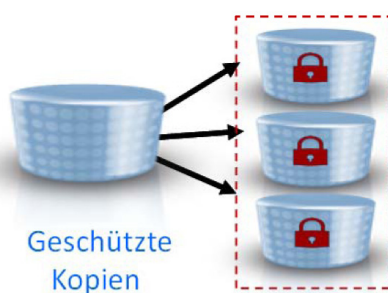
Telefon: +49 (0) 511-51529-441
E-Mail: fricke@netzlink.com

Netzlink Informationstechnik GmbH
IT-Campus Westbahnhof
Hollerithallee 17
30419 Hannover

Vor Datenmanipulationen und Datenlöschungen geschützt

Der große Praxisvorteil von SGC für Storage-Anwender: Safeguarded-Kopien können nicht überschrieben und verändert werden, stehen dem Produktionsbetrieb nicht mehr zur Verfügung und lassen sich ausschließlich für Recovery-Zwecke einsetzen.

Sie sind damit vor Cyberangriffen, Ransomware-Attacken und anderen böswilligen Aktivitäten geschützt und erlauben im Disaster-Fall ein schnelles Recovery im primären Speicher.



Safeguarded Copy Eigenschaften

- **Dedizierte Safeguarded Storage Pools.**
- **Erstellen von sicheren geschützten 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.**
- **Lassen sich nicht einem Host zuteilen.**
- **Anwendungen können nicht darauf zugreifen.**
- **Nicht-authorisierte Benutzer können Daten weder verändern noch löschen.**
- **Automatisierte Verwaltung über Scheduler.**
- **Stehen ausschließlich für Recovery-Zwecke zur Verfügung.**
- **Stellen schnellen Restore im primären Speicher sicher.**

Für Mainframe-Umgebungen entwickelt

Safeguarded Copy wurde im Mainframe-Umfeld entwickelt und steht heute den IBM DS8000-Systemen und der IBM FlashSystem-Familie zur Verfügung. Die Funktion ist kostenloser integraler Bestandteil der IBM Spectrum Virtualize Software ab Release 8.4.2. SGC ergänzt klassische Sicherheitsverfahren im Online-Bereich wie Spiegelung, Mehrfachspiegelung, Disaster-Recovery-Optionen, HyperSwap und Verschlüsselung in idealer Weise.

Auf Tape Backup nicht verzichten

Eine optimale Handhabung der Safeguarded Copy-Funktion bietet die Integration in den IBM Copy Service Manager (CSM). CSM automatisiert Backup und Restores, führt definierte Safeguarded 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. Auch bei aktivem Einsatz von Safeguarded Copy darf auf ein Backup auf Tape als physischer Offline-Datenträger nicht verzichtet werden. Nur Backup-Kopien auf Tape bieten einen ultimativen Schutz, selbst wenn Online-Systeme völlig zerstört werden sollten.

In IBM Security QRadar integrierbar

QRadar kann alle umgebungsrelevanten Aktivitäten überwachen und sucht kontinuierlich nach Anzeichen eines Angriffs unterschiedlichster Natur. Im Angriffsfall startet QRadar proaktiv Safeguarded Copy, um eine geschützte Backup-Kopie sicherzustellen.

Ihr Ansprechpartner:

Jörg Fricke
Vertriebsleitung

Telefon: +49 (0) 511-51529-441
E-Mail: fricke@netzlink.com

Netzlink Informationstechnik GmbH
IT-Campus Westbahnhof
Hollerithallee 17
30419 Hannover