

Sicher in die Zukunft mit IBM® Power® Cyber Vault



Mehr als 330.000 digitale Angriffe im Jahr 2025

BSA Bundeslagebild: Die Gefahr von Cyberangriffen in Deutschland bleibt hoch, Cyberkriminalität ist eine der größten Herausforderungen für die öffentliche Sicherheit.

Nach den USA und Kanada ist Deutschland unter den Top 3 auf der Rangliste der Angriffsziele, es sind vor allem kleinere und mittelständische Unternehmen betroffen, ebenso viele Kommunen und Stadtwerke.

„Der Schaden durch Erpressung, Sabotage oder Hacker-Angriffe ist riesig. Er wird auf mehr als 200 Milliarden Euro im Jahr geschätzt.“

Quelle: <https://ibm.biz/BSA-Cyber2026>



NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Das NIST entwickelt Standards, Richtlinien, Best Practices und Ressourcen für Cybersicherheit und Datenschutz.

Dazu gehört die Erstellung spezifischer Informationen, die Organisationen sofort in die Praxis umsetzen können, wie das Cybersecurity Framework.

Dieses besteht aus fünf Phasen: Identify, Protect, Detect, Respond, Recover.

<https://www.nist.gov/>



IBM Power Cyber Vault

IBM Power Cyber Vault lehnt sich an das NIST Cybersecurity Framework an, fasst jedoch die Phasen Respond und Recover zusammen.

Cyber Security und Cyber Resilience:

Unternehmen müssen sowohl cybersicher als auch cyberresilient sein: Cyber Security hilft, Angreifer fernzuhalten, Cyber Resilience bezeichnet die Fähigkeit einer Organisation, trotz eines Cybervorfalles soweit möglich den Betrieb aufrechtzuerhalten oder schnell wiederherzustellen.



Identify

IBM Security und Resilience Assessment und IBM Power Cyber Vault Solution and Design Workshop

In diesen zwei kostenlosen Workshops wird Ihre Organisation, Ihre Prozesse und Strategie bezüglich operativer und Cyber-Resilienz überprüft und eine individuelle, detaillierte Lösung gemeinsam mit Ihnen erarbeitet.

Starten Sie hier mit der Bewertung Ihrer Cyber Resilienz: ibm.biz/CR-Assessment



Protect

Automatisierte, unveränderliche (immutable) Snapshots und Backups, die im Power Cyber Vault gespeichert sind, schützen Ihre Daten gegen Ransomware-Verschlüsselung oder ungewollte Löschung.

Diese geschützten Snapshots/Backups helfen, die Anforderungen an Ihr Recovery Point Objective (RPO) und Ihr Recovery Time Objective (RTO) zu erfüllen.



Detect

Echtzeit-Bedrohungserkennung

Eine schnelle Erkennung und Meldung von sicherheitsrelevanten Ereignissen und ungewöhnlichen Aktivitäten ist wichtig, um unverzüglich reagieren zu können.

Dies wird gewährleistet durch die Überwachung und Erkennung auf verschiedenen Ebenen der Power Cyber Vault Umgebung:

- Betriebssystem (Trusted Execution)
- IBM Storage mit FCM4 Flash Modulen
- Endpoint Detection and Response (EDR / PowerSC)

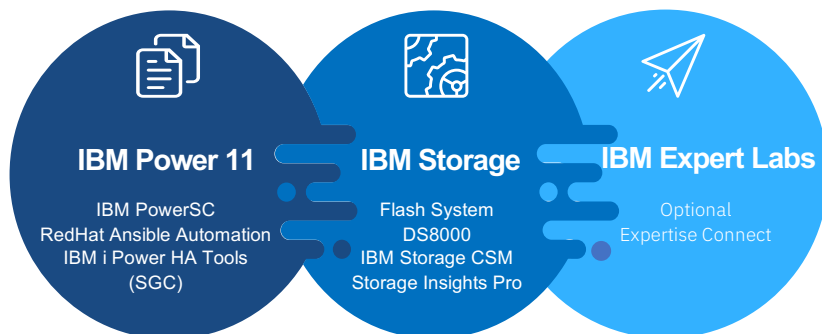


Respond und Recover

Respond: Regelmäßig oder bei Erkennung von Bedrohungen werden automatisiert die Snapshots im Clean Room überprüft und die aktuellsten, nicht betroffenen Kopien markiert.

Recover: Bei Bedarf (kein Fehlalarm bzw. nach Schliessung der Sicherheitslücke) und nach Genehmigung durch den Administrator beginnt die Wiederherstellung in der Produktionsumgebung, um die RPO- und RTO-Anforderungen zu erfüllen.

Schützen Sie Ihren Betrieb mit IBM® Power® Cyber Vault



Eine vollständig integrierte Cyber-Resilienz-Lösung, um sich verändernde Cyber-Bedrohungen zu erkennen, mit schneller Wiederherstellung zu reagieren, die Geschäftskontinuität zu maximieren und Risiken und Komplexität zu minimieren.

Kontaktieren Sie uns:

Power-Team-D-A-CH@ibm.com



IBM PowerSC: EDR & Compliance

Endpoint Detection and Response (EDR): Durch **kontinuierliche Endpunkt-Überwachung** und **Echtzeit-Bedrohungsanalyse** werden verdächtige Aktivitäten schnell erkannt – darunter Trojaner, Viren, Ransomware, Änderungen der Datenintegrität, Netzwerk Intrusion, etc.

Unternehmen können Bedrohungen schnell eindämmen und beheben – automatisiert oder manuell.

Möglichkeit der umfassenden Konformitäts-Prüfung auf Basis vorkonfigurierter Sicherheitsprofile.



IBM Storage Integration

- Mit IBM Storage Defender Copy Services Manager und IBM Flash- oder DS8000 Storage Systemen werden regelmässig unveränderliche Snapshots der relevanten Daten erstellt.
- Die integrierte Ransomware-Threat Detection dieser Storage Systeme sendet in Echtzeit Warnmeldungen zu aktiven Angriffen an IBM PowerSC über Storage Insights Pro.
- Nach einem Cyberangriff werden die erstellten Snapshots im Clean Room geprüft und können bei Bedarf schnell wiederhergestellt werden.



Power11 Systemsicherheit

IBM Power11 Systeme sind nach den **Prinzipien von Zero Trust** entwickelt und bieten Ransomware erheblich geringere Angriffsmöglichkeiten:

- **Quantum Safe** Firmware Integrität
- Möglichkeit zur **Ende-zu-Ende Datenverschlüsselung**
- **Sichere Virtualisierung** mit PowerVM: Deutlich weniger CVEs als andere Hypervisor



Anwendungssicherheit

- **Applikationskonsistente Snapshots** für IBM Db2 und Oracle Datenbanken auf AIX möglich
- **Zero Trust Execution für AIX** hilft beim Erkennen, Verhindern und Melden von nicht genehmigten, ausführbaren Dateien und Anwendungen
- IBM i Workload kann durch die IBM i PowerHA Tools gegen Cyberattacken abgesichert werden



IBM Expert Labs Services

Individueller, kostenloser IBM Power Cyber Vault Workshop – ein Sicherheits- und Resilience Assessment um Risiken zu erkennen und die Lösung zu konzipieren:

- Betrachtung der Organisation, Prozesse und Strategien bezüglich operationaler und Cyber Resilience
- Erstellen einer detaillierten Lösung auf Grundlage der Cyber-Resilience-Ziele, der Infrastruktur und der erforderlichen Services für die IBM Power-Umgebung

Kostenpflichtige Umsetzung der Lösung inklusive **Automatisierung basierend auf Red Hat Ansible Automation Platform.**

Expert Labs Kontakt: systems-expert-labs@ibm.com



PowerHA Tools für IBM i

Kundenspezifische Implementierung des Cyber Vault mit IBM Storage Virtualize oder DS8000 über Copy Services Manager (CSM) auf Basis des IBM Power Cyber Vault Solution und Design Workshops.

Die PowerHA Tools beinhalten die IBM i Befehle, Programme und APIs zur Verwaltung der Storage Systeme und des CSM, um die Lösung von einer IBM i-Partition aus zu automatisieren.

PowerHA Tools können mit Storage Insights Pro oder direkt mit dem Storage-System verbunden werden, um Verschlüsselungen zu erkennen.