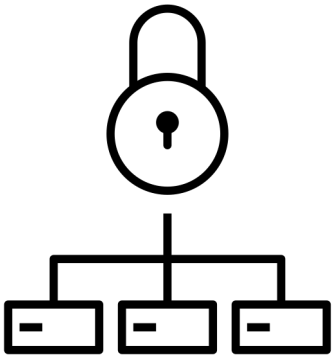


Schützen Sie Ihre Daten mit IBM® Power Servern!

Sicherheit als Designvorgabe

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

- **Quantum Safe Firmware** Integrität
- Starke Isolation der VMs untereinander
- Sicheres Booten des Guest-OS und eingebaute Betriebssystem Runtime Integrität
- Ermöglicht **Ende-zu-Ende Daten-verschlüsselung** und Schlüsselmanagement

Sichere Virtualisierung

Anzahl der Schwachstellen (CVE)

IBM PowerVM	VMware ESXi	MS Hyper-V	KVM (alle Plattformen)
23	**352**	**284**	**434**

Quelle/Suche Stand 24. Juli 2026
https://cve.mitre.org/cve/search_cve_list.html

Hardwareverschlüsselung

Symmetrische, transparente Hauptspeicherverschlüsselung ohne Beeinträchtigung der Performance ist Standard seit IBM Power10 Systemen.

Performante Verschlüsselung durch vier zusätzliche Verschlüsselungseinheiten pro Power Prozessor seit Power10. Damit wird eine **2,5-fach höhere AES-Verschlüsselungsperformance** gegenüber älteren Power Prozessoren erreicht.

IBM Hardware Crypto Cards

Schützen Sie Ihre sensiblen Daten und verschlüsseln Sie diese effizient mit den IBM PCIe Cryptographic Coprocessor Karten.

Diese entsprechen u.a. den **Sicherheits-anforderungen des Deutschen Kreditwirtschaft Ausschusses (GBIC).**

https://ibm.biz/IBMCryptoCard

Post-Quantum Verschlüsselung

IBM Power11 Systeme unterstützen effizient **Post-Quantum-Verschlüsselungs-Algorithmen** (PQC) für Firmware und Live Partition Mobility (LPM).

IBM PowerSC Software kann eine Auflistung erstellen, welche Keys, Certificates und Ciphers bereits Quantum Safe sind – für ihre gesamte System Umgebung.

Die IBM Crypto Express Karten ab 4769 implementieren bereits PQC-Signaturen entsprechend dem aktuellen Entwicklungsstand.

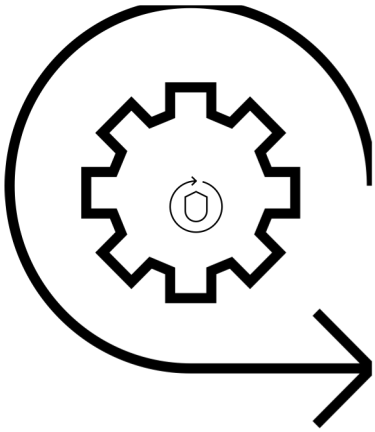
Unterstützung durch Experten

IBM Expert Labs unterstützt Sie bei der Analyse und Optimierung bestehender Security Architekturen für Ihre IBM Power Server und der zugehörigen Storage- und Netzwerk-Infrastruktur.

Wenden Sie sich an Ihren IBM Vertriebspartner oder schicken Sie uns eine E-Mail:

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

Juli 2026



Rundum Sicher! Schützen Sie Ihre Daten und Anwendungen mit den Möglichkeiten der IBM® Power11 Server

SAP HANA

Herausragende Sicherheit rund um SAP HANA mit IBM Power11 Servern durch Härtung von Linux und Schutz der Integrität:

- Proaktiver Schutz vor Side-Channel Attacken
- Strikte read/write Richtlinien für Kernel Seiten

Enterprise Linux Plattform-Sicherheit ab Power10:

- Transparente Hauptspeicherverschlüsselung
- On-Chip Verschlüsselungseinheit integriert sich in das SAP HANA Verschlüsselungs-Framework

ITIC-Studie 2025

„IBM Z und Power dominieren weiterhin und bieten zum **16. Mal** in Folge die beste Zuverlässigkeit, Betriebszeit und Sicherheit für Server."

IBM Power Server haben eine ungeplante durchschnittliche Ausfallzeit im Jahr von **0.3** Sekunden.

„Eine Mehrheit von **88%** der befragten Unternehmen nennt **Sicherheitsvorfälle** als Hauptursache für ungeplante Ausfallzeiten".

Source: ITIC 2025 Global Server Hardware, Server OS Reliability Report

Sicherheits-Zertifizierungen

Zertifizierungen Ihrer IBM Power Umgebung:

- Common Criteria EAL4+ Zertifizierung für das AIX-Betriebssystem[1]
- Common Criteria EAL2+ Zertifizierung für die IBM Power Virtualisierung-Software PowerVM[2]
- FIPS 140-2 Level 4 für IBM Crypto Express Cards 4769[3] und 4770[4]

1) https://ibm.biz/AIX-EAL4
2) https://ibm.biz/PowerVM-EAL2
3) https://ibm.biz/4769-FIPS140-2
4) https://ibm.biz/4770-FIPS140-2

IBM Power Cyber Vault

IBM Power und IBM Storage: Gemeinsam sind sie stärker!

Erkennung von Anomalien in Echtzeit
im FlashCore Modul 4, das in den aktuellen IBM Flash-Systemen eingesetzt wird und Ransomware Warnungen in PowerSC.

Unveränderbare Snapshots:
Datenspeicherung für die schnelle Wiederherstellung.

Automatisierte Snapshot Erstellung, Clean Room Einrichtung mit Validierung der Snapshots mit Red Hat Ansible.

Compliance mit IBM PowerSC

Kontrolle des **Sicherheits- und Compliance-Status** aller IBM Power-Systeme im Rechenzentrum über ein zentrales Kontroll-Center:

- Umfassende Konformitäts-Prüfung mit vorkonfigurierten Sicherheitsprofilen
- Erkennen und Beheben von Sicherheitslücken
- Anzeigen von Anomalien im Betrieb und Orchestrieren von Reaktionen auf Anomalien

Endpoint Detection and Response (EDR) mit IBM PowerSC

Durch **kontinuierliche Endpunkt-Überwachung und Echtzeit-Bedrohungsanalyse** werden verdächtige Aktivitäten sofort erkannt – darunter Trojaner, Viren, Ransomware, Änderungen der Datenintegrität und Network Intrusion.

Je nach Schweregrad des Vorfalls können manuelle oder automatisierte Reaktionen gestartet werden, sodass Unternehmen Bedrohungen schnell eindämmen und beheben können.

Juli 2026