IBM **Power Systems**

Ein mehrschichtiger Sicherheitsansatz mit POWER9

Sorgen Sie für nahtlosen Schutz und eine Optimierung Ihrer IT-Infrastruktur

Weitere Informationen erhalten Sie von Ihrem IBM Business Partner®.

[Name des Business Partner]

[Telefonnummer/E-Mail-Adresse des Business Partner]

[Website des Business Partner]

Enterprise IT im Zeitalter ausgefeilter Cyberangriffe

Schwerwiegende Datenschutzverletzungen, über die in letzter Zeit viel berichtet wurde, haben dafür gesorgt, dass Sicherheit inzwischen für viele Führungskräfte ein zentrales Thema ist. Darum wachsen in Unternehmen die Sicherheitsbudgets. Steigende Ausgaben und technologischer Wandel haben zum Teil jedoch auch mehr Komplexität und Risiken mit sich gebracht, was eine Bedrohung für die IT-Sicherheit darstellt. Eine Forrester-Umfrage unter Sicherheitsexperten aus dem Jahr 2019 hat ergeben, dass „weniger als ein Viertel“ der Befragten „voll zufrieden mit seinem Sicherheitsportfolio ist, wenn es darum geht, moderne Threat-Intelligence-Funktionen zu entwickeln, die Produktivität von Sicherheitspersonal zu erhöhen, Erkenntnisse aus Daten zu ziehen und die Effizienz zu steigern.“[1]

Eine Hauptsorge von Sicherheitsexperten ist die wachsende Zahl und Raffinesse von Angriffen, durch die immer mehr Aspekte moderner Geschäftsabläufe Risiken ausgesetzt werden. Schwachstellen in den Hardware- und Firmwareebenen stellten vor nicht langer Zeit keine großen Bedrohungen dar; sie haben sich jedoch inzwischen zu Hauptzielen entwickelt.

Unterdessen werden die Risiken im Zuge der Weiterentwicklung von IT-Architekturen weiter wachsen. In vielerlei Hinsicht lassen sich die Herausforderungen im Bereich Cybersicherheit, die Ihr Unternehmen heute bewältigen muss, auf zwei Fakten zurückführen: Der IT-Stack wird immer größer, sodass Hacker – als direkte Folge davon – ihre Angriffshorizonte erweitern.

Die Realitäten der aktuellen Bedrohungslandschaft

Unternehmen verlassen sich auf ihre Sicherheitssysteme, wenn es darum geht, Risiken für geistiges Eigentum, vertrauliche Unternehmensinformationen, sensible persönliche Daten und Datenschutz zu verhindern. Welchen strategischen Ansatz für IT-Sicherheit sie dabei wählen, ist von entscheidender Bedeutung.

Oft wird Schutz durch einen Geschäfts-, Compliance- und Budget-orientierten Ansatz implementiert. Dieser Ansatz hat zwar seinen Nutzen, schützt Geschäftsprozesse jedoch nicht ausreichend vor der steigenden Zahl an mit IT-Systemen verbundenen Risiken. Außerdem können dabei wichtige disziplinübergreifende Aspekte übersehen werden.

Eine ideale Vorgehensweise beinhaltet Planung und Evaluierung zur Ermittlung von Risiken in zentralen, sicherheitsrelevanten Bereichen. IBM Power® Systems und der POWER9™ Prozessor bieten einen ganzheitlichen, mehrschichtigen Ansatz für Ihre Sicherheitsstrategie, die in Ihrem Unternehmen zuverlässigen Schutz und Compliance ermöglicht. Dieser mehrschichtige Ansatz umfasst

- Hardware
- Firmware
- Hypervisor
- Betriebssystem
- PowerSC

Durch Anwendung eines ganzheitlichen Sicherheitsansatzes kann Ihr Unternehmen die Anforderungen von vier Realitäten, die sich aktuell auf die Sicherheitslandschaft auswirken, zuverlässig bewältigen.

Hacker werden immer ausgefeilter.
Je mehr Unternehmen die Begrenzungen traditioneller lokaler Rechenzentren hinter sich lassen, desto mehr müssen sich Cyberangreifer besondere Methoden einfallen lassen. Diese beschränken sich nicht mehr nur auf die Netzwerkebene, was breitere Angriffshorizonte und gefährlichere Angriffe mit sich bringt.

Immer mehr Geschäfte werden über mobile und Edge-Geräte erledigt. Daten in einem Unternehmen lassen sich von Mitarbeitern nun praktisch überall speichern und aufrufen — egal ob über Server, Hybrid-Cloud-Umgebungen oder verschiedene mobile sowie Edge-Geräte. Dieses ständige Hin und Her zwischen Server und Geräten ist eine Nebenwirkung der fortgesetzten digitalen Transformation — dabei entsteht jedoch ein völlig neuer Angriffsvektor, den Hacker für sich nutzen können.

Strengere Vorschriften wirken sich auf Risikoprofile aus.
Die Prozesse, die zur Einhaltung regulatorischer Auflagen implementiert werden, können unbeabsichtigte Risiken mit sich bringen. Dabei ist die DSGVO der Europäischen Union nur eine aktuelle Entwicklung eines wachsenden Trends: Behörden achten viel genauer darauf, wie Unternehmen mit Daten umgehen. Dadurch steigt jedoch die Komplexität im Geschäftsbetrieb Ihres Unternehmens.

Mitarbeiter stellen regemässig Schwachstellen dar.
Ihr Personal ist stets mit einem gewissen Risiko verbunden – egal, welche Sicherheitskontrollen Sie implementieren oder wie gut Sie mit Sicherheitsschwachstellen umgehen. Die harte Arbeit, die Sie in die Sicherung von Endpunkten und Einhaltung von Vorschriften stecken, kann durch unbeabsichtigte Fehler oder schlau ausgeführte Angriffe zunichte gemacht werden Gleichzeitig fällt es vielen Unternehmen schwer, kompetentes Sicherheitspersonal zu finden und zu halten, sodass ein fortwährendes Kompetenzdefizit besteht.

Volumen, Vielfalt und Geschwindigkeit moderner Cyberbedrohungen werden weiter zunehmen, während IT-Infrastrukturen weiterentwickelt und an neue Anforderungen bei Technologie, Arbeitskultur und Compliance angepasst werden. Das heißt, dass Sie Ihre Sicherheitsstrategie über die Netzwerkebene hinaus ausbauen müssen.

Der Bedarf nach einem ganzheitlichen, mehrschichtigen Sicherheitsansatz

Eine Integration von Sicherheit in jede Ebene Ihres Stacks lässt sich durch Implementierung verschiedener Sicherheitslösungen von Drittanbietern erreichen. Dieser Ansatz erhöht die vorhandene Komplexität jedoch weiter – und ist mit zusätzlichen Schwachstellen und Risiken für Ihr Netzwerk verbunden. Ihre optimale Wahl besteht in der Verwendung eines mehrschichtigen, ganzheitlichen Ansatzes, der alle Daten und Systeme Ihres Unternehmens schützt und gleichzeitig Komplexität minimiert.

Vor diesem Hintergrund hat IBM® das IBM Security Framework entwickelt, damit Sie bei Nutzung eines umfassenden Ansatzes für geschäftsorientierte Sicherheit alle Aspekte von IT-Sicherheit richtig verwalten können.

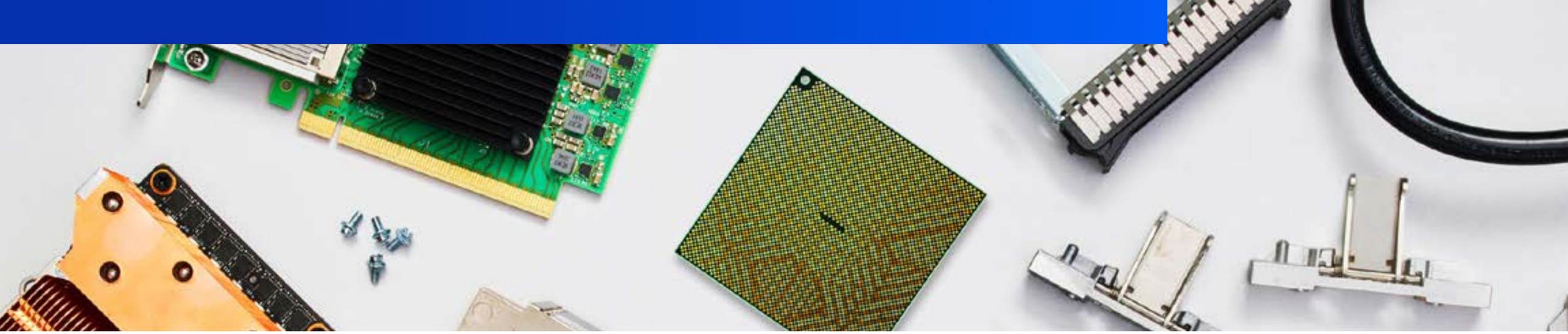
Das IBM Security Framework beinhaltet folgende Schwerpunkte:

1. **Infrastruktur** – Schützen Sie Ihr Unternehmen mit Informationen über Benutzer, Inhalte und Anwendungen vor ausgefeilten Angriffen.
2. **Erweiterte Sicherheits- und Bedrohungsdaten** – Verschaffen Sie sich Informationen über Schwachstellen und Angriffsmethoden und wenden Sie sie mithilfe von Sicherheitstechnologien an.
3. **Menschen** — Verwalten und erweitern Sie die Unternehmensidentität mit fortschrittlicher Identitäts-Überwachung über Sicherheitsdomänen hinweg.
4. **Daten** — Schützen Sie die Vertraulichkeit und Integrität der wichtigsten Ressourcen Ihres Unternehmens.
5. **Anwendungen** – Reduzieren Sie die Kosten für die Entwicklung sicherer Anwendungen.
6. **Sicherheitsinformationen und -analysen** – Erhöhen Sie die Sicherheit durch zusätzlichen Kontext, Automatisierung und Integration.

Erfahren Sie mehr über das IBM Security Framework und darüber, wie Sie noch gründlicher analysieren können mit dem IBM Security Blueprint.

Wie IBM Power Systems und POWER9 den gesamten Stack schützen

Mit IBM Power Systems profitieren Sie von durchgängiger Sicherheit, die nahtlos in den gesamten Stack integriert ist – von Prozessor und Firmware über OS und Hypervisoren bis hin zu Anwendungen und Netzwerkressourcen sowie der Verwaltung von Sicherheitssystemen.



Hardware, Firmware und Hypervisor

24 Verschlüsselungs-Engines

Der POWER9 Prozessor hat doppelt so viele Verschlüsselungs-Engines wie sein Vorgänger POWER8®. Somit können Sie ruhende oder aktive Daten in allen Ebenen des Stacks 2-mal so schnell (oder noch schneller) verschlüsseln wie vorher.

On-Chip-Beschleuniger

POWER9 verfügt über On-Chip-Beschleuniger, die GZIP-Dateien deutlich schneller komprimieren und dekomprimieren als Software. So können Sie ganze VMs rasch verschlüsseln und entschlüsseln sowie im Netzwerk sicher verschieben.

Secure Boot in POWER9

Secure Boot schützt die Systemintegrität durch Verifizierung und Validierung aller Firmwarekomponenten mithilfe digitaler Signaturen. Die gesamte von IBM veröffentlichte Firmware ist digital signiert und überprüfbar. Alternativ können Sie Ihre eigene Firmware installieren und die Hierarchie der öffentlichen Schlüssel ersetzen, welche für die Verifizierung benötigt werden.

Trusted Boot und Trusted Platform Module (TPM)

Die Trusted Boot Funktion in POWER9 ermöglicht die Überprüfung und Remoteverifizierung (Attestation) aller Firmwarekomponenten auf Ihrem Server. Die Trusted Boot Funktion nutzt das TPM, welches als Root of Trust (RoT) zur Messung des Software-Stacks dient. Die Verifizierung wird vom TPM selbst signiert, damit Sie genau wissen, dass die Firmware in keiner Weise manipuliert worden ist.

IBM PowerVM® Enterprise Hypervisor

IBM PowerVM® hat im Vergleich zu wichtigen Wettbewerbern eine herausragende Erfolgsbilanz im Bereich der Sicherheit vorzuweisen, sodass Sie Ihre virtuellen Maschinen (VMs) und Cloud-Umgebungen zuverlässig schützen können.

Betriebssystem

IBM Power Systems bietet branchenführende Sicherheitsfunktionen für eine breite Palette an Betriebssystemen wie IBM AIX®, IBM i und Linux®. Die Merkmale variieren je nach Betriebssystem; Beispiele für Funktionen sind jedoch:

- Zuweisung von Verwaltungsfunktionen, die normalerweise dem Root-Anwender vorbehalten sind, ohne Beeinträchtigung der Sicherheit
- Verschlüsselung von Daten auf der Dateiebene mittels individueller Schlüsselspeicher
- Mehr Kontrolle über die Benutzern zur Verfügung stehenden Befehle und Funktionen sowie Steuerung der Objekte, auf die sie zugreifen können
- Protokollierung des Zugriffs auf ein Objekt im Sicherheitsprüfjournal durch Verwendung von Systemwerten und Objektprüfungswerten für Benutzer und Objekte
- Verschlüsselung ganzer Laufwerke, erst durch Verschlüsselung eines Objekts und dann durch Schreiben in der verschlüsselten Form
- Messung und Verifizierung jeder einzelnen Datei vor dem Ausführen oder Öffnen für den anfordernden Benutzer

Workloads, VMs und Container

Workloads sind nicht mehr auf lokale Rechenzentren beschränkt; vielmehr werden sie kontinuierlich in virtualisierte und Cloud-Umgebungen migriert.

Darum nutzen viele Unternehmen Container, um neue und vorhandene Anwendungen über hybride Infrastrukturen hinweg bereitzustellen. Diese zunehmend dynamischen Umgebungen und Workloads setzen ebenso flexible Sicherheitsfunktionen voraus.

Live Partition Mobility (LPM)

IBM Power Systems bietet Ihnen die Möglichkeit, aktive Daten zu schützen. LPM schützt VMs durch Verschlüsselung, wenn Sie eine Migration von einem System auf ein anderes vornehmen. Wenn Sie über virtualisierte lokale Rechenzentren und/oder hybride Cloud-Umgebungen verfügen, ist diese Fähigkeit essentiell.

Protected Execution Facility

Die Protected Execution Facility ist ein Beispiel dafür, wie IBM Power Systems diese Ebene des Stacks schützt. Es handelt sich dabei um eine POWER9 Funktion, die Ihre VMs in sicherem Arbeitsspeicher verschlüsselt und ausführt, um Zugriff durch kompromittierte Hypervisoren zu verhindern. Außerdem erhalten böswillige Insider oder Administratoren mit Zugriff auf die VMs in Cloud-Umgebungen keinen Zugriff auf die Workloads, die im sicheren Arbeitsspeicher ausgeführt werden. Die Entschlüsselung erfolgt ausschließlich in verifizierten Systemen.

In IBM Power Systems integrierte Sicherheitsprodukte

IBM PowerSC ist ein integriertes Portfolio für Enterprise Security und Compliance in cloudbasierten und virtuellen Umgebungen. Es befindet über Ihrem Stack und bietet eine webgestützte UI für die Verwaltung der Sicherheitsmerkmale von IBM Power Systems, welche von unten nach oben angeordnet sind.

IBM PowerSC reduziert den Zeitaufwand, Kosten und Risiken

Dank seiner Vereinfachungs- und Automatisierungsfunktionen hilft Ihnen IBM PowerSC dabei, durch Optimierung von Compliance- und Audit-Prozessen Zeit zu sparen und Kosten zu verringern. Außerdem werden Sicherheitsrisiken reduziert, da die Transparenz im Stack erhöht wird.

Funktionen der IBM PowerSC Standard Edition

Compliance-Automatisierung

IBM PowerSC ist mit vordefinierten Profilen ausgestattet, die verschiedenste Branchenstandards unterstützen. Sie können diese Profile anpassen und mit Enterprise-Regeln kombinieren, ohne XML anfassen zu müssen.

Real-time Compliance

Erkennt und warnt Sie, wenn jemand sicherheitskritische Dateien öffnet oder handhabt.

Trusted Network Connect (TNC)

Warnt Sie, wenn eine VM nicht das vorgeschriebene Patch-Level aufweist. Außerdem werden Sie benachrichtigt, wenn Fixes verfügbar werden.

Trusted Boot

Ermöglicht die Überprüfung und Remoteverifizierung aller Firmwarekomponenten, die auf Ihrem Server ausgeführt werden.

Trusted Firewall

Schützt und leitet internen Netzwerkverkehr zwischen den AIX, IBM i und Linux-Betriebssystemen weiter.

Trusted Logging

Erstellt zentrale Prüfprotokolle, die sich leicht sichern, archivieren und verwalten lassen.

Vorkonfigurierte Berichterstattung & interaktive Zeitleiste

Die IBM PowerSC Standard Edition unterstützt das Auditing mit fünf vorkonfigurierten Berichten. Außerdem verfügen Sie über eine interaktive Zeitleiste zum Anzeigen der Lebensdauer und Ereignisse einer VM.

Wenn Sie mehr über die Leistungsmerkmale von IBM PowerSC erfahren möchten, konsultieren Sie das folgende IBM Redbook, “Simplify Management of Security and Compliance with IBM PowerSC in Cloud and Virtualized Environments.”

Der effektivste Sicherheitsansatz ist ein optimierter Ansatz

Da die Fähigkeiten von Hackern immer ausgefeilter werden und der technologische Fortschritt neue Schwachstellen in Unternehmen mit sich bringt, benötigen Sie eine mehrschichtige, ganzheitliche Sicherheitslösung, die die Betriebskomplexität nicht weiter erhöht. IBM Power Systems schützt alle Ebenen Ihres Stacks mit nahtlos integrierten, umfassenden Lösungen aus der Hand eines Anbieters. Eine Sicherheitsstrategie, die auf verschiedenen Komponenten unterschiedlicher Anbieter basiert, verursacht Komplexität, die letztendlich teuer werden kann – und das in mehrerer Hinsicht.

Sicherheit aus der Hand eines Anbieters bietet natürliche Vorteile, die Ihre Sicherheitsstrategie vereinfachen und stärken. Aufbauend auf drei Jahrzehnten Branchenführerschaft im Bereich Sicherheit beinhaltet IBM Power Systems umfangreiche Partnerschaften mit anderen Unternehmen innerhalb und außerhalb von IBM, die vorhandene Sicherheitskenntnisse ergänzen und vertiefen. Dank dieser Partnerschaften kann IBM Power Systems auf eine noch größere Community an Sicherheitsexperten zurückgreifen und dafür sorgen, dass sich Probleme schnell erkennen und zuverlässig beheben lassen. Mit Unterstützung der Abteilungen IBM Security und IBM Research™ sowie unter Verwendung des PowerSC Portfolios wehren POWER9 Server zudem verschiedenste Bedrohungen ab, darunter auch Insider-Angriffe – egal wo im Stack.

Optimieren Sie mit einem ganzheitlichen, mehrschichtigen Ansatz die Sicherheit im gesamten Stack – und sorgen Sie für einen sicheren Geschäftsbetrieb.

Wenn Sie genau wissen möchten, wie POWER9 Server zum Schutz Ihrer Infrastruktur beitragen können, wenden Sie sich an Ihren IBM Vertriebsbeauftragten oder IBM Business Partner.

1. “Complexity In Cybersecurity Report 2019: How Reducing Complexity Leads To Better Security Outcomes,” Forrester Research, Inc., Mai 2019

33028633DEDE-00