Ein mehrschichtiger Sicherheitsansatz mit IBM Power

Wesentliche Infrastruktur für einen Zero-Trust-Ansatz

Inhaltsverzeichnis

Unternehmens-IT im Zeitalter hoch entwickelter Cyberangriffe

Die heutige IT-Landschaft

Seit Beginn der COVID-19-Pandemie wurde eine enorme Zahl verheerender Datenschutzverletzungen verzeichnet. Die durchschnittlichen Kosten einer Datenschutzverletzung belaufen sich inzwischen auf 4,24 Mio. USD. Das sind 10 % mehr als im vergangenen Jahr (3,86 Mio. USD). Dies ist der stärkste Anstieg, den die Branche in den letzten sieben Jahren erlebt hat[1], und macht Sicherheit zu einer ihrer wichtigsten Prioritäten. In der hochverfügbaren Welt von heute steht die Verbesserung der Sicherheitsstrategie im Fokus vieler Führungskräfte, damit ihr Unternehmen sicher, schnell und zuverlässig arbeiten kann. Dies hat jedoch zur Folge, dass die Sicherheitsbudgets immer weiter steigen. Die steigenden Ausgaben und der technologische Wandel führen jedoch zu neuen Komplexitäten und Risiken, die die IT-Sicherheit fortwährend bedrohen. Eine der größten Sorgen von Sicherheitsfachleuten ist die wachsende Zahl ausgeklügelter Angriffsvektoren, die heute mehr Aspekte der Unternehmen gefährden als je zuvor.

Schwachstellen auf der Ebene von Hard- und Firmware waren in nicht allzu ferner Vergangenheit vielleicht noch kein großer Grund zur Besorgnis. In der heutigen Bedrohungslandschaft sind sie jedoch zu Hauptzielen geworden.

In vielerlei Hinsicht lassen sich die Herausforderungen der Cybersicherheit, die Ihr Unternehmen heute bewältigen muss, auf zwei empirische Wahrheiten reduzieren:

- Der IT-Stack wird immer größer und Hacker erweitern ihre Angriffsbereiche.
- Unternehmen müssen zukünftigen Bedrohungen immer einen Schritt voraus sein, um ihre Plattformen mit der höchsten Sicherheitsstufe zu schützen und ihre Hybrid-Cloud-Infrastruktur zu sichern.

4,24 Mio. USD

Die durchschnittlichen Kosten einer Datenschutzverletzung belaufen sich inzwischen auf **4,24 Mio. USD**. Das sind 10 % mehr als im vergangenen Jahr (3,86 Mio. USD).

Die Realität der aktuellen Bedrohungslandschaft

Ein ganzheitlicher Ansatz

Um aktuelle und künftige Bedrohungen von geistigem Eigentum, vertraulichen Unternehmensinformationen, Kundendaten und dem Datenschutz zu verhindern, verlassen Unternehmen sich auf ihre Sicherheitssysteme.

Die strategische Herangehensweise von IT-Sicherheitsfachleuten ist bei der Prävention von Datenschutzverletzungen und Cyberangriffen von entscheidender Bedeutung. Sicherheitslücken können nicht nur zu Ausfallzeiten führen, sondern sind für Unternehmen auch sehr kostspielig. Angriffe durch Ransomware stellen dabei die größte Bedrohung dar und kosten Unternehmen im Durchschnitt 4,62 Mio. USD pro Angriff[1]. Die Integrität der IBM® Power®-Plattform kann das Risiko von Ransomware durch die Implementierung von Endpunkterkennung und -reaktion (Endpoint Detection and Response/EDR) und Zero Trust-Konzepten wie die kontinuierliche Mehrfaktorauthentifizierung (MFA) verringern.

Ein geschäftsorientierter, auf die Einhaltung von Vorschriften ausgerichteter oder monetär begründeter Ansatz allein kann keinen ausreichenden Schutz der Geschäftsprozesse gegen die zunehmende Zahl von IT-Systemrisiken bieten. Bei isolierten Ansätzen können wichtige disziplinübergreifende Aspekte einer effizienten, integrierten Sicherheitsstrategie übersehen werden. Die ideale Vorgehensweise beinhaltet eine Planung und Bewertung, um die Risiken in allen wichtigen sicherheitsrelevanten Bereichen zu ermitteln. Die Technologie von IBM Power und die Systeme auf IBM® Power10-Prozessorbasis bieten einen ganzheitlichen, mehrschichtigen Zero-Trust-Ansatz für Ihre Sicherheitsstrategie, der sicherstellt, dass Ihr Unternehmen geschützt ist und die gesetzlichen Anforderungen einhält. Dieser mehrschichtige Ansatz umfasst:

- Hardware
- Betriebssystem
- Firmware
- IBM® PowerSC 2.0-Technologie
- Hypervisor

Mit einem ganzheitlichen Sicherheitsansatz kann Ihr Unternehmen den Anforderungen der Bedrohungen begegnen, die die Sicherheitslandschaft beeinträchtigen.

Hacker werden immer raffinierter

Je mehr ein Unternehmen die Grenzen traditioneller lokaler Rechenzentren verlässt und in hybride Cloud- oder Multi-Cloud-Umgebungen wechselt, desto mehr Raum haben Cyberangreifer, neue Strategien zu entwickeln. Die Umsetzung des Prinzips der geringstmöglichen Zugriffsrechte und die Verstärkung perimeterbasierter Kontrollmechanismen tragen dazu bei, die zunehmende Zahl von Bedrohungen zu bewältigen. Ihre Methoden beschränken sich nicht mehr nur auf die Netzwerkebene wie früher. Cyberkriminelle arbeiten heute in einem erweiterten Tätigkeitsbereich und dies führt zu noch wirksameren Angriffen.

Mit höherem Datenzugriff wird Sicherheit immer wichtiger

Daten innerhalb eines Unternehmens können heute praktisch überall von Beschäftigten gespeichert und abgerufen werden – auf Servern, in Hybrid-Cloud-Umgebungen und auf zahlreichen mobilen und Edge-Geräten. Diese unentwirrbare Überschneidung aus Servern und Geräten ist ein Nebenprodukt der anhaltenden digitalen Transformation und Modernisierung. Durch diese Zugriffsmöglichkeiten wird eine Vielfalt an Angriffsvektoren geschaffen, die ausgenutzt werden können.

Strengere gesetzliche Bestimmungen wirken sich auf Risikoprofile aus

Dieselben Prozesse, die für die Einhaltung von gesetzlichen Bestimmungen eingerichtet werden, können auch zu einem unbeabsichtigten Risikopotenzial führen. Die Datenschutz-Grundverordnung (DSGVO) ist nur eine dieser jüngsten Entwicklungen eines wachsenden Trends. Die Behörden achten nun sehr viel genauer darauf, wie Unternehmen Daten nutzen. Dies erhöht jedoch auch die Komplexität der täglichen Betriebsabläufe.

Beschäftigte sind Schwachstellen, die ausgenutzt werden können

20 % aller Datenschutzverletzungen im vergangenen Jahr gingen auf kompromittierte Anmeldedaten von Beschäftigten zurück[1]. Abgesehen von Anmeldedaten sind Phishing-Betrug und E-Mail-Kompromittierung weitere Einfallstore, mit denen Beschäftigte unwissentlich Unternehmensdaten gefährden. Ihre Belegschaft stellt immer ein gewisses Risiko dar – ganz gleich, welche Sicherheitsmaßnahmen Sie eingerichtet haben oder wie gut Sie mit Schwachstellen umgehen. Im Zeitalter der Cyberkriminalität ist es unerlässlich, Beschäftigte zu diesen häufigen Sicherheitsbedrohungen zu schulen und ein Meldesystem einzurichten. Die mühsame Arbeit, die Sie in die Sicherung von Endgeräten und in Ihre Compliance investiert haben, kann durch einen Fehler oder einen raffinierten bösartigen Angriff zunichte gemacht werden.

Gleichzeitig fällt es vielen Unternehmen schwer, kompetentes Personal für die Cybersicherheit zu finden und zu halten, und sie sehen sich mit einem ständigen Mangel an Fachkräften konfrontiert. Um diesem Fachkräftemangel entgegenzuwirken, können Unternehmen ein vereinfachtes Sicherheitsmanagement einführen, das den Betrieb, die Compliance, das Patching und das Monitoring automatisiert. Profitieren Sie von einer End-to-End-Sicherheit, die durch zusätzliche Endgerät-Erkennung schützt, ohne zusätzliche Ressourcen zu benötigen.

Umfang, Vielfalt und Geschwindigkeit der heutigen Cyberbedrohungslandschaft werden sich nur noch vervielfachen, da sich die IT-Architekturen weiterentwickeln und an die sich ändernde Technologie, Arbeitskultur und Compliance anpassen. Das bedeutet, dass sich auch Ihre Sicherheitsstrategie über die Netzwerkebene hinaus weiterentwickeln muss.

Zero-Trust-Strategie als wesentliche Komponente

Ein ganzheitlicher Ansatz

Die Umsetzung von Zero Trust-Konzepten kann Unternehmen helfen, die Sicherheit in einer oft komplexen IT-Umgebung zu gewährleisten. IT-Fachkräfte haben Probleme mit der Transparenz und den Kontrollmaßnahmen in Hybrid-Cloud- und Multi-Cloud-Landschaften. Mit Zero Trust werden die Risiken durch die Umstellung auf eine umfassendere Strategie gemanagt. Dabei werden die Zugriffskontrollen eingeschränkt, ohne die Leistung oder das Benutzererlebnis zu beeinträchtigen. Die Integration von Sicherheit in jede Ebene Ihres Stacks kann durch die Implementierung verschiedener Sicherheitslösungen von Drittanbietern erreicht werden. Dieser Ansatz ist jedoch noch komplexer und führt zu noch mehr Sicherheitslücken und Angriffspunkten in Ihrem Netzwerk. Am besten ist es, wenn Sie sich für einen mehrschichtigen Zero-Trust-Ansatz entscheiden. Dadurch werden alle Daten und Systeme Ihres Unternehmens gesichert und gleichzeitig die Komplexität minimiert. Vor diesem Hintergrund trägt das IBM® Information Security Framework dazu bei, dass jeder IT-Sicherheitsaspekt angemessen berücksichtigt werden kann, indem ein ganzheitlicher Ansatz für geschäftsorientierte Sicherheit genutzt wird.

Das IBM Information Security Framework hat folgende Schwerpunkte:

1. Infrastruktur – Schutz vor raffinierten Angriffen mit Erkenntnissen zu Usern, Inhalten und Anwendungen.
2. Erweiterte Sicherheits- und Bedrohungsanalyse – mehr Wissen über Schwachstellen und Angriffsmethoden und Anwendung dieser Erkenntnisse mithilfe von Schutztechnologien.
3. Personen – Verwaltung und Erweiterung der Unternehmensidentität über Sicherheitsdomänen hinweg mit umfassenden Identitätsinformationen.
4. Daten – Sicherung des Datenschutzes und der Integrität der vertraulichsten Daten in Ihrem Unternehmen.
5. Anwendungen – Reduzierung der Kosten für die Entwicklung sicherer Anwendungen.
6. Sicherheitsinformationen und Analysen – Optimierung der Sicherheit durch zusätzlichen Kontext, Automatisierung und Integration.
7. Zero-Trust-Philosophie – Verbindung und Schutz der richtigen User mit den richtigen Daten bei gleichzeitigem Schutz Ihres Unternehmens.

Erfahren Sie mehr über das IBM Security Framework (PDF, 25,2 MB) und informieren Sie sich noch umfassender.

So sichert IBM Power-Technologie den Stack

Mehr über IBM Power erfahren

Mit der Technologie von IBM Power können Sie die Cyberresilienz verbessern und Risiken mit umfassender End-to-End-Sicherheit managen, die sich über den gesamten Stack erstreckt – angefangen mit dem Prozessor und der Firmware über das Betriebssystem und Hypervisoren bis hin zu Anwendungen, Netzwerkressourcen und zum Sicherheitssystemmanagement.

Hardware, Firmware und Hypervisor

On-Chip-Beschleuniger
Der Prozessorchip von IBM Power10 wurde entwickelt, um die Leistung der Seitenkanalentschärfung zu erhöhen. Er ist mit einer verbesserten CPU-Isolation gegenüber Serviceprozessoren ausgestattet. Dieser 7-nm-Prozessor kann eine bis zu dreimal höhere Kapazität und damit eine höhere Leistung liefern[2].

End-to-End-Verschlüsselung
Die transparente Speicherverschlüsselung der IBM Power-Lösungen wurde entwickelt, um eine End-to-End-Sicherheit zu ermöglichen, die den anspruchsvollen Sicherheitsstandards entspricht, die Unternehmen heute erfüllen müssen. Zudem wird die Beschleunigung der Kryptografie, quantensichere Kryptografie und vollständig homomorphe Verschlüsselung zum Schutz vor künftigen Bedrohungen unterstützt. Die beschleunigte Verschlüsselung für das neueste IBM Power-Systemmodell bietet eine 2,5-mal schnellere Advanced Encryption Standard (AES)-Verschlüsselungsleistung pro Kern als die IBM Power E980-Technologie[3]. Unternehmen können von der transparenten Speicherverschlüsselung profitieren, ohne zusätzliche Verwaltungseinstellungen vornehmen zu müssen.

EDR-Software
Aufgrund der zunehmenden Bedrohungen von außen ist die Endpunktsicherheit für den Schutz von Kundendaten und digitalen Ressourcen von entscheidender Bedeutung. Indem potenzielle Bedrohungen am Endpunkt erkannt werden, können Unternehmen schnell handeln und Vorfälle beheben, ohne dass die Geschäftskontinuität unterbrochen wird. Ein integrierter Ansatz eliminiert Komplikationen und schützt Ihr Unternehmen selbst vor gefährlichsten Angriffen.

2,5-mal

Die beschleunigte Verschlüsselung für das neueste IBM Power-Systemmodell bietet eine **2,5-mal schnellere Advanced Encryption Standard (AES)-Verschlüsselungsleistung pro Kern** als die IBM Power E980-Technologie[3].

Prinzipien wie Mehrfaktorauthentifizierung und minimale Rechtevergabe bieten zusätzlichen Schutz, indem sie alle APIs, Endpunkte, Daten und Hybrid-Cloud-Ressourcen sichern.

Zero-Trust-Prinzipien
Unternehmen führen zunehmend Zero-Trust-Prinzipien ein, um diesen wachsenden Bedrohungen zu begegnen. Methoden wie Mehrfaktorauthentifizierung und Least Privilege bieten zusätzlichen Schutz, indem sie alle APIs, Endpunkte, Daten und Hybrid-Cloud-Ressourcen schützen.

Das IBM-Zero-Trust-Framework setzt dieses Konzept in die Praxis um.

- **Sammeln von Erkenntnissen** – Verständnis von Usern, Daten und Ressourcen, um Sicherheitsrichtlinien zu erstellen, die für einen umfassenden Schutz erforderlich sind.
- **Schutz** – Schutz des Unternehmens durch schnelle, konsistente Überprüfung von Kontexten und Durchsetzung von Richtlinien.
- **Erkennung und Reaktion** – Behebung von Sicherheitsverletzungen mit minimalen Auswirkungen auf den Geschäftsbetrieb.
- **Analyse und Verbesserung** – Kontinuierliche Verbesserung des Sicherheitsniveaus durch Anpassung von Richtlinien und Praktiken, um fundiertere Entscheidungen treffen zu können.

Mit der Einführung von Zero-Trust-Prinzipien können Unternehmen auf sichere Weise innovativ sein und skalieren.

Secure-Boot-Funktion der IBM Power10-Lösungen
Die Secure-Boot-Funktion wurde entwickelt, um die Systemintegrität zu schützen, indem alle Firmware-Komponenten durch digitale Signaturen verifiziert und validiert werden. Die gesamte von IBM bereitgestellte Firmware ist digital signiert und wird im Rahmen des Boot-Prozesses überprüft. Alle IBM Power-Systeme werden mit dem Trusted Platform Module ausgeliefert, das Messwerte zu allen auf einem Server geladenen Firmware-Komponenten sammelt und deren Überprüfung und Remote-Verifizierung ermöglicht.

IBM PowerVM Enterprise Hypervisor
Der IBM PowerVM® Enterprise Hypervisor verfügt über eine hervorragende Sicherheitsbilanz im Vergleich zu den großen Konkurrenzprodukten, sodass Sie Ihre virtuellen Maschinen (VMs) und Cloud-Umgebungen zuverlässig schützen können.

Betriebssystem

IBM Power Systems bietet führende Sicherheitsfunktionen für ein breites Spektrum an Betriebssystemen wie IBM® AIX®, IBM i und Linux®. EDR für IBM Power-Technologie kann zusätzliche Sicherheit für VM-Workloads bereitstellen und so einen vollständigen Schutz an jedem Endpunkt innerhalb des Netzwerks sicherstellen.
Für Systeme mit Kennwortschutz verwenden die Betriebssysteme AIX und Linux die Mehrfaktorauthentifizierung (MFA) von IBM PowerSC, bei der zusätzliche Authentifizierungsebenen für alle Benutzer erforderlich sind und die vor Malware zum Entschlüsseln von Kennwörtern schützt. Die genauen Funktionen variieren je nach Betriebssystem. Einige Beispiele umfassen folgende Möglichkeiten:

- Zuweisung von Verwaltungsfunktionen, die normalerweise dem Root-Benutzer vorbehalten sind, ohne die Sicherheit zu beeinträchtigen
- Verschlüsselung von Daten auf Dateiebene durch individuelle Schlüsselspeicher
- Größere Kontrolle über die Befehle und Funktionen, die Usern zur Verfügung stehen, sowie über die Objekte, auf die sie zugreifen können
- Protokollierung des Zugriffs auf ein Objekt im Sicherheitsprotokoll unter Verwendung von Systemwerten und Objekt-Prüfwerten für User und Objekte
- Verschlüsselung über ein ganzes Laufwerk hinweg, indem ein Objekt zunächst verschlüsselt und dann in dieser verschlüsselter Form geschrieben wird
- Messung und Überprüfung jeder Datei, bevor sie für den aufrufenden User geöffnet wird

Workloads, VMs und Container

Workloads sind nicht mehr auf lokale Rechenzentren beschränkt, sondern werden immer weiter in virtualisierte Hybrid-Cloud- und Multi-Cloud-Umgebungen verlagert. Viele Unternehmen führen beispielsweise Container ein, um neue und bestehende Anwendungen in hybriden Infrastrukturen bereitzustellen.

Diese zunehmend dynamischen Umgebungen und Workloads erfordern ebenso vielseitige Sicherheitsfunktionen. Die Lösungen von IBM Power werden den Sicherheitsanforderungen gerecht, indem sie den Schutz der Workloads durch beschleunigte Verschlüsselungsalgorithmen, sichere Schlüsselspeicherung und CPU-Support für Post-Quantum-Kryptografie und vollständig homomorphe Verschlüsselungsalgorithmen (FHE) wahren.

Um den besonderen Sicherheitsanforderungen von Container-Implementierungen gerecht zu werden, ist IBM zudem Partnerschaften mit unabhängigen Softwareanbietern (ISVs) wie Aqua Security eingegangen, die mit der IBM Power-Technologie und der Red Hat® OpenShift® Container Platform arbeiten, um Container während ihres gesamten Lebenszyklus umfassend zu sichern.

IBM Power-Server sind so konzipiert, dass sie Daten vom Unternehmensstandort bis zur Cloud mit End-to-End-Speicherverschlüsselung und beschleunigter kryptografischer Leistung schützen. Die integrierten Richtlinien für cloudnative Workloads, einschließlich VMs, Container und Serverless-Funktionen, wurden entwickelt, um Red Hat OpenShift- und IBM Power-Kunden bei der Integration ihrer Sicherheits- und Compliance-Anforderungen für die Anwendungsmodernisierung zu unterstützen.

Live Partition Mobility (LPM)
Mit der IBM Power-Technologie können Sie Daten in Bewegung sichern. LPM schützt VMs durch Verschlüsselung, wenn Sie von einem System auf ein anderes migrieren müssen. Wenn Sie virtualisierte Rechenzentren vor Ort, Hybrid-Cloud-Umgebungen oder beides nutzen, ist diese Funktionalität entscheidend.

Integrierte Sicherheitsprodukte für IBM Power-Lösungen

IBM PowerSC 2.0-Technologie

Die IBM® PowerSC 2.0-Technologie ist ein integriertes Portfolioangebot für Unternehmenssicherheit und Compliance in Cloud- und virtuellen Umgebungen. Es arbeitet oberhalb Ihres Stacks und bietet eine webbasierte Benutzeroberfläche für die Verwaltung der Sicherheitsfunktionen der IBM Power-Technologie, die auf der untersten Ebene der Lösungen liegen.

Mit seinen Funktionen für die Vereinfachung und Automatisierung kann die IBM PowerSC 2.0-Technologie Zeit, Aufwand und Risiken reduzieren, indem Überwachung und Durchsetzung der Compliance rationalisiert werden. Diese Lösung kann Protokollprozesse unterstützen und ermöglicht es Kunden, Compliance-Zertifizierungen effizienter zu erreichen. Sie kann außerdem Sicherheitsrisiken verringern, indem die Transparenz über den Stack erhöht wird.

Funktionen der IBM PowerSC 2.0 Standard Edition

Mehrfaktorauthentifizierung (MFA)-Technologie
MFA ist jetzt in IBM PowerSC 2.0-Lösungen integriert. Dies vereinfacht die Bereitstellung von MFA-Mechanismen nach dem Zero-Trust-Prinzip „Never trust, always verify“. Dieser Ansatz unterstützt alternative Faktoren für die Benutzeranmeldung mit RSA SecurID-basierten Authentifizierungs- und Zertifikatsauthentifizierungsoptionen, einschließlich gemeinsamer Zugriffskarten (Common Access Card/CAC) und Schlüsselkarten für die Überprüfung der persönlichen Identität (Personal Identification Verification, PIV). IBM PowerSC MFA erhöht das Sicherheitsniveau von Systemen, indem zusätzliche Authentifizierungsfaktoren für die Benutzer verlangt werden.

IBM PowerSC 2.0-Technologie reduziert Zeit, Aufwand und Risiken

EDR-Funktionen
IBM PowerSC 2.0-Lösungen führen EDR für Linux auf IBM Power-Workloads ein. Sie bieten die neuesten, dem Branchenstandard entsprechenden Funktionen für die Verwaltung der Endpunktsicherheit, einschließlich der Erkennung und Prävention von unbefugtem Zugriff, Protokollprüfung und -analyse, Anomalieerkennung und Reaktion auf Sicherheitsvorfälle.

Compliance-Automatisierung
Die IBM Power-Familie verfügt über vordefinierte Profile, die eine Vielzahl von Branchenstandards unterstützen. Sie können diese Profile anpassen und mit Unternehmensregeln zusammenführen, ohne Extensible Markup Language (XML) anfassen zu müssen.

Compliance in Echtzeit
Erkennt und warnt Sie, wenn jemand sicherheitskritische Dateien öffnet oder mit ihnen interagiert.

Trusted Network Connect
Warnt Sie, wenn eine VM nicht das vorgeschriebene Patch-Level erreicht hat. Diese Funktion benachrichtigt Sie auch, wenn Fixes verfügbar werden.

Trusted Boot
Ermöglicht die Überprüfung und Remote-Verifizierung der Integrität aller Softwarekomponenten, die auf logischen AIX-Partitionen laufen.

Trusted Firewall
Schützt und leitet den internen Netzverkehr zwischen den Betriebssystemen AIX, IBM i und Linux.

Trusted Logging
Erstellt zentralisierte Protokolldateien, die einfach als Backup zu sichern, zu archivieren und zu verwalten sind.

Vorkonfigurierte Berichterstellung und interaktive Zeitachse
Die IBM PowerSC Standard Edition unterstützt die Protokollierung mit fünf vorkonfigurierten Berichten. Sie erhalten zudem die Funktion einer interaktiven Zeitleiste, um den Lebenszyklus und die Ereignisse einer VM zu verfolgen.

Erfahren Sie, wie Sie die Verwaltung der IT-Sicherheit und Compliance mit IBM PowerSC in der Cloud und in virtualisierten Umgebungen vereinfachen können.

Ein leistungsstarker Sicherheitsansatz mit nahtloser Integration

Nahtlose Integration

Da Cyberkriminelle ihre Methoden immer weiter verbessern und die technologische Entwicklung neue Schwachstellen in heutige Unternehmen trägt, ist die Integration einer mehrschichtigen Zero-Trust-Sicherheitslösung, die Ihr Unternehmen nicht noch komplexer macht, von entscheidender Bedeutung. IBM Power-Lösungen können jede Ebene Ihres Stacks, vom Edge über die Cloud bis zum Kern, mit den nahtlos integrierten, umfassenden Lösungen eines einzigen Anbieters schützen. Die Zusammenarbeit mit mehreren Anbietern verursacht Komplexität, die sich letztlich als kostspielig erweisen kann – und zwar in mehr als einer Hinsicht. Die IBM Power-Technologie unterstützt die End-to-End-Verschlüsselung auf Prozessorebene, ohne dass die Leistung beeinträchtigt wird. Die Integration Ihrer Infrastruktur nimmt jede Schicht des Stacks in den Fokus.

Sicherheit von einem einzigen Anbieter kann natürliche Vorteile bieten, die Ihre Sicherheitsstrategie vereinfachen und stärken. Aufbauend auf drei Jahrzehnten Führungsposition in der IT-Sicherheit umfasst die Technologie von IBM Power auch umfangreiche Partnerschaften mit anderen Unternehmen innerhalb und außerhalb von IBM, die die Sicherheitsexpertise des Unternehmens noch weiter vertiefen und erweitern. Durch diese Partnerschaften kann die Technologie von IBM Power auf eine noch größere Community von Sicherheitsfachleuten zugreifen und sicherstellen, dass aufkommende Fragen schnell erkannt und mit Verlässlichkeit angegangen werden. Mit der Unterstützung der Geschäftsbereiche IBM Security® und IBM Research® sowie des PowerSC 2.0-Portfolios können Power10-Server vielfältige Bedrohungen, einschließlich Insiderangriffen, von Grund auf abwehren.

Vereinbaren Sie ein Beratungsgespräch, um das Potenzial von IBM Power-Lösungen kennenzulernen

Kontakt →

Anmerkungen

1. Cost of a Data Breach Report 2021, IBM Security, Juli 2021 (PDF, 3,6 MB)
2. Die dreifache Leistung basiert auf einer Pre-Silicon-Analyse von Integer-, Enterprise- und Floating-Point-Umgebungen auf einem Power10 Dual-Socket-Server mit 2 x 30-Kern-Modulen, die mit den Tests auf einem POWER9 Dual-Socket-Server verglichen wurden, der mit 2 x 12-Kern-Modulen ausgestattet ist. Beide Module haben das gleiche Energieniveau. 2 Die 10- bis 20-fache Verbesserung des KI-Inferencing basiert auf einer Pre-Silicon-Analyse verschiedener Workloads (Linpack. Resnet-50 FP32, Resnet-50 BFloat16 und Resnet-50 INT8) auf einem POWER10 Dual-Socket-Server mit 2 x 30-Kern-Modulen im Vergleich mit einem POWER9 Dual-Socket-Server mit 2 x 12-Kern-Modulen.
3. AES-256 in GCM- und XTS-Modi laufen im Vergleich mit IBM Power10 E1080 (15-Kern-Module) etwa 2,5-mal schneller pro Kern verglichen mit IBM POWER9 E980 (12-Kern-Module) nach vorläufigen Messwerten, die auf RHEL Linux 8.4 und der OpenSSL 1.1.1g-Bibliothek abgerufen wurden.

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

USA
Hergestellt in den Vereinigten Staaten von Amerika.
Juni 2022