Hewlett Packard Enterprise

Schutz, Erkennung, Wiederherstellung

HPE ProLiant Gen10 und AMD EPYC Technologie für sichere Virtualisierung

Bestandteil des Portfolios der weltweit sichersten Server nach Industriestandard[1]

1,9 Milliarden

Rekorde in 6 Monaten gebrochen[2]

15 x

Anstieg der Ransomware-Angriffe[3]

6 Billionen $

erwartete Kosten der Cyber-Kriminalität im Jahr 2021[4]

Sind Sie geschützt?

Virtualisierung bleibt das wichtigste Verfahren zur Maximierung der Agilität und Effizienz in einer Hybridumgebung. Im Jahr 2016 waren 26 % der Workloads virtualisiert und die Führungskräfte in Unternehmen waren nicht abgeneigt, mehr als 80 % ihrer Workloads zu virtualisieren.[5] Die Servervirtualisierung war das am häufigsten geplante Infrastrukturprojekt.[6] Gemäß den Prognosen von Analysten werden im Jahr 2020 41 % der neu ausgelieferten Server virtualisiert sein, gegenüber 33 % im Jahr 2015.[7] Und das ist alles andere als erstaunlich – Unternehmen erzielen durch Servervirtualisierung Einsparungen in Höhe von fast 20 %.[8]

Bei einem ansteigenden Virtualisierungsgrad im Rechenzentrum sollten Server Ihre stärkste Verteidigungslinie sein, die die neuesten Innovationen bereitstellt, um Sicherheitsangriffe zu verhindern und zu erkennen sowie die Systeme nach Angriffen wiederherzustellen. Aus diesem Grund haben wir einzigartige Sicherheitstechnologien entwickelt, die Ihnen eine neue Sicherheitsgrundlage für den Schutz Ihrer Daten – und Ihres Unternehmens – bieten.

HPE ProLiant DL325 Gen10 und HPE ProLiant DL385 Gen10 Server sind für Virtualisierung konzipiert und umfassen Sicherheitsmerkmale, die dazu beitragen, Ihre Hardware, Firmware und Ihr Netzwerk vor unberechtigtem Zugriff und Missbrauch zu schützen. HPE hat außerdem eine Vielzahl integrierter und optionaler Software und Firmware im Angebot, sodass Sie die richtige Mischung aus Remote-Zugriff und Kontrolle für Ihr Netzwerk und Rechenzentrum auswählen können.

HPE ProLiant DL325 Gen10 und HPE ProLiant DL385 Gen10 Server mit AMD EPYC™ Prozessoren stellen erweiterte, zuverlässige Sicherheitsmerkmale bereit und bilden eine herausragende, sichere Serverlösung für die Virtualisierung.

[1] Basierend auf Penetrationstests zur Cyber-Sicherheit für eine Reihe von Serverprodukten verschiedener Hersteller, die durch ein externes Unternehmen im Mai 2017 durchgeführt wurden.

[2] CNBC, „**The number of devastating cyberattacks is surging—and it's likely to get much worse**", September 2017.

[3, 4] Forbes, „**Hewlett Packard Enterprise Releases iLO Amplifier Pack With Server System Restore**", Februar 2018.

[5, 6] IDC, „**Market Trends in Virtualization Infrastructure and Software, 2016: Market Survey Report**", Dezember 2016.

[7] TechTarget, „IT Priorities 2017", Februar 2017.

[8] Funktion mit einer HPE iLO Advanced Premium Security Edition Lizenz.

Gemäß FIPS 140–2 Level 1 validiert
HPE ProLiant DL325 Gen10 und HPE ProLiant DL385 Gen10 Server mit HPE iLO 5 nutzen einen intelligenten Mikroprozessor, sicheren Speicher und eine dedizierte Netzwerkschnittstelle und werden damit in einem Modus betrieben, der die Anforderungen von FIPS 140–2 Level 1 erfüllt.

Weitere Informationen zu HPE Sicherheitsmerkmalen

- **HPE Secure Compute Lifecycle Whitepaper**
- **HPE Gen10 Security Reference Guide**
- **Demystifying Server Root of Trust – Moor Insights & Strategy Whitepaper**

[9] Interne HPE Tests, Februar 2017

Unser Lösungspartner

AMD

Sie haben Fragen zum Kauf? Klicken Sie hier, um mit unseren Presales-Experten zu chatten.

Jetzt teilen

Updates abrufen

Schutz

HPE Silicon Root of Trust
HPE ist der einzige Hersteller, der die Silicon Root of Trust bereitstellt. Diese verankert grundlegende Firmware im angepassten HPE iLO 5 Chip. So wird ein unveränderbarer Fingerabdruck erstellt, mit dem sichergestellt werden kann, dass der Firmware-Code gültig und nicht manipuliert ist. Zudem wird verhindert, dass der Server mit manipulierter Firmware bootet.

Secure Boot
Secure Boot ist eine Sicherheitsfunktion nach Industriestandard, die im BIOS implementiert ist. Secure Boot sorgt dafür, dass die beim Bootprozess gestarteten Treiber und der Bootloader für das Betriebssystem digital signiert sind und mit einer Gruppe vertrauenswürdiger Zertifikate verglichen werden, die das BIOS sicher speichert. Wenn Secure Boot aktiviert ist, werden nur validierte Treiber und Bootloader des Betriebssystems ausgeführt.

AMD Secure Processor
Im AMD EPYC-System ist en dedizierter AMD Secure Processor in einen Chip integriert. Er verwaltet Secure Boot, ist auf der Firmware-Ebene mit der HPE Silicon Root of Trust verbunden und validiert das HPE BIOS während des Bootprozesses. AMD Secure Memory Encryption (SME) unterstützt die Inline-Verschlüsselung und -Entschlüsselung mit sicherer Schlüsselgenerierung und -verwaltung – und minimaler Beeinträchtigung der Leistung. Mit AMD Secure Encrypted Virtualization kann der Speicherinhalt einer virtuellen Maschine (VM) mit einer Verschlüsselungs-Engine mit hoher Leistung transparent verschlüsselt werden. Die Engine kann mit mehreren Schlüsseln für die verschiedenen VMs im System programmiert werden.

Sichere Lieferkette
HPE verringert das Risiko für Bedrohungen der Lieferkette – z. B. durch gefälschte Materialien, böswillige Software und andere nicht vertrauenswürdige Komponenten – indem wir die Komponentenanbieter sorgfältig überprüfen und Komponenten nur aus Ländern beschaffen, die im Trade Agreement Act (TAA) aufgeführt sind. HPE reduziert Sicherheitsprobleme und Bedrohungen durch die interne Entwicklung des BIOS, der Management-Firmware und des iLO 5 Chips noch weiter. Sichere Serveroptionen wie das Angriffserkennungs-Kit für das Chassis können das Risiko für Manipulationen noch weiter verringern – selbst wenn der Server ausgeschaltet ist.

Ermitteln

Firmware-Überprüfung zur Laufzeit
Schutz zur Laufzeit des Servers wird durch eine exklusive HPE Technologie bereitgestellt, die tägliche Überprüfungen der grundlegenden Server-Firmware ausführen kann. Wird in die kritische Firmware manipulierter Code oder Malware eingeführt, wird ein Warnhinweis in einem HPE iLO-Prüfprotokoll erstellt, um Sie über die Manipulation zu informieren. Diese Funktionalität wird durch die exklusive HPE Silicon Root of Trust ermöglicht.

Wiederherstellung

Automatische Wiederherstellung der grundlegenden Firmware
Im Fall einer Sicherheitsverletzung bei der Firmware – die aufgrund der erweiterten Sicherheitsfunktionen, die in ProLiant Gen10 Server integriert wurden, unwahrscheinlich ist – können Sie sicher und automatisch einen bekannten, einwandfreien vorherigen Status der Firmware wiederherstellen.[9]

Serverwiederherstellung in großen Umgebungen
Die exklusive Systemwiederherstellungsfunktion für **HPE Server** nutzt **HPE iLO** Amplifier Pack Software, um bis zu 10.000 Server mit einem einzigen Mausklick wiederherzustellen. Bei einem Ransomware-Angriff oder einem anderen Sicherheitsverstoß können Sie die grundlegende Firmware, die Konfigurationseinstellungen für die Firmware, das Betriebssystem und die Hostumgebungen eines Servers manuell oder automatisch in einen betriebsbereiten Zustand zurücksetzen.

HPE Innovationen

HPE ProLiant DL325 Gen10 und HPE ProLiant DL385 Gen10 Server vereinen in Kombination mit AMD EPYC Prozessoren die allerneuesten Innovationen in Sachen Sicherheit und Leistung. Die erweiterten Funktionen von iLO 5 bieten sicheren Boot, tägliche Überprüfungen der Firmware und automatische Wiederherstellung der letzten bekannten einwandfreien Konfiguration.

Erfahren Sie noch heute mehr

Warten Sie nicht mit dem Schutz Ihrer Server vor Cyber-Kriminellen. Wenden Sie sich noch heute an Ihren HPE Ansprechpartner oder autorisierten Channel Partner, um weitere Informationen zu erhalten.

Weitere Informationen unter
hpe.com/servers/dl385
hpe.com/servers/dl325

a00049646DEE, Apr. 2019, Rev. 1