ActualTech Media

Hewlett Packard Enterprise

HPE bietet integrierte Sicherheit für KMU

Ed Tittel

INHALT

THEMA

HPE bietet integrierte Sicherheit, die sich von der Chipebene bis zur Server-Lieferkette erstreckt, um den gesamten IT-Lebenszyklus zu schützen. Diese technische Kurzübersicht zeigt, wie HPE sich mit verschiedenen Mechanismen direkt und explizit um die Sicherheit kümmert.

Sicherheit spielt in alle Aspekte des IT-Betriebs im gesamten Unternehmen hinein. Aus diesem Grund ist Sicherheit nicht nur für Systemhardware und -software wichtig, sondern auch für die Personen, die damit arbeiten. Aufbau und Pflege eines sicheren Umfelds gelingt Unternehmen am besten, die sich für einen Anbieter entscheiden, der weiß, dass Sicherheit für Systeme und Software konzipiert, von Anfang an darin integriert und im Rahmen eines umfassenden Lifecylce-Prozesses erhalten werden muss. HPE bietet durchgängige Sicherheitsabdeckung für das gesamte Unternehmen, für alle Systeme und alle Benutzer.

Bedeutung der Sicherheit im Jahr 2021

Eine gute allgemeine Definition von Cybersicherheit ist eine Struktur von Technologien, Prozessen und Verfahren, die zum Schutz digitaler Systeme und Assets – einschließlich Netzwerken, Geräten, Software und Daten – vor Angriffen, Schäden oder Verlust sowie vor unbefugtem Zugriff konzipiert und eingeführt werden. Daher ist Sicherheit von Natur aus allumfassend und deckt Systeme, Kommunikation, Programme, Daten und Verbindungen ab. Vertrauliche Daten erfordern besondere Aufmerksamkeit und besonderen Schutz, ganz gleich, ob es sich um geistiges Eigentum, Finanzdaten, personenbezogene Daten, Patientenakten oder sonstige Arten von Daten handelt. Wenn diese in die falschen Hände geraten, kann dies negative Auswirkungen sowohl für das Unternehmen, das diese Daten speichert, als auch für die Partei, auf die sich die Daten beziehen oder der die Daten gehören, haben.

Sicherheit wird häufig für bestimmte Schwerpunkte oder Anliegen angewendet und umfasst in der Regel Folgendes:

- **Serversicherheit:** Die Tools, Technologien, Einstellungen, Firmware und Software (innerhalb und außerhalb des Serverbetriebssystems), die Sicherheit für Netzwerkserver eines Unternehmens definieren und bereitstellen. Dies umfasst häufig den Zugriff auf Sicherheitselemente der Infrastruktur und Server-Firmware sowie eigenständige und Betriebssystem-Softwarekomponenten.
- **Clientsicherheit:** Die Tools, Technologien, Einstellungen, Firmware und Software (innerhalb und außerhalb des Clientbetriebssystems), die Sicherheit für Netzwerkclients, die zum Netzwerk eines Unternehmens gehören oder damit verbunden sind, definieren und bereitstellen. Dies wird häufig mit Endpunktsicherheit gleichgesetzt, da Clients in den meisten Unternehmen den Großteil der Endpunkte ausmachen. In der Regel sind Komponenten für Bedrohungserkennung und -vermeidung wie Anti-Malware, Patch- und Update-Management etc. integriert. Außerdem besteht lokale und (falls zutreffend) ferne Interaktion mit Infrastruktursicherheitselementen.
- **Netzwerksicherheit:** Die Tools, Technologien, Geräte und Software, die auf Netzwerkgeräten ausgeführt werden oder diese überwachen und verwalten (physisch und virtuell). Dies umfasst im Allgemeinen die Überprüfung und Filterung von Netzwerkverkehr, insbesondere an den Netzwerkgrenzen zur Kontrolle von ein- und ausgehendem Datenverkehr. Es können auch Infrastruktursicherheitselemente per Hosting bereitgestellt werden, häufig in Form von Software Defined Networking (SDN) für Local oder Wide Area Network-Komponenten und -Services (SD-WAN).
- **Cloud-Sicherheit:** Die Tools, Technologien und Software, die in der Cloud ausgeführt werden oder Cloud-Zugriff und -Nutzung, Einrichtung und Bereitstellung, Abbau und Außerbetriebnahme sowie Datenverkehr/Aktivitäten in der Cloud überwachen und verwalten. Cloud-Sicherheit soll die zugrunde liegende physische Infrastruktur schützen, kann aber auch auf in der Cloud ausgeführte virtuelle Infrastrukturen und Services sowie in der Cloud verwendete Daten erweitert werden.
- **Infrastruktursicherheit:** Die Tools, Technologien und Software, die für Überwachung und Management aller Komponenten der Netzwerke und Infrastruktur eines Unternehmens, einschließlich Client-, Server- und Netzwerkgeräten, sowie aller Cloud-Komponenten und -Services, die für das Unternehmen zugänglich sind, verwendet werden. Infrastruktursicherheit bietet eine umfassende Übersicht ganzer Infrastrukturen über Dashboards, Automatisierung und andere Tools, die verwendet werden, um die darin enthaltenen Elemente und Komponenten anzuzeigen, zu verwalten und zu kontrollieren.

> **HPE kann kleine Unternehmen dabei unterstützen, diesen Schwerpunkten und Anliegen im Sicherheitsbereich gerecht zu werden, und sicherstellen, dass ihre Strategien für Risikomanagement mit ihren Geschäftszielen im Einklang sind.**

Interessanterweise schließt Cybersicherheit all diese verschiedenen Schwerpunkte und Anliegen ein. Sie umfasst Software, Hardware und Firmware auf Clients, Servern und Netzwerken, die direkt von einem Unternehmen kontrolliert werden. Sie umfasst auch Cloud-basierte Komponenten, die oft von einem Dritten kontrolliert werden (häufig ein Cloud-Plattform-, Service- oder Software-as-a-Service-Provider [SaaS], der eine Public oder Private Cloud ausführt).

> **Silicon Root of Trust verhindert die Ausführung von manipuliertem Firmware-Code.**

Services für Risikomanagement spielen auch in die Cybersicherheit hinein, da sie mit Abwehr- oder Schutzmaßnahmen Risikoquellen reduzieren oder beseitigen sollen, die sich negativ auf Einnahmen, Geschäftstätigkeit oder Ruf eines Unternehmens auswirken können. Digitale Abwehrmaßnahmen müssen priorisiert und verwaltet werden, um die möglichen negativen Auswirkungen von Bedrohungen auszugleichen (auf kleine oder geringe Risiken erfolgt eine entsprechend reduzierte oder gar keine Reaktion, wohingegen große oder wesentliche Risiken entsprechend umfassende und umfangreiche Reaktionen bewirken). HPE kann kleine Unternehmen dabei unterstützen, diesen Schwerpunkten und Anliegen im Sicherheitsbereich gerecht zu werden, und sicherstellen, dass ihre Strategien für Risikomanagement mit ihren Geschäftszielen im Einklang sind. In den folgenden Abschnitten werden spezifische HPE Technologien erläutert, die verwendet werden, um bestimmte Sicherheitsrisiken auszugleichen, insbesondere für HPE Server und deren Clients.

Silicon Root of Trust

Silicon Root of Trust wurde konzipiert, um Schutz vor spezifischen, gezielten Firmware- und BIOS-Angriffen zu bieten. Die Lösung funktioniert bei HPE ProLiant Servern und stellt eine Verbindung zwischen der angepassten HPE Silicon Lösung auf diesen Servern und deren Integrated Lights Out (iLO) Firmware her. Im Wesentlichen verhindert Silicon Root of Trust die Ausführung von manipuliertem Firmware-Code. Dies erfolgt mittels Integritätsprüfungen im Firmware-Code bevor er ausgeführt werden darf, unter Verwendung spezieller, schreibgeschützter Prüfsummen und Vergleichstools, die für das Betriebssystem oder Programme, die auf dem Betriebssystem ausgeführt werden, nicht direkt zugänglich sind.

Sobald ein Hinweis auf Manipulationen oder Veränderungen erkannt wird, bereinigt die HPE iLO Firmware den potenziell (oder tatsächlich) manipulierten Firmware-Code. Es wird ein gültiges, bekanntermaßen richtiges Firmware-Image aus einer vertrauenswürdigen Quelle verwendet, um den gefundenen Code zu ersetzen. Dann wird diese bekannte, einwandfrei funktionierende Kopie automatisch ausgeführt. HPE iLO integriert Verschlüsselungsfunktionen in die Tools für die Erkennung von Sicherheitsverletzungen, damit nur sicherer Firmware-Code ausgeführt werden kann. Falls der Server diesen sicheren Firmware-Code nicht beschaffen oder ausführen kann, wird er heruntergefahren, bevor möglicherweise manipulierte Firmware ausgeführt wird. Damit wird sichergestellt, dass HPE ProLiant Server vor Rootkit- und sonstigen Pre-Boot-Angriffsmethoden und -vektoren geschützt sind.

HPE Pointnext Security Services

HPE Pointnext Services ist die Support, Advisory, Professional und Education Services-Organisation von HPE. HPE Experten unterstützen HPE Kunden bei Herausforderungen in den Bereichen Sicherheits- und Risikomanagement bei der digitalen Transformation und beim IT-Betrieb von Edge bis Cloud. HPE unterstützt KMU gerne dabei, ihre Mitarbeiter entsprechend vorzubereiten und mit Sicherheitsschulungen und -zertifizierungen weiterzubilden. Digital Learner Abonnements fassen technische Schulungen von HPE zur Nutzung durch Teams in KMU zusammen und kombinieren den Nutzen von HPE Schulungen – zu einem günstigeren Preis.

Trusted Platform Module (TPM)

TPM wird in Form eines Computer-Chips (Mikrocontroller) bereitgestellt, der Artefakte für die Authentifizierung einer Laufzeitplattform, einschließlich Servern und Client-PCs (Laptops, Tablets, All-in-One-Systeme etc.), sicher speichert. Seit Januar 2021 fordert Microsoft, dass alle neuen Windows Server-Plattformen über TPM Version 2.0 mit standardmäßig aktivierter Secure Boot-Option verfügen, und empfiehlt, dass alle Server zudem BitLocker-Verschlüsselung verwenden, um zusätzlichen Schutz vor potenziellen „Rootkit"-Malware-Angriffen zu bieten. HPE unterstützt TPM seitdem es 2009 ISO/IEC-Standard (11990) wurde. Heute werden alle verfügbaren modernen HPE ProLiant Server und PCs von HP Inc. diesen Anforderungen gerecht oder übertreffen diese sogar.

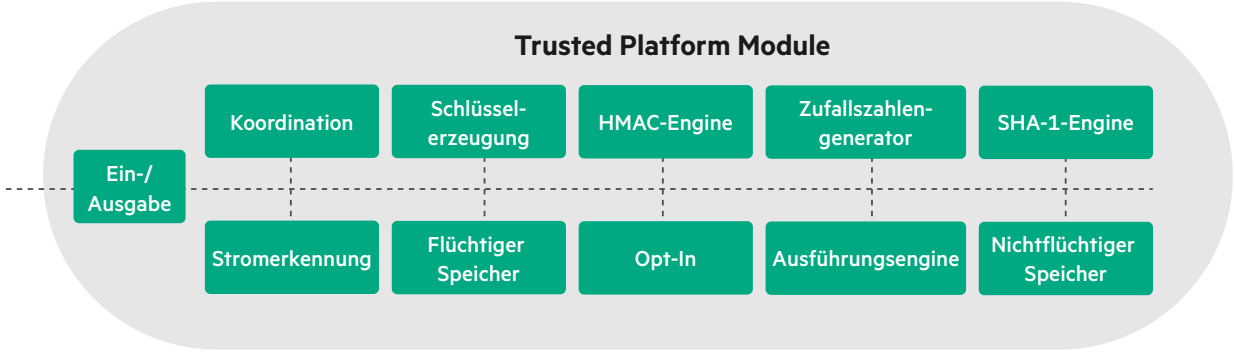

Abbildung 1: Trusted Platform Module bietet geschützte, chipbasierte Speicher-, Verarbeitungs- und Verschlüsselungstools zur Verwendung beim Systemstart

Wie in **Abbildung 1** dargestellt, bietet TPM eine geschützte Umgebung, in der sichere Anmeldedaten wie Schlüssel, Zertifikate, Kennwörter etc. außerhalb der normalen Verarbeitungsumgebung von Geräten sicher generiert, gespeichert und verwendet werden können. TPM ist so konzipiert, dass es sehr manipulationssicher ist und hohen Schutz sowie Sicherheit auf Basis von Silicon Root of Trust bietet, um Rootkit-, Firmware- und sonstige Pre-Boot-Angriffsvektoren abzuwehren.

Auf einem PC (Server oder Client) bietet TPM sicheren Speicher für administrativen Zugriff und BIOS-Updates. Es unterstützt zudem Verschlüsselung auf Laufwerksebene (z. B. Microsoft BitLocker), Biometriedaten (z. B. Microsoft Windows Hello Gesichtserkennung oder Fingerabdruckdaten) und die Secure Boot-Funktion von Microsoft. Auf diese Weise aktiviert und unterstützt TPM hardwarebasierten Low-Level-Schutz vor Low-Level-Angriffen. Microsoft arbeitet mit allen großen Chipherstellern (AMD, Intel und Qualcomm) zusammen, um eine angemessene Integration von TPM-Funktionalität auf CPU-Ebene sicherzustellen. Moderne Server von HPE und Client-PCs von HP Inc. unterstützen mindestens TPM 2.0 und bieten leistungsfähige, geschützte Silicon Root of Trust-Funktionalität für Benutzer und Unternehmen.

> **Moderne Server von HPE und Client-PCs von HP Inc. unterstützen mindestens TPM 2.0 und bieten leistungsfähige, geschützte Silicon Root of Trust-Funktionalität für Benutzer und Unternehmen.**

HPE Trusted Supply Chain

Für Kunden mit überdurchschnittlich hohen Sicherheitsanforderungen und Einsatzszenarien mit hoher Sicherheit betreibt HPE eine Trusted Supply Chain. Benutzer dieser Supply Chain sind unter anderem Kunden aus dem öffentlichen Sektor und der US-Regierung, die ausschließlich Produkte aus den USA mit nachweisbarer Cybersicherheit erwerben dürfen. Käufer außerhalb der USA können über diese Trusted Supply Chain weltweit einkaufen (ausgenommen China, Taiwan und Indien). Sicherheit wird auf zwei spezifische Arten direkt in diese Trusted Supply Chain integriert. Erstens durch Aufnahme zusätzlicher verstärkter Sicherheitsfunktionen in Produkte selbst. Zweitens durch Überwachung durch HPE Mitarbeiter, die diese Produkte während des Fertigungsprozesses beaufsichtigen. HPE Mitarbeiter prüfen alle Teile, beobachten die Montage und stellen sicher, dass verpackte Geräte bis zur Annahme der Lieferung durch den Kunden manipulationssicher bleiben.

Darüber hinaus bietet HPE ein exklusives Silicon Root of Trust-Konzept, bei dem Sicherheit auf Chipebene in Industriestandard-Server eingebettet wird, und unterhält Sicherheitskontrollen in der gesamten Lieferkette, um strikte Sicherheit auf Hardware-Ebene zu etablieren und zu erhalten. Zu den Absicherungsverfahren von HPE gehören unter anderem UEFI Secure Boot, eine verkleinerte Angriffsfläche, Manipulationssicherheit auf Chipebene, integrierte Warnhinweise in Systemen und physische Sperren.

Auf der Seite mit HPE Sicherheitslösungen erfahren Sie mehr über die integrierte, durchgängige Sicherheit von HPE im Rahmen der Funktionalität von Silicon Root of Trust, TPM, Trusted Supply Chain etc.