DELL Technologies

Lösungsübersicht

Anpassung von UEFI Secure Boot für Dell EMC PowerEdge

Bei den Serverumgebungen in Rechenzentren lag der Schwerpunkt der Sicherheitsbemühungen herkömmlich auf der Betriebssystem-, Anwendungs- und Netzwerkebene. Angesichts der weiterhin zunehmenden Sicherheitsbedenken rund um die Hardwareinfrastruktur wächst auch die Komplexität für IT-Sicherheitsadministratoren. Daher müssen Server- und Sicherheits-IT-Teams eine vertrauenswürdige Computing-Grundlage schaffen und dieses Vertrauen auf die Betriebssysteme und Anwendungen ausdehnen. Die üblicherweise für die sichersten und sensibelsten Anwendungen und Datenvolumen reservierte kundenspezifische Infrastruktursicherheit gerät zunehmend ins Blickfeld. Die sich ständig weiterentwickelnde Bedrohung der Serverhardware erfordert einen umfassenderen Ansatz, einschließlich der Anpassung von UEFI Secure Boot, um diese vertrauenswürdige Grundlage zu stärken.

Das beginnt mit der cybersicheren Architektur von Dell EMC, die das BIOS und die Firmware für den Integrated Dell Remote Access Controller (iDRAC) validiert, bevor dieser geladen wird. Die Firmware für andere kritische Komponenten wird ebenfalls mithilfe von gespeicherten kryptografischen Zertifikaten validiert, um sicherzustellen, dass authentische Firmware auf dem Server ausgeführt wird.

Cybersichere Architektur von Dell EMC

Effektiver Schutz

- Chipbasierte Sicherheit für Hardware
- Signierte Firmwareupdates
- Systemsperre
- Sichere Standardkennwörter

Zuverlässige Erkennung

- Erkennung von Konfigurations- und Firmwareabweichungen
- Persistente Ereignisprotokollierung einschließlich Nutzeraktivität
- Sichere Warnmeldung

Schnelle Recovery

- Automatische BIOS-Recovery
- Schnelle OS-Recovery
- System Erase

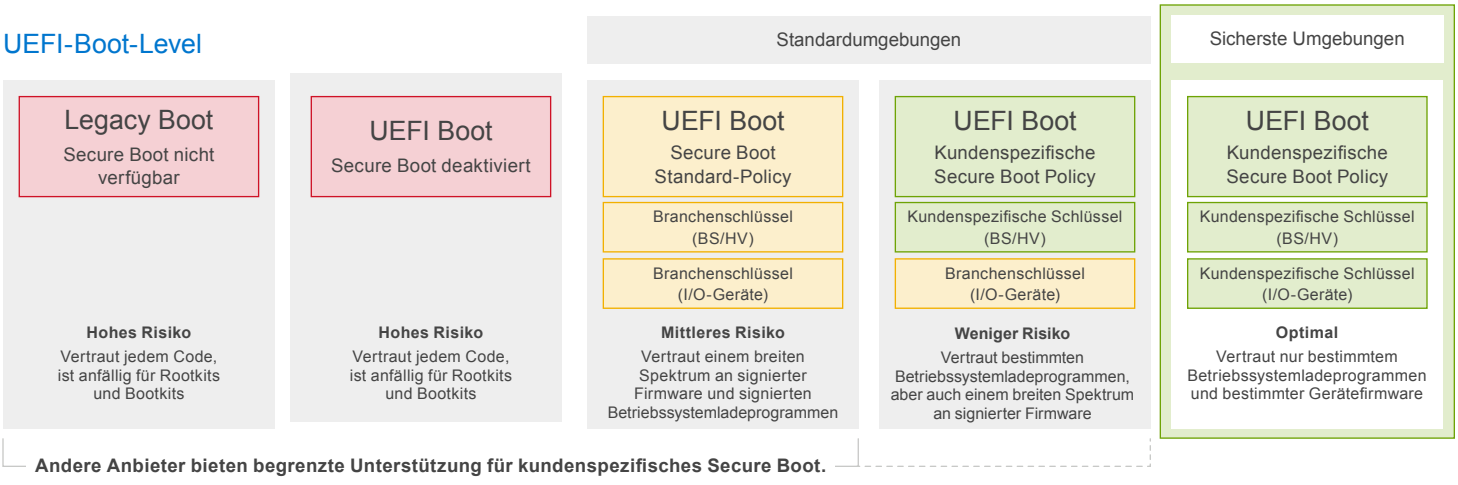
Als moderner Ersatz für die Legacy-BIOS-Konfiguration und -Startsteuerung initialisiert UEFI Secure Boot die Baseline-Funktionen des Servers, bevor ein Hypervisor oder Betriebssystem gestartet wird. PowerEdge-Server verwenden UEFI Secure Boot, um die kryptografisch erzeugten Zertifikate der UEFI-Treiber und Betriebssystembootloader zu prüfen. Dies sind die „Schlüssel“, mit denen der Server Folgendes validieren kann:

- UEFI-Treiber, die von PCIe-Karten geladen werden
- UEFI-Treiber und ausführbare Dateien, die von Massenspeichergeräten geladen werden
- Betriebssystembootloader – in der Regel Linux oder Microsoft Windows

Dieser Validierungsprozess ist von entscheidender Bedeutung, um den Server vor dem Starten des Betriebssystems vor einer Initiierung von nicht autorisiertem Code zu schützen. Durch die Prüfung der Signatur des Bootloaders, des Kernels und des anderen Userspace-Codes ist die UEFI-Firmwarevalidierung darauf ausgelegt, die Ausführung von nicht signierter Software auf dem System zu verhindern.

Die Anpassung von UEFI Secure Boot für Dell EMC PowerEdge bietet außerdem die einzigartige Funktion, kundenspezifische Zertifikate zu unterstützen, die von einer anderen Zertifizierungsstelle als Microsoft erstellt und signiert wurden. Microsoft ist die Standardzertifizierungsstelle für UEFI-unterstützte Geräte und Betriebssysteme. Viele Standard-Linux-Distributionen haben ein Microsoft-Zertifikat implementiert. In Situationen, in denen eine nicht standardmäßige Linux-Umgebung verwendet wird (d. h. proprietäre Kernel- oder Treibermodifikationen), müssen vom Nutzer kryptografisch signierte kundenspezifische Zertifikate erstellt werden, um den Bootloader selbst zu validieren und die Vertrauenskette zwischen Hardware und Software aufrechtzuerhalten.

UEFI-Boot-Level



Erweiterung der Serversicherheit ohne Kompromisse

Der Startprozess ist die Grundlage der Sicherheit für jedes Gerät. Er basiert auf einer Fülle an Firmware, die steuert, wie die Komponenten und Peripheriegeräte eines Geräts initiiert werden, und lädt das Betriebssystem. Je früher Code geladen wird, umso privilegierter ist er und umso mehr Schaden kann er anrichten, wenn er nicht zuerst authentifiziert wird. Wenn der Startprozess gefährdet ist, können Angreifer Sicherheitskontrollen unterlaufen und damit unbefugten Zugriff auf verschiedene Teile des Systems erlangen. Es könnte sogar möglich sein, Ransomware mit bösartigen UEFI-Bootloadern zu erstellen, um die Kontrolle über Server beim Hochfahren zu übernehmen, den Computer neu zu konfigurieren, Daten zu verschlüsseln und Chaos zu verursachen.

Weniger Risiken

Mit modernen Steuerungs- und Konfigurationsoptionen sind Sie besser denn je dazu gerüstet, Ihre Server vor Firmware- oder Bootloaderangriffen zu schützen. Die Anpassung von UEFI Secure Boot für Dell EMC PowerEdge erhöht die Sicherheit Ihrer Serverinfrastruktur und lässt gleichzeitig BIOS-basierte Legacy-Startmethoden hinter sich. Eine aktuelle Empfehlung der National Security Agency (NSA) der US-Regierung dokumentiert das Thema der erhöhten Serverhardwaresicherheit und nennt dabei ausdrücklich die Nutzung der Anpassung von UEFI Secure Boot für PowerEdge als eine Methode, die ein deutlich höheres Level an Sicherheit sowie die Flexibilität zur Unterstützung mehrerer Betriebssysteme bietet. In einem damit zusammenhängenden technischen Bericht zu Cybersicherheit der NSA wird erwähnt, dass der „Systemeigentümer mit dem kundenspezifischen Modus die Auswahl vertrauenswürdiger Hardware- und Softwarelösungen eingrenzen oder erweitern kann“. Zudem wird erläutert, wie dies mit dem eingebetteten UEFI-Konfigurationsdienstprogramm von Dell[1] erreicht werden kann. Mit dieser fein abgestimmten Steuerung kann die Bedrohung durch Fehlkonfigurationen, Manipulation und Malware reduziert oder eliminiert werden. Systemadministratoren können schneller auf neue Startbedrohungen reagieren und sind vor potenziellen Zertifikatsignaturfehlern durch Anbieter geschützt.

Funktionen von UEFI Secure Boot mit kundenspezifischen Zertifikaten

Leistungsmerkmale	Beschreibung	Vorteile
Secure Boot	• Validierung von Kernkomponenten und Firmware	• Einführung einer modernen Firmwarevalidierung ohne die Einschränkungen und Sicherheitsbedrohungen des Legacy-BIOS
Selbstsignierte Zertifikate	• Aufrechterhaltung einer sicheren Firmware-, Bootloader- und Betriebssysteminitiierung für den gesamten Serverbetrieb	• Unterstützung für kundenspezifische BS-Builds in hochgradig sicheren Bereitstellungen • Unabhängigkeit von der standardmäßigen Signaturzertifizierungsstelle bei der Implementierung kundenspezifischer Hardware und zugehöriger Firmware
Compliance mit Sicherheitsrichtlinien	• Ausrichtung an Sicherheitsstandards für den Serverstartprozess, die Firmwarevalidierung und das kundenspezifische Zertifikatmanagement	• Festlegung des Standards für Serverhardware- und Firmwaresicherheit • Positionierung des Serverbetriebs für die Compliance mit zukünftigen Serversicherheitsrichtlinien in sensiblen Umgebungen
Integration in iDRAC und TPM	• Nutzung vorhandener Hardware- und Firmwaresicherheitsfunktionen, die bereits in PowerEdge-Server integriert sind	• Maximierung des Werts integrierter Sicherheitsfunktionen zum Aufbau einer umfassenden chipbasierten Sicherheit

[1] Wie bei den meisten Systemeinstellungen nutzt ein Administrator möglicherweise neben dem Systemsetup auch andere Tools für die Aktivierung der Secure Boot-Standard-Policy. Die Secure Boot-Standard-Policy kann über das Dell Deployment Toolkit™ (DTK), den Lifecycle Controller™, OpenManage™-Tools, die RACADM-Konsole und WS-MAN-Konsolen aktiviert werden.

Erfahren Sie mehr über PowerEdge-Server.

Erfahren Sie mehr über Dell EMC OpenManage Enterprise

Weitere Informationen zu unseren Systemmanagementlösungen

Durchsuchen Sie unsere Ressourcenbibliothek

Folgen Sie PowerEdge-Server auf Twitter

Wenden Sie sich an einen Dell Technologies Experten für Vertrieb oder Support