DELL Technologies

Whitepaper

Technisches Whitepaper: Cybersicherheit ohne Ausfallrisiko für Dell EMC PowerEdge-Server

Dezember 2020

Versionen

Datum	Beschreibung
Januar 2018	Erstveröffentlichung
November 2020	Revised Version

Inhaltsverzeichnis

Inhaltsverzeichnis

Zusammenfassung

Der Dell Technologies Ansatz für Sicherheit ist intrinsisch: Sicherheit ist integriert – nicht nachträglich „eingebaut“ – und wird über den Secure Development Lifecycle von Dell in jeden Schritt berücksichtigt. Wir arbeiten stetig daran, unsere Sicherheitskontrollen, -funktionen und -lösungen für den PowerEdge kontinuierlich weiterzuentwickeln, um der ständig wachsenden Bedrohungslandschaft gerecht zu werden. Und wir verankern Sicherheit weiterhin mit einer Silicon Root of Trust. In diesem Whitepaper werden die Sicherheitsfunktionen beschrieben, die in die cybersichere Plattform für den PowerEdge integriert sind. Viele davon werden über den Dell Remote Access Controller (iDRAC9) aktiviert. Es gibt zahlreiche neue Funktionen, die seit dem vorherigen Whitepaper für PowerEdge-Sicherheit hinzugefügt wurden. Sie reichen von der Zugriffskontrolle über die Datenverschlüsselung bis zur Lieferkettensicherheit. Dazu zählen: Live-BIOS-Scanning, UEFI Secure Boot Customization, RSA SecurID MFA, Secure Enterprise Key Management (SEKM), Secured Component Verification (SCV), verbesserte SystemErase-Funktion, automatische Zertifikatregistrierung und -verlängerung, Cipher Select und CNSA-Support. Alle Funktionen nutzen Intelligenz und Automatisierung, um Sie vor Bedrohungen zu schützen und die Skalierung zu ermöglichen, die von ständig wachsenden Nutzungsmodellen verlangt wird.

1. Einführung

Die Bedrohungslandschaft entwickelt sich weiter und die IT- und Sicherheitsexperten haben Probleme, die Risiken für ihre Daten und Ressourcen zu managen. Daten werden auf zahlreichen Geräten, On-Premise sowie in der Cloud verwendet und nach wie vor finden Datenschutzverletzungen mit negativen Folgen statt. In der Vergangenheit wurde der Sicherheitsschwerpunkt auf Betriebssysteme, Anwendungen, Firewalls sowie IPS- und IDS-Systeme gelegt. Diese Bereiche sind auch weiterhin wichtig. Aber angesichts der Ereignisse in den letzten ein bis zwei Jahren, in denen Hardwarebedrohungen aufgetreten sind, ist der Schutz von hardwarebasierten Infrastrukturen wie Firmware, BIOS, BMC sowie anderer Hardwareschutz (z. B. die Lieferkettensicherheit) ebenfalls notwendig geworden.

Laut Dell Technologies Digital Transformation Index 2020 sind Bedenken hinsichtlich Datenschutz und Cybersicherheit die Hauptbarriere für die digitale Transformation.[1] Aufgrund einer ausgenutzten Sicherheitslücke erlebten 63 % der Unternehmen eine Datengefährdung[2]. Die weltweiten Schäden im Zusammenhang mit Cyberkriminalität werden im Jahr 2021 die Summe von 6 Billionen erreichen[3].

Da Server in einer softwarebasierten Rechenzentrumsarchitektur immer wichtiger werden, wird die Sicherheit dieser Server zur Grundlage der gesamten Unternehmenssicherheit. Die Server müssen die Sicherheit sowohl auf Hardware- als auch auf Firmwareebene gewährleisten. Dazu verwenden sie eine unveränderliche Root of Trust, mit der Folgevorgänge im Server verifiziert werden. Dadurch entsteht eine Vertrauenskette, die sich über den gesamten Serverlebenszyklus erstreckt, von der Bereitstellung über die Wartung bis zur Außerbetriebnahme.

Die 14. und die 15. Generation der Dell EMC PowerEdge-Server mit iDRAC9 bieten diese Vertrauenskette und kombinieren sie mit Sicherheitskontrollen und umfassenden Managementtools, um robuste Sicherheitsebenen für Hardware und Firmware bereitzustellen. Das Ergebnis ist eine cybersichere Architektur, die jeden Aspekt des Servers umfasst, darunter integrierte Serverfirmware, im System gespeicherte Daten, Betriebssystem, Peripheriegeräte und interne Managementabläufe. Unternehmen können einen Prozess zum Schutz ihrer wertvollen Serverinfrastruktur und der enthaltenen Daten erstellen, Anomalien, Verstöße oder nicht autorisierte Vorgänge erkennen und nach unbeabsichtigten oder bösartigen Ereignissen eine Recovery durchführen.

[1] Dell Technologies Digital Transformation Index 2020

[2] Match Present-Day Security threats with BIOS-Level Control. Ein von Dell in Auftrag gegebenes Thought Leadership Paper von Forrester Consulting, 2019

[3] Ransomware Attacks Predicted to Occur... The National Law Review, 2020

2. Der Weg zu einer sicheren Serverinfrastruktur

Dell EMC PowerEdge-Server bieten seit mehreren Generationen robuste Sicherheit, darunter auch die innovative Datensicherheit auf Chipebene. Bei der 14. Generation (14G) der Dell EMC PowerEdge-Server wurde diese Sicherheit auf Chipebene ausgeweitet, um BIOS und Firmware während des Server-Boot-Prozesses mit einem kryptografischen Root-of-Trust-Verfahren zu authentifizieren. Das Dell EMC Produktteam hat beim Design für die PowerEdge-Server der 14. und 15. Generation zahlreiche wichtige Anforderungen berücksichtigt, um den Sicherheitsbedrohungen in modernen IT-Umgebungen zu begegnen:

- **Schutz:** Schutz von Servern in allen Lebenszyklen, einschließlich BIOS, Firmware, Daten und physischer Hardware
- **Erkennung:** Erkennung bösartiger Cyberangriffe und nicht autorisierter Änderungen, proaktive Einbindung von IT-Administratoren
- **Recovery:** Recovery von BIOS, Firmware und Betriebssystem in einen fehlerfreien, bekannten Zustand, sichere Stilllegung oder neue Verwendung von Servern

Dell EMC PowerEdge-Server entsprechen den in diesem Dokument dargelegten wichtigen Branchenstandards für Kryptografie und Sicherheit. Zudem werden neue Sicherheitslücken fortlaufend nachverfolgt und gemanagt.

Dell EMC hat den Security Development Lifecycle-Prozess implementiert, der in puncto Sicherheit bei allen Aspekten von Entwicklung, Beschaffung, Fertigung, Versand und Support das Kernelement ist. Dies führt zu einer cybersicheren Architektur.

2.1 Security Development Lifecycle (SDL)

Die Bereitstellung einer cybersicheren Architektur erfordert Sicherheitsbewusstsein und Disziplin in jeder Phase der Entwicklung. Dieser Prozess wird als Security Development Lifecycle(SDL)-Modell bezeichnet, bei dem Sicherheit nicht nachträglich implementiert wird, sondern ein integraler Bestandteil des gesamten Serverdesignprozesses ist. Dieser Designprozess umfasst eine Betrachtung der Sicherheitsanforderungen im gesamten Serverlebenszyklus, die nachstehend aufgeführt und in Abbildung 1 angegeben werden:

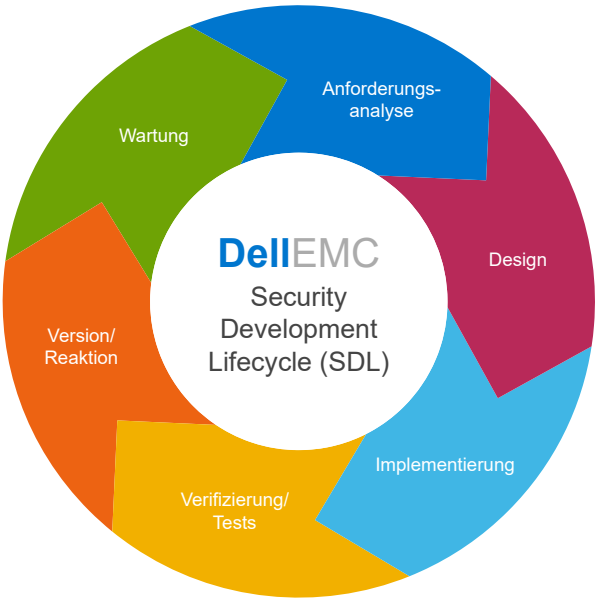


Abbildung 1: Security Development Lifecycle (SDL) von Dell EMC

- Bei Konzeption, Entwicklung, Prototyping, Implementierung, Übernahme in die Produktion, Bereitstellung und Wartung der Funktionen kommt der Sicherheit eine Hauptpriorität zu.
- Die Serverfirmware ist so entwickelt, dass sie die Einschleusung von bösartigem Code in allen Phasen des Produktentwicklungslebenszyklus blockiert, sich dieser entgegenstellt und sie bekämpft.
  - » Bedrohungsmodellierung und Penetrationstests im Designprozess
  - » Sichere Programmierverfahren in jeder Phase der Firmwareentwicklung
- Bei kritischen Technologien ergänzen externe Audits den internen SDL-Prozess, um sicherzustellen, dass die Firmware den bekannten Best Practices für Sicherheit entspricht.
- Fortlaufende Tests und Evaluierungen neuer potenzieller Sicherheitslücken werden mithilfe der neuesten Sicherheitsbewertungstools ausgeführt.
- Schnelle Reaktion auf kritische häufige Sicherheitslücken und Anfälligkeiten (Common Vulnerabilities and Exposures, CVEs), einschließlich empfohlener Korrekturmaßnahmen, sofern zugesichert.

2.2 Cybersichere Architektur

Die Dell EMC PowerEdge-Server der 14. und 15. Generation verfügen über eine verbesserte cybersichere Architektur, die ein robustes Serverdesign zum Schutz vor und zur Erkennung von Cyberangriffen sowie zur Recovery bietet. Zu den wichtigsten Aspekten dieser Architektur zählen:

- **Effektiver Schutz vor Angriffen**
  - » Chipbasierte Root of Trust
  - » Secure Boot
  - » Signierte Firmwareupdates
  - » Dynamische Systemsperre
  - » Festplattenverschlüsselung und Enterprise-Key-Management
- **Zuverlässige Angriffserkennung**
  - » Erkennung von Konfigurations- und Firmwareabweichungen
  - » Kontinuierliche Ereignisprotokollierung
  - » Auditprotokollierung und Warnmeldungen
  - » Erkennung von Gehäuseangriffen
- **Schnelle Recovery ohne oder mit nur kurzer Geschäftsunterbrechung**
  - » Automatische BIOS-Recovery
  - » Schnelle BS-Recovery
  - » Firmware-Rollback
  - » Schnelles SystemErase

2.3 Heutige Bedrohungen

In der heutigen, sich stets verändernden Landschaft gibt es viele Bedrohungsvektoren. In Tabelle 1 ist der Ansatz von Dell EMC für das Management kritischer Back-End-Bedrohungen zusammengefasst.

Tabelle 1: Umgang von Dell EMC mit gängigen Bedrohungsvektoren

Serverplattformebenen		
Sicherheitsschicht	**Bedrohungsvektor**	**Dell EMC Lösung**
Physischer Server	Manipulation von Servern/Komponenten	Secured Component Verification (SCV), Erkennung von Gehäuseangriffen
Firmware und Software	Firmwarebeschädigung, Einschleusung von Malware	Chipbasierte Root of Trust, Intel Boot Guard, AMD Secure Root of Trust, UEFI Secure Boot Customization Kryptografisch signierte und validierte Firmware
	Software	CVE-Reporting, Patching nach Bedarf
Funktionen zur Bestätigung der Vertrauenswürdigkeit (Trust Attestation)	Spoofing von Serveridentitäten	TPM, TXT, Vertrauenskette
Servermanagement	Nicht autorisierte Konfigurationen und Updates, Angriffe über unautorisierte offene Anschlüsse	iDRAC9, Remotebestätigung

Serverumgebungsebenen		
Sicherheitsschicht	**Bedrohungsvektor**	**Dell EMC Lösung**
Daten	Datenschutzverletzung	SED (selbstverschlüsselnde Festplatte) – FIPS oder Opal/TCG Secure Enterprise Key Management – reine ISE(Instant Secure Erase)-Festplatten Sichere Nutzerauthentifizierung
Integrität der Lieferkette	Gefälschte Komponenten Bedrohungen durch Malware	ISO 9001-Zertifizierung für alle globalen Serverfertigungsstandorte, Secured Component Verification (SCV), Nachweis des Besitzes Implementierung von Sicherheitsmaßnahmen im Rahmen des Secure Development Lifecycle(SDL)-Prozesses
Sicherheit der Lieferkette	Physische Sicherheit an Fertigungsstandorten Diebstahl und Manipulation während des Transports	FSR (Facility Security Requirements) gemäß Transported Asset Protection Association (TAPA) Customs-Trade Partnership Against Terrorism (C-TPAT), SCV

3. Schutz

Die Schutzfunktion („Protect“) ist eine Kernkomponente im NIST Cybersecurity Framework und schützt vor Angriffen auf die Cybersicherheit. Diese Funktion umfasst mehrere Kategorien, darunter Zugriffskontrolle, Datensicherheit, Wartung und Schutztechnologie. Der grundlegende Gedanke ist, dass die Infrastrukturressourcen – als Teil einer umfassenden sicheren Installations- und Computing-Umgebung – einen robusten Schutz vor unbefugtem Zugriff auf Ressourcen und Daten bieten müssen. Dazu gehört auch der Schutz vor unbefugten Modifikationen an kritischen Komponenten, wie z. B. BIOS und Firmware. Die Plattform erfüllt die aktuellen Empfehlungen gemäß NIST SP 800-193.

Die cybersichere Architektur der PowerEdge-Server bietet einen sehr hohen Plattformschutz mit folgenden Funktionen:

- Kryptografisch verifiziertes Trusted Booting
- Nutzerzugriffssicherheit
- Signierte Firmwareupdates
- Verschlüsselter Daten-Storage
- Physische Sicherheit
- Lieferkettenintegrität und -sicherheit

3.1 Kryptografisch verifiziertes Trusted Booting

Als einer der wichtigsten Aspekte bei der Serversicherheit muss sichergestellt werden, dass der Startvorgang als sicher verifiziert werden kann. Dieser Prozess bietet einen vertrauenswürdigen Anker für alle Folgevorgänge, wie z. B. den Betriebssystemstart oder das Firmwareupdate. PowerEdge-Server verwenden bereits seit mehreren Generationen die chipbasierte Sicherheit für Funktionen wie z. B. den iDRAC-Zugangsdaten-Vault, das ist ein verschlüsselter, sicherer Arbeitsspeicher in iDRAC für die Speicherung sensibler Daten. Der Startvorgang wird mit einer chipbasierten Root of Trust verifiziert, um die Empfehlungen gemäß NIST SP 800-147B („BIOS Protection Guidelines for Servers“) und NIST SP 800-155 („BIOS Integrity Measurement Guidelines“) zu erfüllen.

3.1.1 Chipbasierte Root of Trust

In PowerEdge-Servern der 14. und 15. Generation (auf Basis von Intel und AMD) wird nun eine unveränderliche chipbasierte Root of Trust (oder Silicon Root of Trust) eingesetzt, um die Integrität von BIOS und iDRAC-Firmware kryptografisch zu bestätigen. Diese Root of Trust basiert auf einmal programmierbaren, schreibgeschützten öffentlichen Schlüsseln, die Schutz vor Manipulationen durch Malware bieten. Der BIOS-Startprozess nutzt entweder die Intel Boot Guard-Technologie oder die AMD Root of Trust-Technologie. Diese verifiziert, dass die digitale Signatur vom kryptografischen Hash des Boot-Image mit der Signatur übereinstimmt, die werkseitig von Dell EMC im Chip gespeichert wurde. Im Falle einer fehlgeschlagenen Verifizierung wird der Server heruntergefahren und der Nutzer erhält eine Benachrichtigung über das Lifecycle Controller-Protokoll. Anschließend kann der BIOS-Recovery-Prozess vom Nutzer gestartet werden. Nach einer erfolgreichen Validierung durch Boot Guard werden die restlichen BIOS-Module in einem Vertrauenskettenverfahren bestätigt, bis die Steuerung an das Betriebssystem oder den Hypervisor übergeben wird.

Zusätzlich zum Verifizierungsmechanismus von Boot Guard stellt iDRAC9 4.10.10.10 oder höher einen Root-of-Trust-Mechanismus für die Überprüfung des BIOS-Image beim Hoststart bereit. Der Host kann nur starten, nachdem das BIOS-Image erfolgreich validiert wurde. iDRAC9 bietet außerdem einen Mechanismus für die Validierung des BIOS-Image zur Laufzeit, bei Bedarf oder zu von den Nutzern geplanten Intervallen.

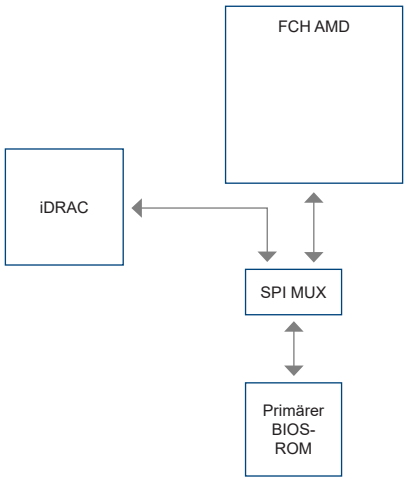
Betrachten wir die Vertrauenskette nun im Detail. Jedes BIOS-Modul enthält den Hash des nächsten Moduls in der Kette. Die wichtigsten Module im BIOS sind IBB (Initial Boot Block), SEC (Security), PEI (Pre-EFI Initialization), MRC (Memory Reference Code), DXE (Driver Execution Environment) und BDS (Boot Device Selection). Nachdem Intel Boot Guard das Modul IBB (Initial Boot Block) authentifiziert hat, validiert IBB die Module SEC und PEI, bevor diesen die Steuerung übergeben wird. SEC und PEI wiederum validieren dann PEI und MRC, die anschließend die Module DXE und BDS validieren. Zu diesem Zeitpunkt wird die Steuerung an UEFI Secure Boot übergeben, wie im nächsten Abschnitt beschrieben.

Ebenso stellt bei Dell EMC PowerEdge-Servern, die auf AMD EPYC basieren, die AMD Secure Root of Trust-Technologie sicher, dass die Server nur von vertrauenswürdigen Firmwareimages gestartet werden. Darüber hinaus verschlüsselt die AMD Secure Run-Technologie den Hauptspeicher, sodass dieser vor bösartigen Eindringlingen, die Zugriff auf die Hardware haben, geschützt bleibt. Zur Verwendung dieser Funktion sind keine Anwendungsänderungen nötig und der Sicherheitsprozessor exponiert die Verschlüsselungsschlüssel niemals außerhalb des Prozessors.

iDRAC übernimmt ebenfalls die Rolle von hardwarebasierten Sicherheitstechnologien und greift – zusätzlich zum AMD Fusion Controller Hub (FCH) – über SPI auf den primären BIOS-ROM zu und führt das Root-of-Trust-Verfahren durch.

Unter folgenden Bedingungen stellt iDRAC9 das BIOS wieder her:

1. Fehlgeschlagene BIOS-Integritätsprüfung
2. Fehlgeschlagener BIOS-Selbsttest
3. Verwendung des RACADM-Befehls – **racadm recover BIOS.Setup.1-1**



Der iDRAC-Startprozess verwendet eine eigene, unabhängige chipbasierte Root of Trust, um das iDRAC-Firmwareimage zu verifizieren. Diese iDRAC Root of Trust ist zudem ein wichtiger Vertrauensanker für die Authentifizierung der Signaturen von Dell EMC Firmwareupdatepaketen (DUPs).

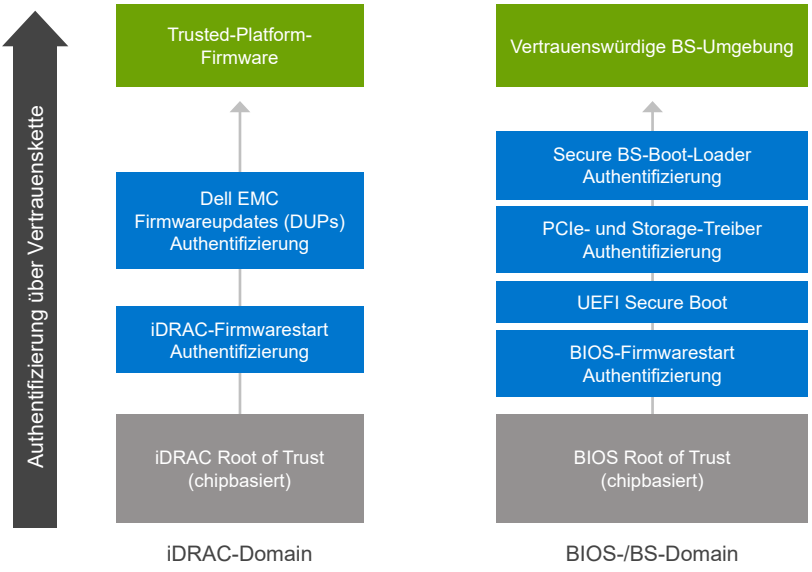


Abbildung 2: Chipbasierte Root-of-Trust-Domains in PowerEdge-Servern

3.1.2 BIOS-Live-Scanning

Mit BIOS-Live-Scanning werden die Integrität und die Authentizität des BIOS-Image im primären ROM beim Einschalten des Hosts verifiziert (aber nicht im POST-Prozess). Das ist eine reine AMD-Funktion, die nur mit iDRAC9 4.10.10.10 oder höher und einer Datacenter-Lizenz verfügbar ist. Zur Ausführung dieses Vorgangs sind Administratorrechte oder Operator-Berechtigungen mit der Debug-Berechtigung „Execute Debug Commands“ erforderlich. Der Scan kann über die iDRAC-UI sowie über die RACADM- und die Redfish-Schnittstelle eingeplant werden.

3.1.3 UEFI Secure Boot Customization

PowerEdge-Server unterstützen auch den Branchenstandard UEFI (Unified Extensible Firmware Interface) Secure Boot, der die kryptografischen Signaturen von UEFI-Treibern und anderem Code überprüft, der vor der BS-Ausführung geladen wurde. Secure Boot ist ein branchenweiter Standard für die Sicherheit in der Pre-Boot-Umgebung. Anbieter von Computersystemen, Erweiterungskarten und Betriebssystemen arbeiten gemeinsam an dieser Spezifikation, um deren Interoperabilität zu fördern.

Ist diese Option aktiviert, verhindert UEFI Secure Boot das Laden von unsignierten (d. h. nicht vertrauenswürdigen) UEFI-Gerätetreibern, zeigt eine Fehlermeldung an und unterbindet den Betrieb des Geräts. Um unsignierte Gerätetreiber laden zu können, muss Secure Boot deaktiviert werden.

Darüber hinaus bieten die 14. und 15. Generation der PowerEdge-Server den Kunden die einzigartige Flexibilität, ein kundenspezifisches Boot-Loader-Zertifikat zu verwenden, das nicht von Microsoft signiert ist Diese Funktion richtet sich in erster Linie an Administratoren von Linux-Umgebungen, die ihre eigenen BS-Boot-Loader signieren möchten. Nutzerdefinierte Zertifikate können über die bevorzugte iDRAC-API hochgeladen werden, um den spezifischen BS-Boot-Loader der Kunden zu authentifizieren. Diese von PowerEdge verwendete UEFI Customization-Methode wird von der NSA für die Reduzierung von Grub2-Sicherheitslücken in Servern angegeben.

3.1.4 TPM-Support

PowerEdge-Server unterstützen drei TPM-Versionen:

- TPM 1.2 FIPS + Common Criteria + TCG-zertifiziert (Nuvoton)
- TPM 2.0 FIPS + Common Criteria + TCG-zertifiziert (Nuvoton)
- TPM 2.0 China (NationZ)

Mithilfe des TPM lassen sich kryptografische Funktionen für den öffentlichen Schlüssel ausführen, Hash-Funktionen berechnen, Schlüssel generieren, managen und sicher speichern sowie Bestätigungen erstellen. Die TXT-Funktion (Trusted Execution Technology) von Intel und das Microsoft-Feature der Platform Assurance in Windows Server 2016 werden ebenfalls unterstützt. Das TPM kann auch verwendet werden, um die BitLocker™-Festplattenverschlüsselung in Windows Server 2012/2016 zu aktivieren.

Bestätigungs- und Remotebestätigungslösungen nutzen das TPM, um zur Startzeit der Hardware, des Hypervisors, des BIOS und des Betriebssystems auf einem Server Messungen durchzuführen und diese (auf kryptografisch sichere Weise) mit den im TPM gespeicherten Basiswerten zu vergleichen. Sind sie nicht identisch, wurde möglicherweise die Serveridentität kompromittiert. Die Systemadministratoren können den Server dann entweder lokal oder remote deaktivieren und trennen.

Server können mit oder ohne TPM bestellt werden, aber für viele Betriebssysteme und andere Sicherheitsvorkehrungen wird es zum Standard. Das TPM wird über eine BIOS-Option aktiviert. Es handelt sich um eine Plug-in-Modullösung, der Planar verfügt über einen Anschluss für das Plug-in-Modul.

3.1.5 Sicherheitszertifizierungen

Dell EMC hat Zertifizierungen für Standards wie z. B. NIST FIPS 140-2 und Common Criteria EAL-4 erhalten. Diese sind wichtig für die Einhaltung von Anforderungen des US-Verteidigungsministeriums und anderen Behörden. Für die PowerEdge-Server liegen folgende Zertifizierungen vor:

- Serverplattform: Common Criteria EAL4+ mit RHEL, auch zur Unterstützung der CC-Zertifizierungen von Partnern
- iDRAC und CMC FIPS 140-2 Level 1
- OpenManage Enterprise – Modular mit EAL2+
- FIPS 140-2 und Common Criteria für TPM 1.2 und 2.0

3.2 Nutzerzugriffssicherheit

Die ordnungsgemäße Authentifizierung und Autorisierung sicherzustellen, ist eine wichtige Voraussetzung für eine moderne Zugriffskontroll-Policy. Die primären Zugriffsschnittstellen für PowerEdge-Server sind die APIs, CLIs oder die GUI des eingebetteten iDRAC. Die bevorzugten APIs und CLIs für das automatisierte Servermanagement sind:

- iDRAC RESTful API mit Redfish
- RACADM CLI
- SELinux

Jede Option bietet zuverlässige Zugangsdaten (wie Nutzername und Kennwortsicherheit), die auf Wunsch über eine verschlüsselte Verbindung transportiert werden (z. B. HTTPS). SSH authentifiziert einen Nutzer mithilfe eines übereinstimmenden Satzes von kryptografischen Schlüsseln (damit entfällt die Eingabe von weniger sicheren Kennwörtern). Ältere Protokolle (wie z. B. IPMI) werden zwar unterstützt, aber aufgrund von verschiedenen Sicherheitsproblemen, die in den letzten Jahren erkannt wurden, für neue Bereitstellungen nicht empfohlen. Wenn Sie derzeit IPMI verwenden, sollten Sie einen Wechsel zur iDRAC Restful API mit Redfish in Betracht ziehen.

TLS/SSL-Zertifikate können zur Authentifizierung von Webbrowsersitzungen in iDRAC hochgeladen werden. Es gibt drei Optionen:

- **Selbstsigniertes Dell EMC TLS/SSL-Zertifikat:** Das Zertifikat wird automatisch generiert und von iDRAC selbst signiert.
  - » Vorteil: Es ist keine separate Zertifizierungsstelle (Certificate Authority, CA) mehr erforderlich (siehe X.509-/IETF PKIX-Standards).
- **Nutzerdefiniertes TLS/SSL-Zertifikat:** Das Zertifikat wird automatisch generiert und mit einem privaten Schlüssel signiert, der bereits in iDRAC hochgeladen wurde.
  - » Vorteil: Eine einzige vertrauenswürdige CA für alle iDRACs. Es ist möglich, dass Ihre interne CA auf Ihren Managementstationen bereits als vertrauenswürdig gilt.
- **CA-signiertes TLS/SSL-Zertifikat:** Eine Zertifikatsignierungsanforderung (Certificate Signing Request, CSR) wird generiert und an Ihre interne CA oder an die eines Drittanbieters (z. B. VeriSign, Thawte und Go Daddy) übermittelt.
  - » Vorteile: Eine kommerzielle Zertifizierungsstelle kann verwendet werden (siehe X.509-/IETF PKIX-Standards). Eine einzige vertrauenswürdige CA für all Ihre iDRACs. Bei Verwendung einer kommerziellen CA wird diese vermutlich auf Ihren Managementstationen bereits als vertrauenswürdig gelten.

iDRAC9 ermöglicht die Integration in **Active Directory** und **LDAP**, und zwar durch die Nutzung vorhandener Authentifizierungs- und Autorisierungsschemata des Kunden, die bereits einen sicheren Zugriff auf PowerEdge-Server bieten. Außerdem wird die **rollenbasierte Zugriffskontrolle (Role-Based Access Control, RBAC)** unterstützt, um die korrekte Zugriffsebene zu gewähren – Administrator, Operator oder schreibgeschützt –, die für die Rolle der Mitarbeiter im Serverbetrieb erforderlich ist. Es wird dringend empfohlen, RBAC auf diese Art und Weise zu verwenden und nicht einfach allen Nutzern die höchsten Zugriffsberechtigungen (also Administrator) zu erteilen.

iDRAC9 bietet zudem zusätzlichen Schutz vor unbefugtem Zugriff, einschließlich **IP-Blockierung und -Filterung**. Bei der IP-Blockierung wird dynamisch erkannt, wenn bei einer bestimmten IP-Adresse zu viele Anmeldefehler auftreten. Die Funktion blockiert dann diese Adresse bzw. verhindert für einen vorab festgelegten Zeitraum die Anmeldung an iDRAC9. Die IP-Filterung schränkt den IP-Adressbereich der Clients ein, die auf iDRAC zugreifen können. Sie vergleicht die IP-Adresse einer eingehenden Anmeldung mit dem angegebenen Bereich und gewährt den iDRAC-Zugriff nur von einer Managementstation, deren Quell-IP-Adresse innerhalb dieses Bereichs liegt. Alle anderen Anmeldeanfragen werden abgelehnt.

Die **Multifaktor-Authentifizierung (MFA)** wird heutzutage – aufgrund der zunehmenden Sicherheitslücken bei einstufigen Authentifizierungssystemen, die auf dem Nutzernamen und einem Kennwort basieren – häufig verwendet. iDRAC9 ermöglicht die Verwendung von Smartcards für den Remote-GUI-Zugriff und unterstützt RSA-Token. In beiden Fällen erfordert die Multifaktor-Authentifizierung das physische Vorhandensein eines Geräts oder einer Karte und die zugehörige PIN.

3.2.1 RSA SecurID MFA

RSA SecurID kann als weiteres Verfahren zur Authentifizierung von Nutzern auf einem System verwendet werden. iDRAC9 beginnt mit der Unterstützung von RSA SecurID mit einer Datacenter-Lizenz und Firmware 4.40.00.00 als weitere Multifaktor-Authentifizierungsmethode.

3.2.2 Vereinfachte 2FA

Eine weitere angebotene Authentifizierungsmethode ist Easy 2FA, die ein zufällig generiertes Token an die E-Mail-Adresse des Nutzers sendet, wenn dieser sich an iDRAC anmeldet.

3.2.3 SELinux Framework

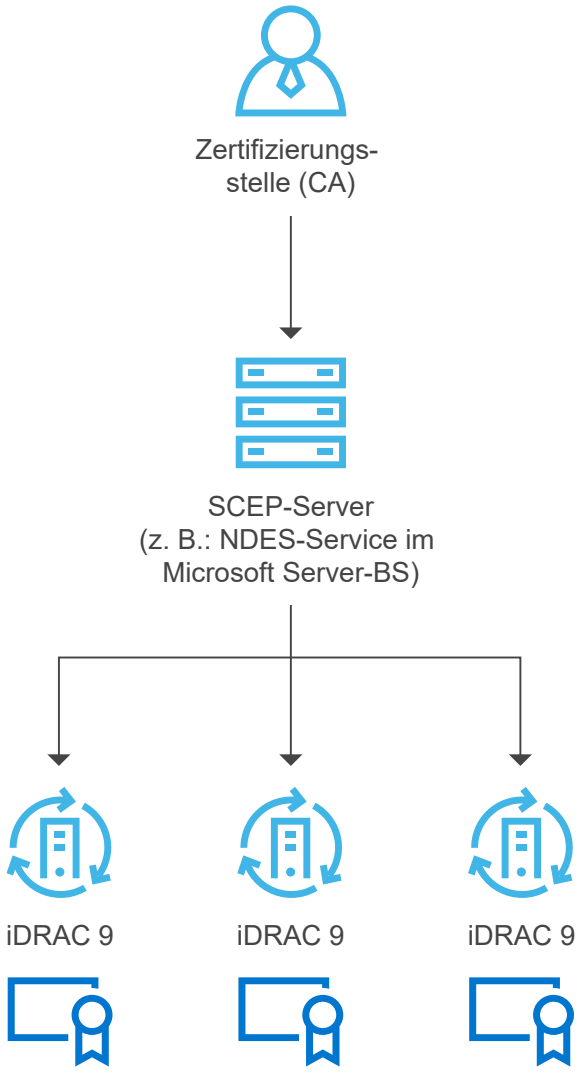
SELinux funktioniert auf der Core-Kernel-Ebene von iDRAC und benötigt weder eine Eingabe noch die Konfiguration von Nutzern. Nach Erkennung eines Angriffs protokolliert SELinux Sicherheitsmeldungen. Diese Protokollmeldungen geben an, wann und wie ein Angreifer versucht hat, in das System einzudringen. Derzeit sind diese Protokolle über SupportAssist für Kunden verfügbar, die sich für diese neue Funktion angemeldet haben. In zukünftigen Versionen von iDRAC werden diese Protokolle in den Lifecycle Controller-Protokollen zur Verfügung stehen.

3.2.4 Geringste Rechte

Alle intern in iDRAC ausgeführten Prozesse erfolgen auf Grundlage der geringsten Rechte. Das ist ein grundlegendes UNIX-Sicherheitskonzept. Dieser Schutz stellt sicher, dass der Prozess eines Systems, das angegriffen wird, nicht auf Dateien oder Hardware außerhalb dieses Prozesses zugreifen kann. Beispielsweise sollte der Prozess, der Unterstützung für virtuelle KVMs bietet, nicht die Lüftergeschwindigkeit ändern können. Die Ausführung dieser beiden Prozesse als separate Funktionen trägt zum Schutz des Systems bei, da Angriffe nicht von einem Prozess zu einem anderen „überspringen“ können.

3.2.5 Automatische Zertifikatregistrierung und -verlängerung

iDRAC9 v4.0 verfügt über einen hinzugefügten Client zur Unterstützung des Simple Certificate Enrollment Protocol (SCEP) und erfordert eine Datacenter-Lizenz. SCEP ist ein Protokollstandard, der einen automatischen Registrierungsprozess nutzt, um Zertifikate für eine große Anzahl von Netzwerkgeräten zu managen. iDRAC kann nun mit SCEP-kompatiblen Servern wie dem Network Device Enrollment Service (NDES) in Microsoft Server integriert werden, mit dem sich SSL-/TLS-Zertifikate automatisch verwalten lassen. Diese Funktion kann für die Registrierung und Verlängerung eines in Kürze ablaufenden Webserverzertifikats verwendet werden. Sie lässt sich auf einer 1:1-Basis in der iDRAC-GUI ausführen, über das Serverkonfigurationsprofil einstellen oder über Tools wie RACADM als Skript erstellen.



3.2.6 Werkseitig generiertes Standardkennwort

Standardmäßig werden alle PowerEdge-Server der 14. Generation mit einem eindeutigen, werkseitig generierten iDRAC-Kennwort ausgeliefert, das zusätzliche Sicherheit bietet. Dieses Kennwort wird im Werk generiert und befindet sich auf dem herausziehbaren Informationsetikett auf der Vorderseite des Gehäuses neben dem Etikett für den Server. Nutzer, die diese Standardoption auswählen, müssen das Kennwort notieren und es bei der ersten Anmeldung an iDRAC verwenden (anstelle eines universellen Standardkennworts). Aus Sicherheitsgründen empfiehlt Dell EMC dringend, das Standardkennwort zu ändern.

3.2.7 Dynamische Systemsperre

iDRAC9 bietet eine neue Funktion, die die Hardware- und Firmwarekonfiguration eines Servers oder mehrerer Server „sperrt“ und eine Enterprise- oder Datacenter-Lizenz erfordert. Dieser Modus kann über die GUI, über CLIs wie z. B. RACADM oder als Teil des Serverkonfigurationsprofils aktiviert werden. Nutzer mit Administratorrechten können den Systemsperrmodus einstellen. Er verhindert, dass Nutzer mit geringeren Rechten Änderungen am Server vornehmen. Diese Funktion kann vom IT-Administrator aktiviert bzw. deaktiviert werden. Alle Änderungen, die bei deaktivierter Systemsperre erfolgen, werden im Lifecycle Controller-Protokoll erfasst. Der aktivierte Sperrmodus verhindert Konfigurationsabweichungen im Rechenzentrum, wenn Sie Dell EMC Tools und Agents verwenden, und schützt vor bösartigen Angriffen auf integrierte Firmware, wenn Sie Dell EMC Update Packages verwenden. Der Sperrmodus lässt sich dynamisch aktivieren, ohne dass ein Systemneustart erforderlich ist. Mit iDRAC9 v4.40 werden Verbesserungen eingeführt, mit denen die aktuelle Systemsperrfunktion, die nur über Dell Update Package (DUP) ausgeführte Updates steuert, auch auf ausgewählte NICs ausgedehnt wird. (HINWEIS: Die erweiterte Sperrfunktion für NICs umfasst nur die Firmwaresperre, um Firmwareupdates zu verhindern.) Die Konfigurationssperre (x-UEFI) wird nicht unterstützt. Wenn Kunden das System in den Sperrmodus versetzen, indem sie das entsprechende Attribut über eine der unterstützten Schnittstellen aktivieren oder einstellen, führt iDRAC die zusätzlichen Aktionen gemäß der Systemkonfiguration aus. Diese Aktionen hängen von den Drittanbietergeräten ab, die im Rahmen des iDRAC-Erkennungsprozesses ermittelt wurden.

3.2.8 Domain-Isolierung

PowerEdge-Server der 14. und 15. Generation bieten zusätzliche Sicherheit über die **Domain-Isolierung**, eine wichtige Funktion für mehrmandantenfähige Hostingumgebungen. Für den Schutz der Hardwarekonfiguration eines Servers können Hostinganbieter eine Neukonfiguration durch Mandanten blockieren. Bei der Domain-Isolierung handelt es sich um eine Konfigurationsoption, mit der Managementanwendungen im Hostbetriebssystem keinen Zugriff auf den Out-of-Band-iDRAC oder auf Intel Chipsatzfunktionen (wie z. B. Management Engine (ME) oder Innovation Engine (IE)) haben.

3.3 Signierte Firmwareupdates

PowerEdge-Server verwenden seit mehreren Generationen digitale Signaturen für Firmwareupdates, um sicherzustellen, dass nur Originalfirmware auf der Serverplattform ausgeführt wird. Die digitale Signatur von all unseren Firmwarepaketen erfolgt über SHA-256-Hashing mit RSA-Verschlüsselung (2048 Bit) für die Signatur aller wichtigen Serverkomponenten, einschließlich Firmware für iDRAC, BIOS, PERC, I/O-Adapter und LOMs, Stromversorgungseinheiten, Storage-Laufwerke, CPLD- und Rückwandplatinen-Controller. iDRAC scannt die Firmwareupdates und vergleicht deren Signaturen mit den erwarteten Werten in der chipbasierten Root of Trust. Jedes Firmwarepaket, bei dem die Validierung fehlschlägt, wird abgebrochen, und im Lebenszyklusprotokoll (Lifecycle Log, LCL) wird eine Fehlermeldung zur Benachrichtigung der IT-Administratoren protokolliert.

Die erweiterte Firmwareauthentifizierung ist in viele Geräte von Drittanbietern integriert, die eine Signaturvalidierung mithilfe ihrer eigenen Root-of-Trust-Mechanismen bereitstellen. Dadurch wird verhindert, dass über ein kompromittiertes Updatetool von Drittanbietern bösartige Firmware beispielsweise in eine NIC oder ein Storage-Laufwerk geladen werden kann (und die Verwendung von signierten Dell EMC Update Packages umgangen wird). Bei vielen der PCIe- und Storage-Geräte von Drittanbietern, die mit PowerEdge-Servern ausgeliefert werden, wird eine Hardware-Root-of-Trust zur Validierung der jeweiligen Firmwareupdates eingesetzt.

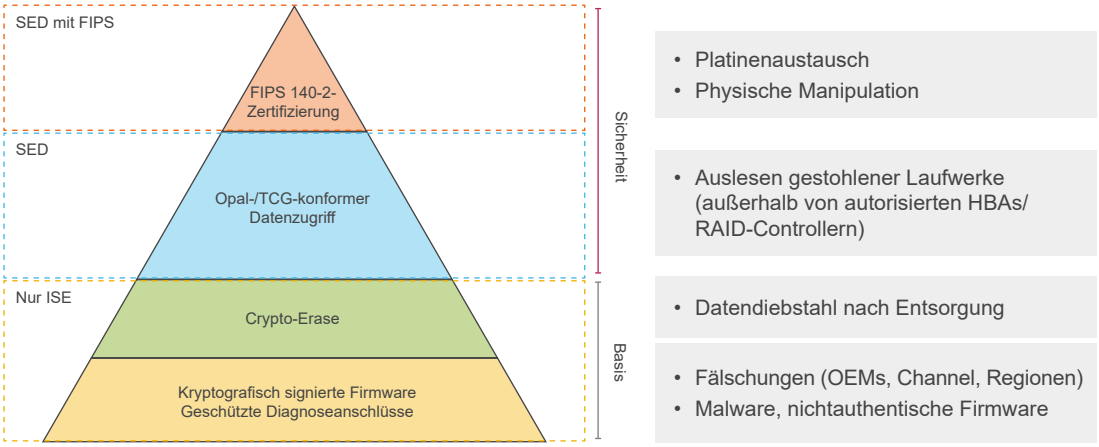
Sollte bei einer Firmware auf einem Gerät eine bösartige Manipulation vermutet werden, können die IT-Administratoren für viele Firmwareimages der Plattformen ein Rollback auf eine frühere vertrauenswürdige Version, die in iDRAC gespeichert ist, durchführen. Wir behalten zwei Versionen der Gerätefirmware auf dem Server: die vorhandene Produktionsversion („N“) und eine vorherige vertrauenswürdige Version („N-1“).

3.4 Verschlüsselter Daten-Storage

PowerEdge-Server der 14. und 15. Generation bieten verschiedene Storage-Laufwerkoptionen für den Schutz der Daten. Wie unten in der Abbildung dargestellt, beginnen die Optionen mit Festplatten, die Instant Secure Erase (ISE) unterstützen, eine neue Technologie für die sofortige und sichere Löschung von Nutzerdaten. Server der 14. und 15. Generation bieten standardmäßig ISE-fähige Festplatten. ISE wird später in diesem Whitepaper im Rahmen der SystemErase-Funktionsbeschreibung ausführlicher erklärt.

Die nächsthöhere Sicherheitsoption sind selbstverschlüsselnde Festplatten (Self-Encrypting Drives, SEDs), mit deren Sperrschutz das Storage-Laufwerk an den verwendeten Server und die verwendete RAID-Karte gebunden wird. Dies schützt vor dem sogenannten Blitzdiebstahl eines Laufwerks und dem nachfolgenden Verlust sensibler Nutzerdaten. Falls ein Dieb versucht, das Laufwerk zu verwenden, kennt er die erforderliche Passphrase nicht und kann daher nicht auf die verschlüsselten Laufwerkdaten zugreifen. Kunden können mithilfe von Secure Enterprise Key Manager (SEKM) den gesamten Server vor Diebstahl schützen. Diese Option wird später in diesem Whitepaper beschrieben.

Den höchsten Schutz bieten NIST FIPS 140-2-zertifizierte SEDs. Festplatten mit diesem Standard wurden von Testlaboren bestätigt und zeichnen sich durch manipulationssichere Aufkleber aus. Die selbstverschlüsselnden Festplatten (SEDs) von Dell EMC sind standardmäßig FIPS 140-2-zertifiziert.



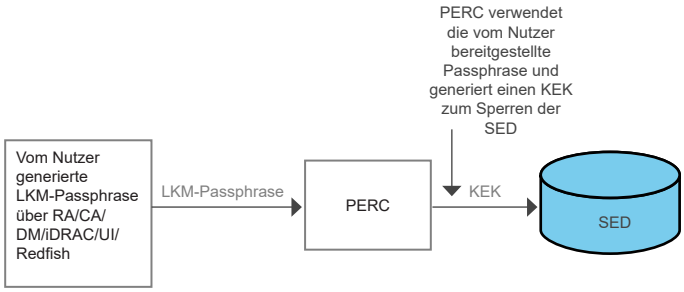
3.4.1 iDRAC-Zugangsdaten-Vault

Der iDRAC-Serviceprozessor bietet einen Arbeitsspeicher als sicheren Storage, der verschiedene sensible Daten schützt, wie z. B. iDRAC-Nutzerzugangsdaten und private Schlüssel für selbstsignierte SSL-Zertifikate. Als weiteres Beispiel für chipbasierte Sicherheit wird dieser Arbeitsspeicher mit einem eindeutigen, unveränderlichen Root-Schlüssel verschlüsselt, der bereits während der Fertigung auf jeden iDRAC-Chip programmiert wird. Das schützt vor physischen Angriffen, bei denen der Angreifer den Chip ablötet, um Zugriff auf die Daten zu erhalten.

3.4.2 Lokales Key-Management (LKM)

Die aktuellen PowerEdge-Server bieten Nutzern die Möglichkeit, die an einen PERC (PowerEdge RAID-Controller) angeschlossenen SEDs mithilfe des lokalen Key-Managements (LKM) zu schützen.

Damit im Falle eines Festplattendiebstahls der Schutz der Nutzerdaten sichergestellt ist, muss die SED mit einem separaten Schlüssel gesperrt werden. Die Entschlüsselung der Nutzerdaten erfolgt erst, wenn dieser Schlüssel – der sogenannte Schlüsselverschlüsselungsschlüssel (Key Encryption Key, KEK) – angegeben wird. Dazu legt der Nutzer eine Schlüssel-ID und Passphrase auf dem PERC fest, an den die SED angeschlossen ist. Der PERC generiert mithilfe der Passphrase einen KEK und verwendet diesen zum Sperren der SED. Die eingeschaltete Festplatte ist dann eine gesperrte SED und ver- bzw. entschlüsselt die Nutzerdaten nur, wenn der KEK zur Aufhebung der Sperre angegeben wird. Der PERC stellt der Festplatte den KEK zum Entsperren zur Verfügung. Sollte also die Festplatte gestohlen werden, ist sie gesperrt. Der Angreifer kann den KEK nicht angeben und somit sind die Nutzerdaten geschützt. Das wird als „lokales“ Key-Management bezeichnet, weil die Passphrase und der KEK lokal auf dem PERC gespeichert sind. Die folgende Abbildung veranschaulicht die LKM-Lösung.

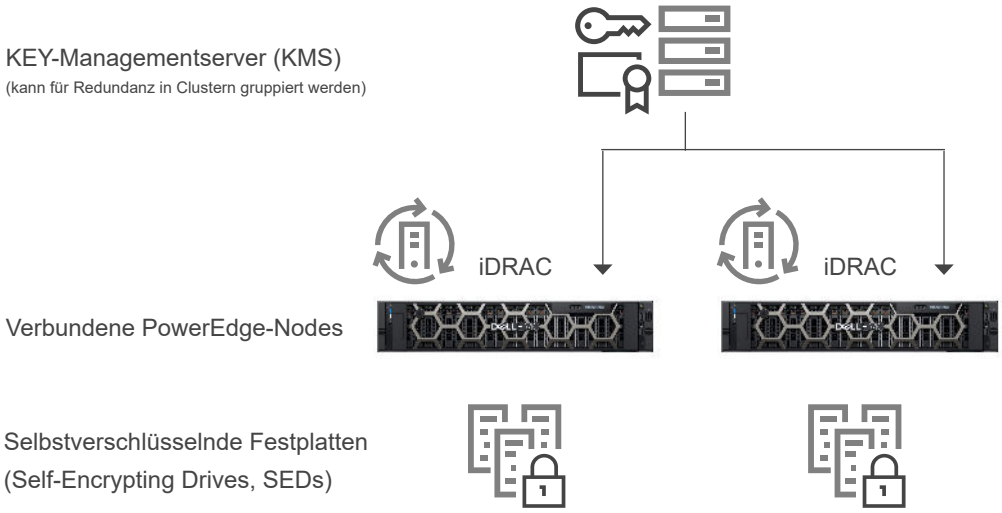


3.4.3 Secure Enterprise Key Manager (SEKM)

OpenManage SEKM bietet eine zentrale Key-Managementlösung für das Data-at-Rest-Management im gesamten Unternehmen. Damit können Kunden einen externen Key-Managementserver (KMS) zum Managen der Schlüssel verwenden, die iDRAC zum Sperren und Entsperren von Storage-Geräten auf einem Dell EMC PowerEdge-Server verwendet. Bei Nutzung von integriertem Code, der mit einer speziellen Lizenz aktiviert wird, fordert iDRAC den KMS auf, einen Schlüssel für jeden Storage-Controller zu erstellen. Diesen ruft iDRAC ab und stellt ihn für jeden Storage-Controller bei jedem Hoststart bereit, damit der Storage-Controller die SEDs (selbstverschlüsselnden Festplatten) entsperren kann.

SEKM bietet gegenüber dem lokalen Key-Management (LKM) folgende Vorteile:

- Schutz vor Serverdiebstahl (da die Schlüssel nicht auf dem Server, sondern extern gespeichert sind und von den verbundenen PowerEdge-Server-Nodes (über iDRAC) abgerufen werden)
- Zentrales und skalierbares Key-Management für verschlüsselte Geräte mit hoher Verfügbarkeit
- Unterstützung des branchenüblichen KMIP-Protokolls (ermöglicht die Verwendung von anderen KMIP-kompatiblen Geräten)
- Data-at-Rest-Schutz im Falle von kompromittierten Laufwerken oder gesamten Servern
- Skalierbare Performance der On-Drive-Verschlüsselung nach Anzahl der Laufwerke



3.5 Hardwaresicherheit

Die Hardwaresicherheit ist ein wichtiger Bestandteil jeder umfassenden Sicherheitslösung. Einige Kunden möchten den Zugriff über Eingabeanschlüsse wie z. B. USB einschränken. Ein Servergehäuse muss in der Regel nicht geöffnet werden, nachdem es in Betrieb genommen wurde. In allen Fällen möchten Kunden solche Aktivitäten mindestens verfolgen und protokollieren. Das übergeordnete Ziel besteht darin, jeglichen physischen Eingriff zu erschweren und einzuschränken.

3.5.1 Warnmeldung bei Gehäuseangriffen

PowerEdge-Server bieten die Erkennung und Protokollierung von Hardwareangriffen mit Funktionen, die auch ohne Netzstrom verfügbar sind. Sensoren am Gehäuse erkennen, wenn das Gehäuse geöffnet oder manipuliert wird, auch während des Transports. Server, die während des Transports geöffnet wurden, generieren einen Eintrag im iDRAC-Lebenszyklusprotokoll, sobald sie an die Stromversorgung angeschlossen werden.

3.5.2 Dynamisches USB-Anschlussmanagement

Für mehr Sicherheit können die USB-Anschlüsse vollständig deaktiviert werden. Zudem besteht auch die Möglichkeit, nur die USB-Anschlüsse an der Vorderseite zu deaktivieren. Beispielsweise können USB-Anschlüsse für den produktiven Betrieb deaktiviert und dann vorübergehend aktiviert werden, um im Notfall für Debugging-Zwecke den Zugriff zu ermöglichen.

3.5.3 iDRAC Direct

iDRAC Direct ist ein spezieller USB-Anschluss, der mit dem iDRAC-Serviceprozessor für das Server-Debugging und -management an der Vorderseite des Servers fest verdrahtet ist (Cold Aisle). Damit können Nutzer ein standardmäßiges Micro-AB-USB-Kabel an diesen Anschluss und das andere Ende (Typ A) an einen Laptop anschließen. Über einen gängigen Webbrowser lässt sich dann die iDRAC-GUI für das umfangreiche Debugging und Management des Servers aufrufen. Sofern eine iDRAC-Enterprise-Lizenz installiert ist, können Nutzer sogar über die virtuelle Konsole in iDRAC auf den BS-Desktop zugreifen.

Da für die Anmeldung normale iDRAC-Zugangsdaten verwendet werden, fungiert iDRAC Direct als sichere Notfallmethode und bietet den zusätzlichen Vorteil von umfangreichem Hardwaremanagement und Servicediagnosen. Das ist eine interessante Option, um den physischen Zugriff auf Server an Remotestandorten zu schützen (die USB-Hostanschlüsse und VGA-Ausgänge können in diesem Fall deaktiviert werden).

3.5.4 iDRAC Connection View mit Geolocation

Über die Connection View-Funktion kann iDRAC die externen Switches und Anschlüsse erkennen, die mit den I/O-Modulen des Servers verbunden sind. Diese Funktion ist nur für ausgewählte Netzwerkgeräte verfügbar, zudem muss LLDP (Link Layer Discovery Protocol) auf den angeschlossenen Switches aktiviert sein.

Die Connection View-Funktion bietet folgende Vorteile:

- Remote- und schnelle Anschlussüberprüfung (ob die I/O-Module der Server (LOMs, NDCs und Add-in-PCIe-Karten) mit die richtigen Switches und Anschlüssen verbunden sind)
- Vermeidung kostspieliger Außendiensteinsätze von Technikern zum Beheben von Verkabelungsfehlern
- Keine Rückverfolgung mehr von Kabeln in Hot Aisles im Serverraum
- Kann über die GUI erfolgen oder über RACADM-Befehle, die Informationen für alle 14G-Verbindungen liefern

Abgesehen von den offensichtlichen Zeit- und Kosteneinsparungen bietet die Connection View-Funktion einen weiteren Vorteil: Sie liefert in Echtzeit den geografischen Standort (Geolocation) eines physischen Servers oder einer virtuellen Maschine. Mithilfe von iDRAC Connection View können Administratoren einen Server präzise lokalisieren und exakt ermitteln, mit welchem Switch und Anschluss der Server verbunden ist. Dadurch wird sichergestellt, dass die Server nicht mit Netzwerken und Geräten verbunden sind, die nicht konform mit den Sicherheitsrichtlinien des Unternehmens oder den Best Practices sind.

Connection View validiert die Position des Servers indirekt durch die Angabe der Switch-Identitäten, mit denen er verbunden ist. Die Switch-Identität trägt dazu bei, den geografischen Standort zu bestimmen und sicherzustellen, dass der Server kein unbefugter Server an einem nichtautorisierten Standort ist. Damit stellt sie eine weitere physische Sicherheitsebene bereit. Das ermöglicht zudem die Validierung, dass eine Anwendung oder VM keine Ländergrenzen „überschritten“ hat und dass sie in einer geprüften, sicheren Umgebung ausgeführt wird.

3.6 Lieferkettenintegrität und -sicherheit

Die Lieferkettenintegrität konzentriert sich auf zwei wichtige Herausforderungen:

1. Aufrechterhaltung der Hardwareintegrität: Es muss sichergestellt werden, dass keine Produktmanipulation stattfindet und keine gefälschten Komponenten in das Produkt gelangen, bevor es an Kunden ausgeliefert wird.
2. Aufrechterhaltung der Softwareintegrität: Es muss sichergestellt werden, dass keine Malware in die Firmware oder in Gerätetreiber eingebracht wird, bevor das Produkt an den Kunden geliefert wird. Außerdem gilt es, Sicherheitslücken in der Programmierung zu vermeiden.

Dell EMC definiert die Lieferkettensicherheit als die Praxis und Anwendung präventiver und erkennender Kontrollmaßnahmen, die physische Ressourcen, Inventar, Informationen, geistiges Eigentum und Menschen schützen. Diese Sicherheitsmaßnahmen helfen auch bei der Lieferkettensicherheit und -integrität, indem sie Möglichkeiten für das bösartige oder fahrlässige Einbringen von Malware und gefälschten Komponenten in der Lieferkette reduzieren.

3.6.1 Hardware- und Softwareintegrität

Der Schwerpunkt von Dell EMC liegt in der Sicherstellung, dass mithilfe von vorhandenen Qualitätskontrollprozessen die Möglichkeiten minimiert werden, gefälschte Komponenten in unsere Lieferkette einzubringen. Zu den Kontrollen von Dell EMC zählen Lieferantenauswahl, Beschaffung, Produktionsprozesse und Governance durch Audits und Tests. Nach der Auswahl eines Lieferanten wird im neuen Produkteinführungsprozess verifiziert, dass alle in sämtlichen Herstellungsphasen verwendeten Materialien aus der Liste der autorisierten Anbieter beschafft wurden und der Materialstückliste entsprechen. Materialprüfungen während der Produktion helfen dabei, Komponenten aufzuspüren, die fehlerhaft sind, von den üblichen Leistungsparametern abweichen oder eine falsche elektronische Kennung aufweisen.

Die Teile werden, soweit möglich, direkt vom Original Design Manufacturer (ODM) oder vom Original Component Manufacturer (OCM) beschafft. Die Materialprüfung des neuen Produkteinführungsprozesses bietet viele Möglichkeiten zur Identifizierung von gefälschten oder beschädigten Komponenten, die in die Lieferkette eingebracht worden sein könnten.

Darüber hinaus hat Dell EMC die ISO 9001-Zertifizierung für alle globalen Fertigungsstandorte. Die strikte Einhaltung dieser Prozesse und Kontrollen trägt dazu bei, das Risiko zu minimieren, dass sich gefälschte Komponenten in die Produkte von Dell EMC einschleichen oder dass Malware in Firmware oder Gerätetreibern versteckt werden kann. Diese Maßnahmen werden als Teil des Software Development Lifecycle(SDL)-Prozesses implementiert.

3.6.2 Physische Sicherheit

Dell EMC verfügt über zahlreiche etablierte und wichtige Vorgehensweisen für die Einrichtung und Aufrechterhaltung der Sicherheit in Fertigungseinrichtungen und Logistiknetzwerken. Beispielsweise müssen die Fabriken, in denen Dell EMC Produkte gefertigt werden, bestimmte FSRs (Facility Security Requirements) der Transported Asset Protection Association (TAPA) erfüllen. Dazu zählen auch die Videoüberwachung von wichtigen Bereichen, die Zugriffskontrolle sowie stets bewachte Ein- und Ausgänge. Außerdem wurden Schutzmaßnahmen ergriffen, um die Produkte während des Transports vor Diebstahl und Manipulation zu schützen. Das ist Teil eines branchenführenden Logistikprogramms. Dieses Programm bietet ein rund um die Uhr besetztes Command Center, mit dem das Monitoring ausgewählter ein- und ausgehender Lieferungen weltweit möglich ist. So wird sichergestellt, dass die Lieferungen ohne Unterbrechungen von einem Bestimmungsort zum anderen gelangen.

Dell EMC engagiert sich auch aktiv für verschiedene freiwillige Sicherheitsprogramme und -initiativen im Zusammenhang mit der Lieferkette. Eine solche Initiative ist die von der US-Regierung nach dem 11. September eingeführte Customs-Trade Partnership Against Terrorism (C-TPAT), die mögliche terroristische Aktivitäten durch verstärkte Grenzkontrollen und weitere Sicherheitsmaßnahmen in der Lieferkette reduziert. Im Rahmen dieser Initiative bittet die US-amerikanische Zoll- und Grenzschutzbehörde die teilnehmenden Unternehmen, die Integrität ihrer Sicherheitsmaßnahmen sicherzustellen und ihre Sicherheitsrichtlinien an die Businesspartner in der Lieferkette zu übermitteln. Dell EMC ist seit 2002 aktiver Teilnehmer und hält den höchsten Mitgliedschaftsstatus.

3.6.3 Dell Technologies Secured Component Verification (SCV) für PowerEdge

Die Dell Technologies Secured Component Verification (SCV) für PowerEdge ist ein Angebot zur Lieferkettensicherheit, mit dem Dell EMC Kunden überprüfen können, ob der erhaltene PowerEdge-Server den Herstellungsspezifikationen im Werk entspricht. Um die Komponenten auf kryptografisch sichere Weise validieren zu können, wird während des Fertigungsprozesses ein Zertifikat im Werk generiert, das eindeutige Komponenten-IDs für einen bestimmten Server enthält. Dieses Zertifikat wird im Dell Technologies Werk signiert und in iDRAC gespeichert, damit die Kunden es später in der SCV-Anwendung nutzen können. Die Kunden erfassen mithilfe der SCV-Anwendung das aktuelle Systeminventar, einschließlich der eindeutigen Komponenten-IDs, und validieren dieses anhand des Inventars im SCV-Zertifikat.

Die SCV-Anwendung generiert einen Bericht, der darlegt, welche Komponenten mit der werkseitigen Installation übereinstimmen und welche nicht. Auch das Zertifikat und die Vertrauenskette werden ebenso wie der Besitznachweis des privaten SCV-Schlüssels für iDRAC überprüft. Die aktuelle Implementierung unterstützt den Direktversand an Kunden und umfasst keine Szenarien für Wiederverkäufer oder den Austausch von Teilen.

4. Erkennung

Es ist wichtig, dass eine Erkennungsfunktion vorhanden ist, die umfassende Sichtbarkeit in Konfiguration, Integritätszustand und Änderungsereignisse eines Serversystems bietet. Diese Sichtbarkeit muss auch bösartige sowie andere Änderungen an BIOS, Firmware und Option ROMs während des Start- und BS-Laufzeitprozesses erkennen. Proaktives Polling muss mit der Möglichkeit einhergehen, Warnmeldungen für alle Ereignisse im System zu senden. Protokolle müssen umfassende Informationen über jedweden Zugriff auf den Server und alle Änderungen am Server enthalten. Am wichtigsten ist jedoch, dass der Server diese Funktionen auf alle Komponenten ausweiten muss.

4.1 Umfassendes Monitoring mit iDRAC

Anstatt die Kommunikation mit gemanagten Ressourcen in einem Server den BS-Agents zu überlassen, nutzt iDRAC einen direkten Seitenbandpfad zu jedem Gerät. Dell EMC setzt branchenübliche Protokolle (wie MCTP, NC-SI und NVMe-MI) für die Kommunikation mit Peripheriegeräten (wie PERC RAID-Controller, Ethernet-NICs, Fibre-Channel-HBAs, SAS-HBAs und NVMe-Laufwerke) ein. Diese Architektur ist das Ergebnis von langen mehrjährigen Partnerschaften mit branchenführenden Anbietern, um ein Agent-freies Gerätemanagement in unseren PowerEdge-Servern zu ermöglichen. Die Konfigurations- und Firmwareupdatevorgänge nutzen auch die leistungsstarken UEFI- und HII-Funktionen, die von Dell EMC und unseren Partnern unterstützt werden.

Dank dieser Funktion kann iDRAC das System auf Konfigurationsereignisse, Angriffsereignisse (wie z. B. die bereits in diesem Whitepaper erwähnte Erkennung von Gehäuseangriffen) und Zustandsänderungen überwachen. Konfigurationsereignisse sind direkt mit der Identität des Nutzers verknüpft, der die Änderung initiiert hat, und zwar unabhängig davon, ob sie über die GUI, die API oder die Konsole vorgenommen wurde.

4.1.1 Lebenszyklusprotokoll

Das Lebenszyklusprotokoll ist eine Sammlung von Ereignissen, die in einem Server in einem bestimmten Zeitraum auftreten. Es enthält eine Beschreibung der Ereignisse mit Zeitstempel, Schweregrad, Nutzer-ID oder Quelle sowie empfohlene Maßnahmen und andere technische Informationen, die für Verfolgungs- oder Warnmeldungszwecke sehr nützlich sein könnten.

Nachfolgende Informationen werden im Lebenszyklusprotokoll erfasst:

- Konfigurationsänderungen an den Hardwarekomponenten des Systems
- Konfigurationsänderungen an iDRAC, BIOS, NIC und RAID
- Protokolle aller Remotevorgänge
- Historie der Firmwareupdates nach Gerät, Version und Datum
- Informationen über ausgetauschte Teile
- Informationen über fehlerhafte Teile
- Ereignis- und Fehlermeldungs-IDs
- Ereignisse zum Hostenergiestatus
- POST-Fehler
- Nutzeranmeldungsereignisse
- Ereignisse zu Sensorstatusänderungen

4.1.2 Warnmeldungen

iDRAC bietet die Möglichkeit, verschiedene Ereigniswarnmeldungen sowie Maßnahmen, die beim Auftreten eines bestimmten Ereignisses im Lebenszyklusprotokoll ausgeführt werden sollen, zu konfigurieren. Ein aufgetretenes Ereignis wird über die Mechanismen des ausgewählten Warnmeldungstyps an die konfigurierten Ziele weitergeleitet. Die Warnmeldungen können in der iDRAC-Weboberfläche, über RACADM oder mit dem Dienstprogramm für iDRAC-Einstellungen aktiviert bzw. deaktiviert werden.

iDRAC unterstützt verschiedene Arten von Warnmeldungen, darunter:

- E-Mail- oder IPMI-Warnung
- SNMP-Trap
- BS- und Remotesystemprotokolle
- Redfish-Ereignis

Warnmeldungen können auch nach Schweregrad kategorisiert werden, also Kritisch, Warnung oder Information.

Folgende Filter können auf Warnmeldungen angewendet werden:

- Systemzustand – z. B. Temperatur, Spannung oder Gerätefehler
- Storage-Zustand – z. B. Controller-Fehler, Fehler auf physischen oder virtuellen Laufwerken
- Konfigurationsänderungen – z. B. Änderung der RAID-Konfiguration, Entfernen von PCIe-Karten
- Auditprotokolle – z. B. Fehler bei der Kennwortauthentifizierung
- Firmware/Treiber – z. B. Upgrades oder Downgrade

Abschließend kann der IT-Administrator verschiedene Maßnahmen für Warnmeldungen festlegen, wie z. B. Neustart, Energiezyklus, Ausschalten oder keine Aktion.

4.2 Abweichungserkennung

Durch die Durchsetzung von Standardkonfigurationen und die Einführung einer „Null-Toleranz“-Policy für alle Änderungen können Unternehmen Exploit-Möglichkeiten reduzieren. Über die Dell EMC OpenManage Enterprise-Konsole können Kunden eine eigene Baseline für die Serverkonfiguration definieren und anschließend die Abweichung der Produktionsserver von dieser Baseline überwachen. Für die Erstellung der Baseline können verschiedene Kriterien herangezogen werden, um unterschiedliche Produktionsumsetzungen zu berücksichtigen, z. B. Sicherheit und Leistung. OpenManage Enterprise kann Abweichungen von der Baseline melden und diese optional mit einem einfachen Workflow beheben, um die Änderungen in iDRAC als „out-of-band“ einzustufen. Die Änderungen werden dann im nächsten Wartungsfenster im Rahmen des Serverneustarts übernommen – und damit ist die Compliance der Produktionsumgebung wiederhergestellt. Durch diesen schrittweisen Prozess können Kunden Konfigurationsänderungen für die Produktion bereitstellen, ohne dass Serverausfallzeiten außerhalb der Wartungsfenster entstehen. Das erhöht die Serververfügbarkeit, ohne Kompromisse bei Betriebsfähigkeit oder Sicherheit einzugehen.

5. Recovery

Serverlösungen müssen als Reaktion auf mehrere Ereignisse die Recovery auf einen bekannten, konsistenten Status unterstützen:

- Neu entdeckte Sicherheitslücken
- Bösartige Angriffe und Datenmanipulation
- Beschädigung der Firmware aufgrund von Arbeitsspeicherausfällen oder fehlerhaften Updateverfahren
- Austausch von Serverkomponenten
- Stilllegung oder neue Verwendung eines Servers

Nachfolgend wird ausführlich dargelegt, wie wir auf neue Sicherheitslücken und Probleme mit Beschädigungen reagieren und wie wir den Server ggf. in den Originalstatus zurückversetzen.

5.1 Schnelle Reaktion auf neue Sicherheitslücken

Häufige Sicherheitslücken und Anfälligkeiten (Common Vulnerabilities and Exposures, CVEs) sind neu entdeckte Angriffsvektoren, die Software- und Hardwareprodukte gefährden. Eine zeitnahe Reaktion auf CVEs ist für die meisten Unternehmen von entscheidender Bedeutung, damit sie die Gefährdung schnell einschätzen und entsprechende Maßnahmen ergreifen können.

CVEs können als Folge von neu erkannten Sicherheitslücken in zahlreichen Bereichen entstehen, darunter:

- Open-Source-Code wie OpenSSL
- Webbrowser und andere Software für den Internetzugang
- Hardware und Firmware für Anbieterprodukte
- Betriebssysteme und Hypervisoren

Dell EMC arbeitet mit Hochdruck an einer schnellen Reaktion der PowerEdge-Server auf neue CVEs und liefert Kunden zeitnah Informationen, wie z. B. die folgenden:

- Welche Produkte betroffen sind
- Welche Schritte zur Korrektur ergriffen werden können
- Wann Updates zur CVE-Behebung verfügbar sind (sofern erforderlich)

5.2 BIOS- und BS-Recovery

Die Dell EMC PowerEdge-Server der 14. und 15. Generation umfassen zwei Recovery-Typen: BIOS-Recovery und schnelle BS-Recovery (Betriebssystem). Mit diesen Funktionen ist die schnelle Recovery von beschädigten BIOS- oder BS-Images möglich. In beiden Fällen ist ein spezieller Storage-Bereich von der Laufzeitsoftware verborgen (BIOS, Betriebssystem, Gerätefirmware usw.). Diese Storage-Bereiche enthalten makellose Images, die als Alternative zur beschädigten Hauptsoftware verwendet werden können.

Die schnelle BS-Recovery ermöglicht die schnelle Recovery eines beschädigten BS-Image (oder eines BS-Image, bei dem der Verdacht auf eine bösartige Manipulation besteht). Als Datenträger für die Recovery können eine interne SD-Karte, SATA-Anschlüsse, M.2-Laufwerke oder ein interner USB-Anschluss fungieren. Das ausgewählte Gerät kann für die Bootliste und das Betriebssystem zur Installation des Recovery-Image verfügbar gemacht werden. Anschließend kann es deaktiviert und wieder aus der Bootliste und dem Betriebssystem ausgeblendet werden. Im ausgeblendeten Status wird das Gerät vom BIOS deaktiviert, damit das Betriebssystem nicht darauf zugreifen kann. Im Falle eines beschädigten BS-Image lässt sich der Recovery-Speicherort dann für den Bootvorgang aktivieren. Auf diese Einstellungen kann über das BIOS oder die iDRAC-Schnittstelle zugegriffen werden.

In extremen Fällen muss es bei einer BIOS-Beschädigung (entweder aufgrund eines bösartigen Angriffs, eines Stromausfalls im Updateprozess oder eines anderen unvorhergesehenen Ereignisses) die Möglichkeit geben, eine BIOS-Recovery auf den Originalstatus auszuführen. Ein Backup-BIOS-Image wird in iDRAC gespeichert, damit es bei Bedarf zur Recovery des BIOS-Image verwendet werden kann. iDRAC orchestriert den gesamten End-to-End-Recovery-Prozess.

- Die automatische BIOS-Recovery wird vom BIOS selbst initiiert.
- Die On-Demand-BIOS-Recovery kann von Nutzern über einen Befehl der RACADM-CLI gestartet werden.

5.3 Firmware-Rollback

Es wird empfohlen, die Firmware stets aktualisiert zu halten, um sicherzustellen, dass die neuesten Funktionen und Sicherheitsupdates vorhanden sind. Falls nach einem Update Probleme auftreten, muss möglicherweise jedoch ein Update-Rollback durchgeführt oder eine frühere Version installiert werden. Wird ein Rollback auf die vorherige Version durchgeführt, erfolgt auch eine Verifizierung anhand der Signatur.

Ein Firmware-Rollback von der vorhandenen Produktionsversion „N“ auf die vorherige Version „N-1“ wird derzeit für folgende Firmwareimages unterstützt:

- BIOS
- iDRAC mit Lifecycle Controller
- Netzwerkschnittstellenkarte (NIC)
- PowerEdge RAID-Controller (PERC)
- Stromversorgungseinheit
- Rückwandplatine

Für ein Firmware-Rollback auf die zuvor installierte Version („N-1“) können folgende Methoden verwendet werden:

- iDRAC-Weboberfläche
- CMC-Weboberfläche
- RACADM-CLI – iDRAC und CMC
- Lifecycle Controller-GUI
- Lifecycle Controller-Remoteservices

Ein Firmware-Rollback kann für iDRAC oder jedes von Lifecycle Controller unterstützte Gerät erfolgen, selbst wenn das Upgrade zuvor über eine andere Schnittstelle durchgeführt wurde. Wenn das Firmwareupgrade beispielsweise mit der Lifecycle Controller-GUI ausgeführt wurde, kann das Firmware-Rollback mithilfe der iDRAC-Weboberfläche durchgeführt werden. Mit einem einzigen Systemneustart lässt sich ein Firmware-Rollback für mehrere Geräte durchführen.

Auf den PowerEdge-Servern der 14. und 15. Generation, die über eine einzige iDRAC- und Lifecycle Controller-Firmware verfügen, erfolgt bei einem iDRAC-Firmware-Rollback stets auch ein Lifecycle Controller-Firmware-Rollback.

5.4 Wiederherstellung der Serverkonfiguration nach einer Hardwarewartung

Die Korrektur von Serviceereignissen ist ein wichtiger Bestandteil jedes IT-Betriebs. Die Fähigkeit, Recovery Time Objectives (RTOs) und Recovery Point Objectives (RPOs) einzuhalten, hat direkte Auswirkungen auf die Lösungssicherheit. Durch die Wiederherstellung der Serverkonfiguration und der Firmware wird die automatische Einhaltung der Sicherheits-Policies für den Serverbetrieb sichergestellt.

PowerEdge-Server bieten Funktionen, mit denen sich die Serverkonfiguration in den folgenden Situationen schnell wiederherstellen lässt:

- Austausch einzelner Teile
- Austausch der Hauptplatine (vollständiges Backup des Serverprofils und dessen Wiederherstellung)
- Austausch der Hauptplatine (einfache Wiederherstellung)

5.4.1 Austausch von Teilen

iDRAC speichert automatisch das Firmwareimage und die Konfigurationseinstellungen für NIC-Karten, RAID-Controller und Stromversorgungseinheiten. Im Falle eines Vor-Ort-Austauschs dieser Teile erkennt iDRAC automatisch die neue Karte und stellt die Firmware und Konfiguration auf der ausgetauschten Karte wieder her. Diese Funktion spart kritische Zeit und sorgt für eine konsistente Konfigurations- und Sicherheits-Policy. Das Update erfolgt automatisch beim Systemneustart nach dem Austausch des unterstützten Teils.

5.4.2 Einfache Wiederherstellung (nach Austausch der Hauptplatine)

Der Austausch von Hauptplatinen kann zeitaufwendig sein und die Produktivität beeinträchtigen. iDRAC bietet die Möglichkeit, ein Backup für die Konfiguration und die Firmware eines PowerEdge-Servers auszuführen und diese Daten wiederherzustellen, um den erforderlichen Aufwand beim Austausch einer ausgefallenen Hauptplatine zu minimieren.

Es gibt zwei Möglichkeiten für das Backup und die Wiederherstellung auf PowerEdge-Servern:

1. PowerEdge-Server führen automatisch ein Backup für die Systemkonfigurationseinstellungen (BIOS, iDRAC, NIC), das Service-Tag, die UEFI-Diagnose-App sowie andere lizenzierte Daten im Flash-Speicher aus.

   Nach dem Austausch der Hauptplatine im Server werden Sie von Easy Restore aufgefordert, diese Daten automatisch wiederherzustellen.

2. Für ein umfassenderes Backup können Nutzer die Systemkonfiguration sichern, einschließlich der installierten Firmwareimages auf verschiedenen Komponenten (wie z. B. BIOS, RAID, NIC, iDRAC, Lifecycle Controller und Netzwerktochterkarten (Network Daughter Cards, NDCs)) und der Konfigurationseinstellungen dieser Komponenten. Der Backupvorgang umfasst auch die Festplattenkonfigurationsdaten, die Hauptplatine und ausgetauschte Teile. Im Rahmen des Backups wird eine einzelne Datei erstellt, die auf einer vFlash-SD-Karte oder über eine Netzwerkfreigabe (CIFS, NFS, HTTP oder HTTPS) gespeichert werden kann.

   Dieses Profilbackup lässt sich jederzeit von den Nutzern wiederherstellen. Dell EMC empfiehlt, den Backupvorgang für jedes Systemprofil durchzuführen, das möglicherweise irgendwann einmal wiederhergestellt werden soll.

5.5 SystemErase

Am Lebenszyklusende eines Systems steht entweder die Stilllegung oder die neue Verwendung. SystemErase hat das Ziel, sensible Daten und Einstellungen aus Storage-Geräten und aus dem nichtflüchtigen Speicher des Servers (wie z. B. Caches und Protokolle) zu löschen, damit nicht versehentlich vertrauliche Informationen offengelegt werden. Es handelt sich um ein Dienstprogramm im Lifecycle Controller, mit dem Protokolle, Konfigurationsdaten, Storage-Daten, Cache und eingebettete Anwendungen gelöscht werden können.

Folgende Geräte, Konfigurationseinstellungen und Apps lassen sich mit der SystemErase-Funktion löschen:

- Zurücksetzung von iDRAC auf die Standardeinstellungen
- LC-Daten (Lifecycle Controller)
- BIOS
- Integrierte Diagnose und BS-Treiberpakete
- iSM
- SupportAssist-Erfassungsberichte

Außerdem können folgende Komponenten gelöscht werden:

- Hardware-Cache (gelöschter PERC NV-Cache)
- vFlash-SD-Karte (Karteninitialisierung) (Hinweis: vFlash ist nicht verfügbar für Server der 15. Generation oder höher.)

Die Daten auf folgenden Komponenten werden wie nachfolgend beschrieben von SystemErase „kryptografisch entsorgt“:

- SED (selbstverschlüsselnde Festplatte)
- Reine ISE(Instant Secure Erase)-Festplatten
- NVM-Geräte (Apache Pass, NVDIMMs)

Darüber hinaus lassen sich SATA-Festplatten ohne ISE mittels einer Datenüberschreibung löschen.

Hinweis: Instant Secure Erase (ISE) zerstört den internen Verschlüsselungsschlüssel, der in den Festplatten der 14. und 15. Generation verwendet wird, sodass die Nutzerdaten nicht wiederherstellbar sind. ISE ist eine anerkannte Methode zur Datenlöschung auf Storage-Laufwerken, auf die in der NIST Special Publication 800-88 „Guidelines for Media Sanitization“ verwiesen wird.

Die neue ISE-Funktion mit SystemErase bietet folgende Vorteile:

- **Geschwindigkeit**: ISE ist viel schneller als Datenüberschreibungsverfahren wie z. B. DoD 5220.22-M (Sekunden im Vergleich zu Stunden).
- **Effektivität**: Mit ISE werden alle Daten auf dem Laufwerk, einschließlich reservierter Blöcke, vollständig unlesbar.
- **Bessere Gesamtbetriebskosten (TCO)**: Storage-Geräte können wiederverwendet werden, anstatt sie zu zerkleinern oder anderweitig physisch zu zerstören.

SystemErase kann mit folgenden Methoden durchgeführt werden:

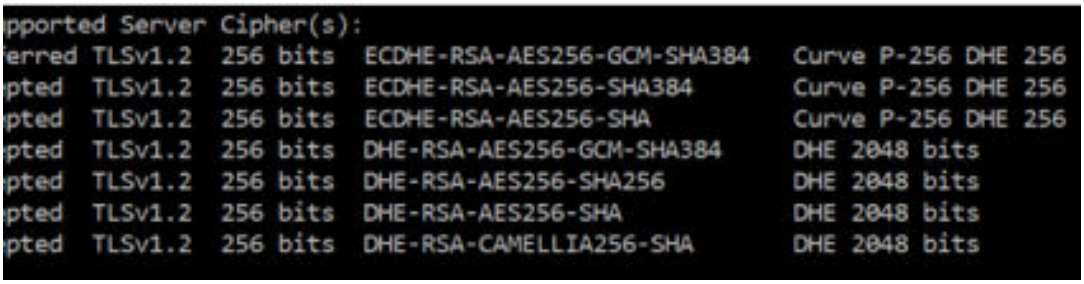
- Lifecycle Controller-GUI (F10)
- RACADM-CLI
- Redfish

5.6 iDRAC9 Cipher Select

Über die Cipher-Suite-Auswahl können die Chiffren, die der Webbrowser für die Kommunikation mit iDRAC verwenden darf, eingeschränkt werden. Zudem lässt sich damit bestimmen, wie sicher die Verbindung ist. Diese Einstellungen erfolgen über die iDRAC-Weboberfläche, RACADM und Redfish. Die Funktion ist für mehrere iDRAC-Versionen verfügbar – iDRAC7, iDRAC8 (2.60.60.60 und höher) und die aktuelle Version iDRAC9 (3.30.30.30 und höher).

5.7 CNSA-Support

Auf dem Screenshot werden die unterstützten Chiffren abgebildet, die in iDRAC9 mit TLS 1.2 und 256-Bit-Verschlüsselung verfügbar sind. Die verfügbaren Chiffren enthalten auch die Chiffren im CNSA-zertifizierten Satz.



5.8 Vollständiger Energiezyklus

Bei einem vollständigen Energiezyklus werden sowohl der Server als auch alle Komponenten neu gestartet. Vom Server und all seinen Komponenten wird die Haupt- sowie die Hilfsenergie abgezogen. Alle Daten in flüchtigem Speicher werden ebenfalls gelöscht.

Für einen physischen vollständigen Energiezyklus muss das Netzkabel abgezogen werden. Nach Ablauf von 30 Sekunden kann das Netzkabel wieder eingesteckt werden. Bei einem Remotesystem stellt das eine Herausforderung dar. Mit der neuen Funktion „Full Power Cycle“ in den Servern der 14. und 15. Generation kann ein effektiver vollständiger Energiezyklus auch über iSM, iDRAC-GUI, BIOS oder ein Skript durchgeführt werden. Der vollständige Energiezyklus findet dann beim nächsten Energiezyklus statt.

Dank der Funktion „Full Power Cycle“ entfällt die Notwendigkeit der physischen Anwesenheit im Rechenzentrum, wodurch die Zeit für Troubleshooting verkürzt wird. So lässt sich beispielsweise Malware, die noch im Arbeitsspeicher verblieben ist, eliminieren.

6. Fazit

Die Rechenzentrumssicherheit ist von höchster Wichtigkeit für den geschäftlichen Erfolg – und die Sicherheit der zugrunde liegenden Serverinfrastruktur ist von entscheidender Bedeutung. Cyberangriffe könnten möglicherweise längere System- und Geschäftsausfälle sowie Umsatzverluste und Kundenabwanderung, rechtliche Schäden und eine Rufschädigung des Unternehmens verursachen. Zum Schutz vor und zur Erkennung von hardwarespezifischen Cyberangriffen sowie zur Recovery muss die Sicherheit in das Design der Serverhardware integriert sein, anstatt nachträglich „eingebaut“ zu werden.

Dell EMC ist Vorreiter bei der Nutzung von chipbasierter Sicherheit zum Schutz der Firmware und von sensiblen Nutzerdaten und setzt diese bereits in den letzten zwei Generationen der PowerEdge-Server ein. Die PowerEdge-Produktlinien der 14. und 15. Generation verfügen über eine erweiterte cybersichere Architektur, die mithilfe von chipbasierter Root of Trust die Serversicherheit erhöht und folgende Funktionen umfasst:

- **Kryptografisch verifiziertes Trusted Booting** – verankert die End-to-End-Serversicherheit und die allgemeine Rechenzentrumssicherheit mithilfe von Funktionen wie chipbasierte Root of Trust, digital signierte Firmware und automatische BIOS-Recovery.
- **Secure Boot** – überprüft die kryptografischen Signaturen von UEFI-Treibern und anderem Code, der vor der BS-Ausführung geladen wurde.
- **iDRAC-Zugangsdaten-Vault** – ist ein sicherer Speicherplatz für Zugangsdaten, Zertifikate und andere sensible Daten, die mit einem chipbasierten Schlüssel verschlüsselt werden, der für jeden Server eindeutig ist.
- **Dynamische Systemsperre** – ist eine einzigartige PowerEdge-Funktion, die jede Systemkonfiguration und Firmware vor bösartigen oder unabsichtlichen Änderungen schützt und die Nutzer mit Warnmeldungen über jedwede versuchte Systemänderung informiert.
- **Enterprise-Key-Management** – bietet eine zentrale Key-Managementlösung für das Data-at-Rest-Management im gesamten Unternehmen.
- **SystemErase** – bietet Nutzern dank der sicheren und schnellen Löschung von Daten auf Storage-Geräten und aus anderen eingebetteten, nichtflüchtigen Speicheroptionen die Möglichkeit, ihre PowerEdge-Server der 14. und 15. Generation ganz einfach stillzulegen oder einer neuen Verwendung zuzuführen.
- **Sicherheit der Lieferkette** – sorgt durch die Sicherstellung, dass keine Produktmanipulation stattfindet und keine gefälschten Komponenten in das Produkt gelangen, bevor es an Kunden ausgeliefert wird, für die Lieferkettensicherheit.

Zusammenfassend kann gesagt werden, dass die PowerEdge-Server der 14. und 15. Generation mit ihrer branchenführenden Sicherheit eine vertrauenswürdige Basis für die IT-Transformation bieten, auf der Kunden ihren IT-Betrieb und ihre Workloads sicher ausführen können.

A. Anhang: Weitere Informationen

Sicherheit – Whitepaper und Begleitmaterialien

- (Direkt aus der Entwicklung) SYSTEMERASE AUF POWEREDGE-SERVERN
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444242
- SCHUTZ VON DELL EMC POWEREDGE-SERVERN DER 14. GENERATION MIT SYSTEMERASE
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444269
- (Direkt aus der Entwicklung) SICHERHEIT IM SERVERDESIGN
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444243
- (Direkt aus der Entwicklung) CYBERSICHERHEIT BEGINNT BEI CHIPSATZ UND BIOS
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444061
- WERKSEITIG GENERIERTES iDRAC9-STANDARDKENNWORT
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444368
- DIE ANTWORT VON DELL EMC iDRAC AUF CVE-2017-1000251 „BLUEBORNE“
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444605
- (Video) SECURE BOOT-KONFIGURATION UND ZERTIFIKATSMANAGEMENT MIT RACADM
  https://youtu.be/mrIIN4X380c
- SECURE BOOT-MANAGEMENT AUF DELL EMC POWEREDGE-SERVERN
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444259/download
- Signieren von UEFI-Images für die Secure Boot-Funktion in Dell EMC PowerEdge-Servern der 14. und 15. Generation und höher
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444255
- SCHNELLE RECOVERY DES BETRIEBSSYSTEMS
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444249
- Management von iDRAC9-Ereigniswarnungen auf Dell EMC PowerEdge-Servern der 14. Generation (14G)
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444266
- UEFI Secure Boot Customization
  https://media.defense.gov/2020/Sep/15/2002497594/-1/-1/0/CTR-UEFI-Secure-Boot-Customization-UOO168873-20.PDF

Whitepaper für PowerEdge

- iDRAC – Übersicht
  http://www.DellTechCenter.com/iDRAC
- OpenManage Console – Übersicht
  http://www.DellTechCenter.com/OME
- OpenManage Mobile – Übersicht
  http://www.DellTechCenter.com/OMM
- Lifecycle Controller – Austausch von Teilen
  http://en.community.dell.com/techcenter/extras/m/white_papers/20276457
- Austausch der Hauptplatine
  http://en.community.dell.com/techcenter/extras/m/white_papers/20168832
- iDRAC – automatische Zertifikatregistrierung
  https://www.dellemc.com/resources/de-de/asset/white-papers/products/software/direct-from-development-idrac-automatic-certificate-enrollment.pdf
- Verbesserte Serversicherheitsfunktionen in iDRAC9 mit SELinux
  https://downloads.dell.com/manuals/all-products/esuprt_solutions_int/esuprt_solutions_int_solutions_resources/dell-management-solution-resources_white-papers20_en-us.pdf
- iDRAC9 Cipher Select – verbesserte Sicherheit für Dell EMC PowerEdge-Server
  https://downloads.dell.com/manuals/all-products/esuprt_software_int/esuprt_software_ent_systems_mgmt/idrac9-lifecycle-controller-v33-series_white-papers11_en-us.pdf

Weitere Informationen über PowerEdge-Server

Weitere Informationen über unsere Dell PowerEdge-Server

Weitere Informationen zu unseren Systemmanagement-lösungen

Durchsuchen Sie unsere Ressourcenbibliothek

Folgen Sie PowerEdge-Server auf Twitter

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

DELL Technologies