DELL Technologies

AMD
together we advance_

Whitepaper

Sichern der digitalen Grenze: Der Zero-Trust-Ansatz von Dell und AMD

Schützen Sie Ihr Unternehmen mit der End-to-End-Sicherheit von Dell und AMD

Inhaltsverzeichnis

Einführung

Die Geräte, die uns verbinden, ermöglichen Unglaubliches. Diese Verbindungen verursachen jedoch auch zusätzliche Sicherheitslücken, die bösartige AkteurInnen ausnutzen können. Manchen Schätzungen zufolge werden Cyberangriffe Unternehmen bis 2025 ganze 10,5 Billionen USD kosten.[1] Laut einer Schätzung dauert die Wiederherstellung nach einem Cyberangriff rund 277 Tage.[2]

Neuere Technologien wie KI (künstliche Intelligenz) optimieren in vielen Unternehmen die Produktivität und den Geschäftsbetrieb, machen Daten aber auch anfällig für ausgefeiltere Cyberangriffe. Mit jedem technologischen Fortschritt müssen Führungskräfte der Technologiebranche ihre Strategien ändern, um Cyberkriminellen effektiv entgegenzuwirken, wenn diese neue Wege finden, an Daten zu gelangen und sie auszunutzen. Um diese Bedrohungen abzuwehren und Daten zu schützen, benötigt jede Komponente des Rechenzentrums – von Servern und Storage bis hin zu Netzwerken, Software und Firmware – einen integrierten Schutz. Dieser Schutz beginnt mit der Eindämmung von Lieferkettenmanipulationen in der Fertigung und setzt sich während des Transports und der Kundennutzung fort. Angriffe beschränken sich außerdem nicht mehr nur auf das Rechenzentrum. Unternehmen mit Präsenz in der Cloud stehen bei der Sicherung ihrer Daten vor zusätzlichen Herausforderungen.

Dell und AMD bieten gemeinsam eine speziell entwickelte, cybersichere Architektur, die Unternehmen bei der Einführung einer Zero-Trust-Strategie unterstützt. Dabei wird davon ausgegangen, dass Systemkomponenten an jedem Glied der Kette anfällig sind und an jedem Punkt Schutz benötigen. Eine Zero-Trust-Strategie basiert auf starken, identitätsbasierten Richtlinien für alle IT-Bestände sowie auf den Prinzipien des Zugriffs mit den geringsten Berechtigungen. Die cybersichere Architektur von Dell bietet umfassende Funktionen rund um Startintegrität und Data Protection sowie Sicherheitsfunktionen in iDRAC (integrated Dell Remote Access Controller). Dell PowerEdge-Server sind mit einer chipbasierten Root of Trust (RoT) verankert, die eine Vertrauenskette für die kryptografische Überprüfung von Hardware- und Softwarekomponenten auf dem Server einrichtet. AMD Infinity Guard bietet eine zusätzliche Sicherheitsebene, die potenzielle Angriffe beim Starten und Ausführen von Software verringert. AMD Infinity Guard umfasst mehrere zusätzliche Sicherheitsfunktionen, einschließlich Platform Secure Boot und Platform Secure Processor, die sicherstellen, dass PowerEdge-Server in jeder Phase ihres Lebenszyklus geschützt sind.

Cybersichere Architektur von Dell

Die cybersichere Architektur von Dell nutzt PowerEdge-Sicherheitsfunktionen, die zusammenarbeiten, um sowohl Ausfallsicherheit zu bieten als auch eine Zero-Trust-Strategie zu ermöglichen. Sicherheitsfunktionen müssen vor potenziellen Bedrohungen schützen, verdächtige Aktivitäten erkennen und im Falle einer Sicherheitsverletzung eine schnelle Wiederherstellung ermöglichen. Gleichzeitig müssen sie nach dem Motto „Vertrauen ist gut, Kontrolle ist besser“ einen Zero-Trust-Ansatz mit den geringsten Berechtigungen bereitstellen, bei dem NutzerInnen und Geräten nur Zugriff auf das gewährt wird, was sie zur Durchführung ihrer Aufgaben benötigen. Dank ihrer Zusammenarbeit bieten diese PowerEdge-Sicherheitskontrollen eine umfassende Sicherheitslösung, die für Ausfallsicherheit sorgt und gleichzeitig einen Zero-Trust-Status durchsetzt. Weitere Informationen zu den vollständigen Funktionen und Services der cybersicheren Architektur von Dell finden Sie im Whitepaper.

Sicherstellen der Startintegrität

Die Pre-Boot-Umgebung wird oft übersehen und kann, wenn keine Sicherheitsvorkehrungen getroffen werden, anfällig für Angriffe sein. Wenn bösartige AkteurInnen das BIOS, die Firmware oder einen Treiber während des Startvorgangs infizieren, können Sie möglicherweise Zugriff auf das gesamte System erhalten. Ohne die richtigen Kontrollen könnten sie das System jederzeit erfolgreich infiltrieren und ihr gewünschtes Ziel erreichen: Ihre Daten.

Um Sicherheitslücken zu minimieren, muss der Serveranbieter nicht nur das BIOS schützen, sondern auch bestimmte Serverkomponenten und Firmware wie Arbeitsspeicher und Prozessoren überprüfen und validieren. Hersteller von Serverhardware müssen sicherstellen, dass sich ihre Komponenten vollständig in die Serverarchitektur integrieren lassen, damit Sicherheits- und Validierungsprüfungen nahtlos funktionieren. Jeder Dell PowerEdge-Server bietet mehrere Sicherheitsebenen zum Schutz des Startzyklus: chipbasierte RoT, UEFI Secure Boot und iDRAC-Sicherheitsfunktionen, einschließlich Firmwarerollback und schneller Betriebssystem-Recovery.

Zusätzlich zu diesen serverbasierten Sicherheitsebenen von Dell PowerEdge verfügen AMD-Prozessoren über Platform Secure Boot (PSB) und Platform Security Processor (PSP) für den Schutz verwendeter Daten. Dell und AMD decken gemeinsam jeden Aspekt des Startzyklus ab, um eine sichere Grundlage für Ihre Daten und Workloads sicherzustellen.

[1] Chuck Brooks, „Cybersecurity Trends & Statistics For 2023; What You Need to Know“, abgerufen am 4. Dezember 2023, https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=9885ce219dba.

[2] Ken Kizzee, „Cyber Attack Statistics to Know“, abgerufen am 19. Dezember 2023, https://parachute.cloud/cyber-attack-statistics-data-and-trends/.

Dell iDRAC und Root of Trust

Beim RoT-Konzept wird davon ausgegangen, dass bei einem System, das ein Fundament oder eine Baseline als sicher verifiziert, alle nachfolgenden Validierungen und Sicherheitsprüfungen in einer kontinuierlichen Vertrauenskette verankert sind. Stellen Sie sich ein Haus vor: Wenn das Fundament instabil ist und zu bröckeln beginnt, spielt die Integrität der Mauerstütze keine Rolle. Wenn das BIOS Ihres Servers kompromittiert wird, kann der Schutz des Serverbetriebssystems ebenfalls vergeblich sein.

Die Vertrauenskette für PowerEdge-Server bietet eine nahtlose kryptografische Verifizierung aller Serverkomponenten von der Grundlage bis zu den Daten. Damit wird sichergestellt, dass die Komponenten des Systemsoftware-Stacks (Hypervisor, BS, Anwendungen) wissen, dass sie dem zugrunde liegenden Server vertrauen können, wenn der Server in Betrieb ist. Diese Schicht bildet die Grundlage für eine Vertrauenskette innerhalb eines Servers und schafft eine vertrauenswürdige und sichere Serverplattform. Dell Server verwenden eine einzigartige chipbasierte RoT, die zur kryptografischen Verifizierung in jeden Server eingebrannt ist und bei jedem Kaltstart oder Ein- und Ausschaltzyklus für einen sicheren Start sorgt. Ab Version 4.10.10.10 bietet iDRAC einen RoT-Mechanismus zur Überprüfung des BIOS-Image beim Start und lässt den Server erst dann starten, nachdem das BIOS-Image verifiziert wurde. Bei PowerEdge-Servern mit AMD-Prozessoren nutzt iDRAC (Integrated Dell Remote Access Controller) die AMD PSB-Technologie, um den BIOS-Code zu überprüfen, bevor das Betriebssystem geladen wird. AMD PSB prüft die BIOS-Integrität und stellt eine Schnittstelle mit dem primären BIOS-ROM und dem AMD Fusion Controller Hub (FCH) für eine gründliche RoT-Verarbeitung her. Diese akribische Validierung erstreckt sich bis zum BS-Bootloader und stellt eine kontinuierliche Vertrauenskette sicher.

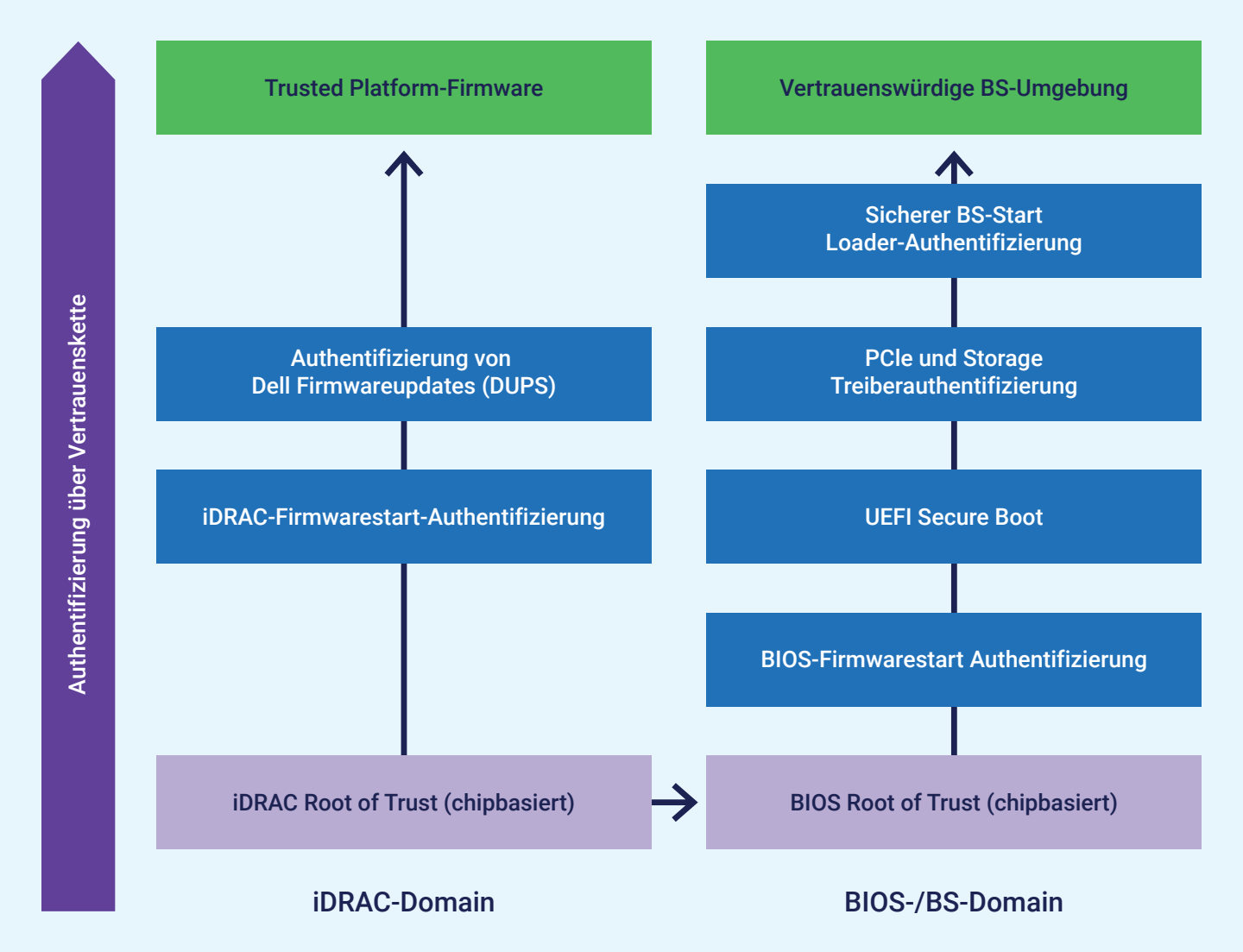

Abbildung 1: Chipbasierte Root-of-Trust-Domains in PowerEdge-Servern mit iDRAC9

Sollte die BIOS-Validierung fehlschlagen, fährt iDRAC den Server sofort herunter und benachrichtigt den/die NutzerIn, um das Starten nicht autorisierter Firmware zu verhindern. iDRAC enthält außerdem ein Backup- und Recovery-System für BIOS- und iDRAC-Firmware, das die Ausfallsicherheit des Servers erhöht und den Serverbetrieb vor potenziellen Firmwarebeschädigungen schützt. Für zusätzlichen Schutz bietet iDRAC darüber hinaus einen Live-BIOS-Scan, den NutzerInnen nach Bedarf oder nach einem regelmäßigen Zeitplan ausführen können. Dieser Scan erfordert die iDRAC Datacenter-Lizenz und ermöglicht es NutzerInnen, potenzielle Probleme vor dem Neustart zu erkennen, sodass eine proaktive Abwehr ermöglicht wird.[3]

UEFI Secure Boot

Dell PowerEdge-Server verwenden den Branchenstandard UEFI Secure Boot, um betriebssystemspezifische Bootloader zu validieren und so die Integrität des BS-Kernels und anderer wichtiger Komponenten sicherzustellen. UEFI dient in Pre-Boot-Umgebungen als Schutz vor Malware und Ransomware. Um die Interoperabilität sicherzustellen, müssen sowohl Server- als auch Komponentenhersteller zusammenarbeiten, damit das UEFI-fähige BIOS Treiber- und Firmwaresignaturen für Komponenten erkennen kann. Durch die Validierung der kryptografischen Signaturen von UEFI-Treibern und anderem Code vor dem Laden des BS versucht UEFI Secure Boot sicherzustellen, dass jeder während des Startvorgangs geladene Code frei von bösartigen Inhalten ist.

Für eine verstärkte Sicherheitsanpassung können AdministratorInnen kundenspezifische BS-Bootloader-Signaturzertifikate für UEFI Secure Boot konfigurieren. (Weitere Informationen zu den Anpassungsoptionen für UEFI Secure Boot finden Sie unter https://infohub.delltechnologies.com/section-assets/direct-from-development-uefi-boot-enhanced-security-to-combat-threats.) Damit wird die Ausführung auf vertrauenswürdige, sichere BS-Bootloader begrenzt, die die Secure Boot-Kette aufrechterhalten, indem sie den BS-Kernel und das Dateisystem authentifizieren. Diese Funktion bietet zusätzliche Flexibilität, insbesondere für Linux-AdministratorInnen, die ihre eigenen BS-Bootloader signieren möchten, statt sich auf standardmäßige UEFI-Drittanbieterzertifizierungsstellen zu verlassen. AdministratorInnen können kundenspezifische Zertifikate über die iDRAC-API hochladen und so die Authentifizierung ihrer spezifischen BS-Bootloader verbessern. Dell PowerEdge-Server unterstützen in einzigartiger Weise die vollständige Anpassung von Secure Boot, einschließlich der Option zum Entfernen aller Standardzertifikate von Microsoft, VMware oder UEFI CA.[4]

CPLD-Validierung

Jeder Dell PowerEdge-Server validiert das Complex Programmable Logic Device (CPLD) bei jedem Ein- und Ausschalten. CPLD, ein vielseitiges programmierbares Logikgerät[5], besteht aus mehreren einfachen PLDs, die durch eine programmierbare Switching-Matrix verbunden sind. Die Firmware, die in der Regel im EEPROM, Flash-Speicher oder SRAM gespeichert ist, ermöglicht Änderungen an den Funktionen der Hauptplatine über die BIOS-Funktionen hinaus, einschließlich der Implementierung einer speziellen Logik für Geräteinteraktionen auf der Hauptplatine. Die CPLD-Validierung stellt sicher, dass Änderungen an der Hauptplatine weder Ihre Server noch Ihre Daten beschädigen.

iDRAC-Hardwaresicherheit

Bei der Erweiterung der Vertrauenskette auf zusätzliche Hardwarekomponenten verwendet iDRAC SPDM (Security Protocol and Data Model), um zu standardisieren, wie Server Informationen über ihre Komponenten sammeln. Die Identitäts-, Firmware- und Konfigurationsinformationen jeder Komponente werden verschlüsselt. Die iDRAC-Hardwaresicherheit verwendet einen authentifizierten Schlüsselaustausch, um die Kommunikationswege zwischen Komponenten und iDRAC zu sichern. Mit SPDM kann iDRAC die Gültigkeit von Komponenten wie PowerEdge-RAID-Controller (PERC) 12 und Netzwerkschnittstellenkarten (NICs) authentifizieren. Dadurch wird nicht nur die Serversicherheit dank Authentifizierung der Geräteidentitätszertifikate der Komponenten erhöht, sondern NutzerInnen werden auch bei Authentifizierungsfehlern gewarnt.

[3] Dell, „Improved security with iDRAC9 using Root of Trust and BIOS Live Scanning“, abgerufen am 19. Dezember 2023, https://dl.dell.com/manuals/common/dell-emc-idrac9-security-root-of-trust-bios-live-scanning.pdf.

[4] Dell, „Cyber Resilient Security in Dell PowerEdge Servers“, abgerufen am 4. Dezember 2023, https://www.delltechnologies.com/asset/en-us/products/servers/industry-market/cyber-resilient-security-with-poweredge-servers.pdf.

[5] Technopedia, „Complex Programmable Logic Device“, abgerufen am 4. Dezember 2023, https://www.techopedia.com/definition/6655/complex-programmable-logic-device-cpld.

AMD Platform Secure Boot

AMD-Prozessoren verfügen über AMD Platform Secure Boot (PSB), um einem weiteren wachsenden Problem in der heutigen digitalen Landschaft entgegenzuwirken: Bedrohungen auf Firmwareebene. PSB nutzt die chipbasierte RoT von AMD und überprüft den Startvorgang vom BIOS-Code bis zum BS-Bootloader über UEFI Secure Boot.[6] Dell verwendet AMD PSB-fähige Hauptplatinen, damit nur der eigene kryptografisch signierte BIOS-Code ausgeführt werden kann. Darüber hinaus bindet Dell jeden AMD-Prozessor an eine spezifische Hauptplatine mit einmalig programmierbaren Sicherungen, die den Prozessor mit den Codesignierungsschlüsseln der Dell Firmware verknüpfen.[7] Zum Schutz vor Angriffen, die darauf abzielen, Malware in die Firmware einzubetten, wird beim Starten mit PSB nur Firmware autorisiert, die von AMD Secure Processor authentifiziert wurde.[8]

Durch die kryptografische Überprüfung des Software-Stacks bietet AMD Platform Secure Boot eine wesentliche Schutzschicht gegen unbefugtes Eindringen über verschiedene Plattformen hinweg, insbesondere in virtualisierten Umgebungen oder in der Cloud.

AMD Platform Secure Processor

Zusammen mit PSB sichert AMD Platform Secure Processor (PSP) den Startvorgang des Dell PowerEdge-Servers weiter ab. Wenn eine CPU im Dell Werk zum ersten Mal eingeschaltet wird, bettet AMD Platform Secure Processor dauerhaft eine eindeutige Dell ID in die CPU ein. Diese ID verknüpft die CPU quasi mit dem PowerEdge-Server und schafft so eine sichere Bindung.[9]

Durch diese Integration verhindert PSP, dass ein PowerEdge-Server gestartet wird, wenn eine CPU von einem anderen Server erkannt wird. CPU-Portabilität ist jedoch im Falle eines Hardwarefehlers weiterhin möglich. Der AMD-Prozessor ist an den Signaturschlüssel des Anbieters statt an die Hauptplatine gebunden, was ein ausgewogenes Verhältnis zwischen Sicherheit und Komponentenmobilität bietet.[10]

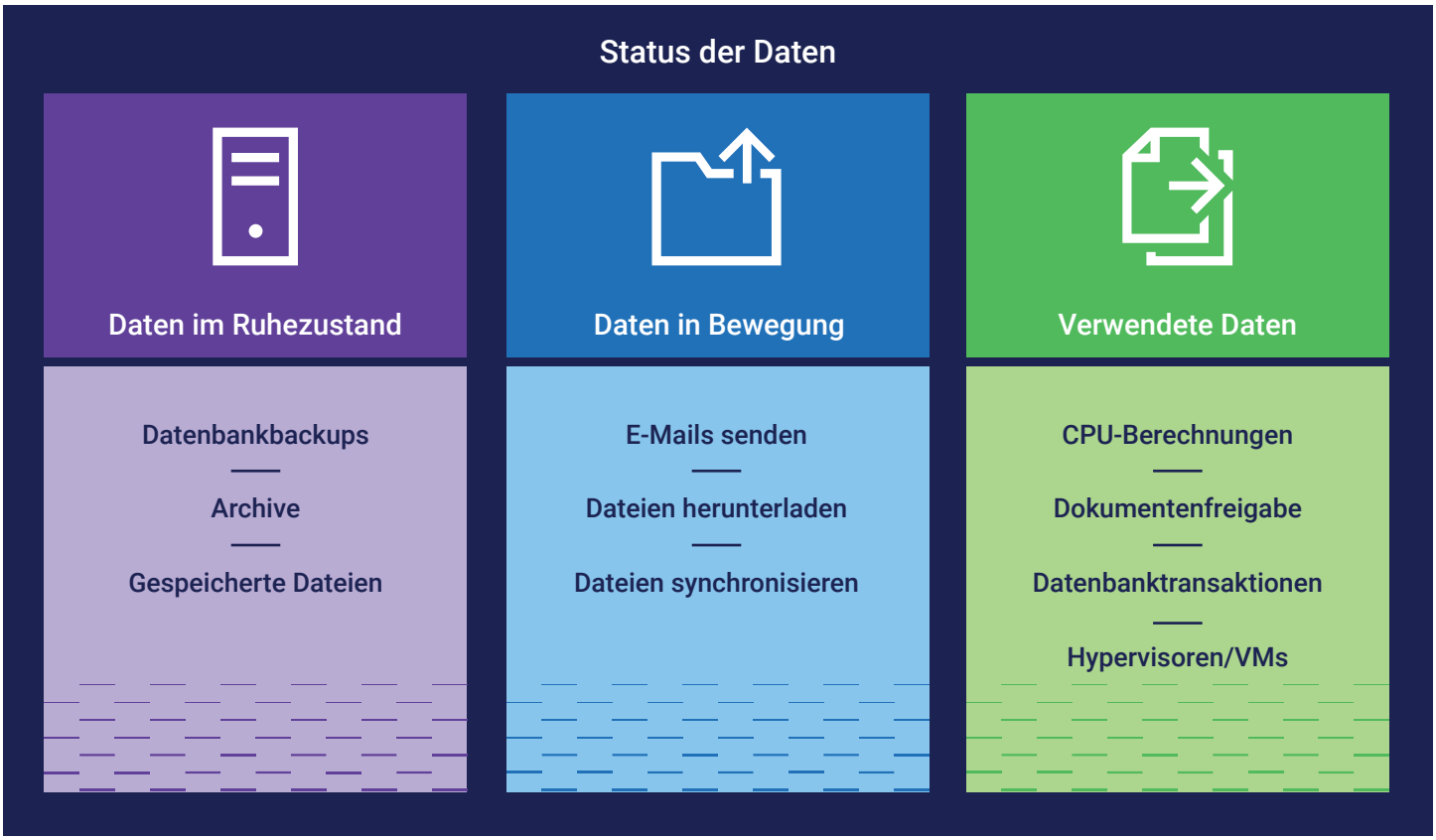

Abbildung 2: Status der Daten

[6] AMD, „AMD Pro Security“, abgerufen am 4. Dezember 2023, https://www.amd.com/en/technologies/pro-security.
[7] AMD, „AMD Infinity Guard“, abgerufen am 4. Dezember 2023, https://www.amd.com/en/technologies/infinity-guard.
[8] AMD, „4 Ways AMD Infinity Guard Helps Protect Your Data“, abgerufen am 4. Dezember 2023, https://www.amd.com/system/files/documents/content-security-infographic.pdf.
[9] AMD, „AMD Infinity Guard“.
[10] Dell, „Defense in-depth: Comprehensive Security on PowerEdge AMD EPYC Generation 2 (Rome) Servers“, abgerufen am 4. Dezember 2023, https://infohub.delltechnologies.com/p/defense-in-depth-comprehensive-security-on-poweredge-amd-epyc-generation-2-rome-servers/.

Schutz Ihrer Daten

Wenn AngreiferInnen Zugriff auf Systeme erhalten, ist das Endziel immer identisch: Ihre Daten zu finden und sie zu stehlen, zu manipulieren, zu verkaufen oder zu vernichten. Der physische Server ist nicht die einzige Schwachstelle. Böswillige AkteurInnen können Netzwerke angreifen, IT-Richtlinien können Fehler enthalten, EndnutzerInnen können schwache Kennwörter verwenden und IT-Teams können zu umfangreiche Zugriffsberechtigungen festlegen. AngreiferInnen können NutzerInnen mit Phishing-E-Mails angreifen, um Malware zu verbreiten.

Dell ermöglicht Kunden die Anwendung eines Zero-Trust-Ansatzes, der sich auf mehrere Sicherheitsebenen verlässt, um vor all diesen Arten von Sicherheitslücken zu schützen. Zum Schutz vor Diebstahl oder Kompromittierung müssen Sie ruhende Daten, Daten während der Verarbeitung und In-Flight-Daten bis hin zur Außerbetriebnahme von Daten sichern.[11] Mit Funktionen wie At-Rest-Verschlüsselung, einem robusten Chiffrierschlüssel-Management und automatisierter Zertifikatsverlängerung blockieren, verhindern und mindern Dell PowerEdge-Server bösartige Angriffe nach dem ersten Start. Dell PowerEdge-Server mit AMD-Prozessoren bieten zusätzliche Funktionen zur Stärkung der Sicherheit, einschließlich AMD Secure Memory Encryption (SME) und Secure Encrypted Virtualization (SEV).

Ruhende Daten

Zum Schutz von ruhenden Daten bietet Dell drei Hauptsicherheitsfunktionen: softwarebasierte Verschlüsselung, Enterprise-Key-Management und Verschlüsselung von Hardwarelaufwerken. Mit Laufwerken, die Instant Secure Erase (ISE) unterstützen, können Dell Kunden kryptografisch alle Daten auf selbstverschlüsselnden Festplatten (SEDs), ISE-Laufwerken und NVM-Geräten wie NVDIMMs löschen. SEDs schützen Daten vor Angriffen in Fällen, in denen verärgerte MitarbeiterInnen oder andere bösartige AkteurInnen Laufwerke physisch aus einem Server entfernen. Da das Sperrschlüsselkennwort des verschlüsselten Laufwerks dieses mit dem spezifischen Server und RAID-Controller verknüpft, von dem es stammt, kann ein anderer Server nicht auf die Daten zugreifen. Für weiteren Schutz kann iDRAC Dell OpenManage Secure Enterprise Key Manager mit lokalem Key-Management (iLKM, LKM) verwenden, das in Verbindung mit einem externen Key-Manager von Drittanbietern arbeitet, um den Storage-Controller beim Starten zu sperren und entsperren. Wenn jemand den Server außerhalb des Key-Managers startet, hält iDRAC die Sperre des Storage-Controllers aufrecht, sodass die auf dem Gerät gespeicherten Daten verschlüsselt bleiben. Weitere Informationen zu anderen Optionen für Verschlüsselungsschlüssel finden Sie unter https://infohub.delltechnologies.com/section-assets/openmanage-sekm-storage-performance-infographic.

In-Flight-Daten

Bei In-Flight-Daten können AngreiferInnen aufgrund von Sicherheitslücken im Netzwerk und bei der Datenzugriffskontrolle Daten abfangen oder ändern, die über das Netzwerk übertragen werden. Die iDRAC-Webverbindung ist ein möglicher Schwachpunkt. Daher bietet Dell mehrere Optionen an, um die Verbindung mit einem TLS-/SSL-Zertifikat zu sichern und so die Angriffsgefahr zu verringern. Obwohl dieses Zertifikat standardmäßig selbstsigniert ist, können AdministratorInnen ein kundenspezifisches Zertifikat oder ein von einer vertrauenswürdigen Zertifizierungsstelle (CA) signiertes Zertifikat erstellen. Dieses Zertifikat ermöglicht verschlüsselte, sichere Verbindungen, mit denen Webbrowser und Tools wie Befehlszeilendienstprogramme sicher über die iDRAC-Verbindung mit dem Server interagieren können.

iDRAC bietet außerdem mehrere Steuerelemente, über die NutzerInnen strenge, eng gefasste Zugriffsregeln ändern können, die einen SSH-Zugriff auf den Server erlauben. Für iDRAC-NutzerInnen mit einer Datacenter-Lizenz bietet iDRAC Simple Certificate Enrollment Protocol (SCEP) für die Verwaltung von Webserverzertifikaten mit automatischer Verlängerung, um versehentliche Ausfälle der Abdeckung zu vermeiden. Eine Studie des Drittanbieters Principled Technologies aus dem Jahr 2020 ergab, dass diese automatische Verlängerungsfunktion für sichere Server sorgt und IT-MitarbeiterInnen wertvolle Zeit spart – insbesondere wenn sie eine ganze Flotte von Serverzertifikaten verwalten müssen.[12]

Verwendete Daten

Um verwendete Daten zu schützen, unterstützen Dell PowerEdge-Server die vertraulichen Compute-Funktionen von AMD, darunter AMD Secure Memory Encryption (SME) und Secure Encrypted Virtualization (SEV), um Daten zu schützen, während sie durch Arbeitsspeicher- und Verarbeitungskomponenten übertragen werden.

[11] Dell, „Reduce Your Risk of Unauthorized Server Data Access“, abgerufen am 24. Januar 2024, https://infohub.delltechnologies.com/section-assets/data-protection-infographic.

[12] Principled Technologies, „Reduce hands-on deployment times to near zero with iDRAC9 automation“, abgerufen am 4. Dezember 2023, https://www.principledtechnologies.com/Dell/iDRAC9-v6.10-provisioning-infographic-0323.pdf.

Secure Memory Encryption

AMD SME verschlüsselt alle Daten, sobald sie in den Arbeitsspeicher gelangen, und sorgt so für einen noch besseren Schutz Ihrer Daten. Ohne Arbeitsspeicherverschlüsselung sind Daten anfällig für bösartige Software und andere Eindringversuche, insbesondere bei neueren Arbeitsspeichertechnologien wie NVDIMMs, die beim Ausschalten keine Daten verlieren. Dieser Schutz erstreckt sich auf den Arbeitsspeicher über leistungsfähige Verschlüsselungs-Engines, die in die Arbeitsspeicherkanäle integriert sind und sowohl Sicherheit als auch Geschwindigkeit bieten. Da AMD SME für die Host-BS- und Anwendungsebene vollständig transparent ist, sind keine Änderungen an der Anwendungssoftware erforderlich. So bietet die Lösung einen nutzerfreundlichen Ansatz für eine verbesserte Arbeitsspeichersicherheit.[13]

Die In-Memory-Datenverschlüsselung von AMD SME ist eine Abkehr von älteren Arbeitsspeicherverschlüsselungsmethoden, die auf bestimmte Anwendungsfälle zugeschnitten waren. Ein Hauptvorteil von AMD SME ist die Flexibilität, dank der Software die Lösung auf verschiedene Weise nutzen kann: entweder durch Verschlüsselung des gesamten DRAM für einen umfassenden Schutz oder durch selektive Verschlüsselung bestimmter Regionen, z. B. Regionen, die von virtuellen Gastmaschinen (VMs) verwendet werden.[14]

AMD Secure Encrypted Virtualization

AMD SEV verbessert die Verschlüsselung für Arbeitsspeicher und virtuelle Maschinen durch die Implementierung einer auf virtuellen Maschinen basierenden vertrauenswürdigen Ausführungsumgebung (Trusted Execution Environment, TEE). Durch die Integration in die AMD-V-Architektur verschlüsselt AMD SEV den Arbeitsspeicher jeder VM separat und schützt die VMs sowohl voreinander als auch vor dem Hypervisor. Bei diesem Ansatz wird Kryptografie eingesetzt, um Code innerhalb einer VM vor potenziell anfälligem Code mit höheren Rechten zu schützen, z. B. vor dem Hypervisor. Die zusätzliche Sicherheitsebene ist besonders in Cloud-Umgebungen von entscheidender Bedeutung. Diese Methode stellt einen verbesserten Schutz für VMs sicher und schützt sie vor externen Sicherheitslücken. Die Verschlüsselung erfolgt direkt am Arbeitsspeicher-Controller, wo die Daten ohne Verlangsamung der Verarbeitungsgeschwindigkeit ver- und entschlüsselt werden – dank AMD Secure Processor, der alle Verschlüsselungsdetails unsichtbar verarbeitet.[15]

Es gibt immer noch einige Situationen, in denen die Daten einer VM mit anderen VMs oder mit dem Hypervisor kommunizieren müssen. In diesen Fällen ermöglicht AMD SEV der VM die Auswahl des Verschlüsselungsschlüssels, der auf bestimmte Arbeitsspeicherseiten angewendet werden soll: einen Gastschlüssel, der die Privatsphäre der Seite gegenüber der VM schützt, oder einen Hypervisor-Schlüssel, mit dem der Hypervisor und andere VMs die Seite entschlüsseln können. Diese Flexibilität ermöglicht Sicherheit und Kommunikation basierend auf den Anforderungen jeder VM.[16]

AMD SEV bietet zusätzliche Funktionen, die die kryptografische Isolierung von VMs erweitern: SEV-Encrypted State (SEV-ES) und SEV-Secure Nested Paging (SEV-SNP). SEV-ES isoliert VMs weiter voneinander und vom Hypervisor, indem CPU-Registerinhalte beim Herunterfahren einer VM verschlüsselt werden. So werden sie vor unbefugtem Zugriff über eine benachbarte VM oder den Hypervisor geschützt. SEV-SNP baut auf SEV und SEV-ES auf und bietet Arbeitsspeicherintegritätsschutz und optionale zusätzliche Sicherheitsfunktionen für VMs. Durch die Verbesserung der Arbeitsspeicherintegrität kann eine VM nur dann auf Daten im Arbeitsspeicher zugreifen, wenn sie den zuletzt geschriebenen Wert lesen kann. Wenn eine andere Entität die Daten im Arbeitsspeicher geändert hat, kann die VM nicht auf die Daten zugreifen. Dadurch wird die VM vor der Ausführung von kompromittierten Daten oder kompromittiertem Code geschützt.

Verschlüsselung und Verschlüsselungsschlüssel

AMD SEV verwendet einen eindeutigen Verschlüsselungsschlüssel für jede VM, um VMs und den Hypervisor kryptografisch zu isolieren. Diese Verschlüsselungs-Engine sichert Daten beim Schreiben und entschlüsselt sie beim Lesen. Jede VM erhält bei Erstellung einen eindeutigen Schlüssel, der sicherstellt, dass jeder unbefugte Zugriffsversuch auf ihren Arbeitsspeicher zu unverständlichen Daten führt. Jeder AMD EPYC™-Prozessor der 4. Generation bietet bis zu tausend Verschlüsselungsschlüssel. Diese Architektur ändert Anwendungen innerhalb der VM nicht. Stattdessen arbeitet sie auf der Betriebssystemebene und erhöht die Datensicherheit. Die in den Arbeitsspeicher-Controller integrierte Verschlüsselungshardware wurde entwickelt, um verwendete Daten zu schützen, einschließlich Arbeitsspeicherinhalten. Sie managt die Verschlüsselung und Entschlüsselung des VRAM-Datenverkehrs und erhöht so den Schutz von verwendeten Daten.[17]

[13] AMD, „AMD Infinity Guard“.
[14] AMD, „AMD Memory Encryption“, abgerufen am 4. Dezember 2023, https://www.amd.com/content/dam/amd/en/documents/epyc-business-docs/white-papers/memory-encryption-white-paper.pdf.
[15] AMD, „AMD Secure Encrypted Virtualization“, abgerufen am 4. Dezember 2023, https://www.amd.com/en/developer/sev.html.
[16] AMD, „AMD Memory Encryption“, https://www.amd.com/content/dam/amd/en/documents/epyc-business-docs/white-papers/memory-encryption-white-paper.pdf.
[17] AMD, „AMD Secure Encrypted Virtualization“.

Fazit

Von der Bestellung eines Dell PowerEdge-Servers mit AMD-Prozessoren bis zur Stilllegung und zu jeder Zeit dazwischen bieten Dell und AMD zahlreiche Sicherheitsebenen, um Ihre Daten zu schützen. Mit eng integrierten chipbasierten RoT-Schichten und Schutz während des Startens auf mehreren Ebenen zum Aussortieren verdächtiger Treiber, Firmware und BIOS-Versionen sind Serverkomponenten ab dem Zeitpunkt der Herstellung sicher. Darüber hinaus sind Ihre Daten durch die Verschlüsselung von SED- und ISE-Laufwerken auch dann sicher, wenn böswillige AkteurInnen Festplatten oder Server physisch aus Ihrem Rechenzentrum entfernen. Durch weitere Sicherheitsfunktionen wie die prozessorbasierte AMD SME- und SEV-Technologie, die Daten während der Verarbeitung schützt, und modernste Softwareprüfungen durch iDRAC können Dell PowerEdge-Server mit AMD-Prozessoren einen reibungslosen Geschäftsbetrieb sicherstellen – ganz gleich, welche neuen Angriffsmethoden sich Cyberkriminelle einfallen lassen. Weitere Informationen zu Dell PowerEdge-Servern mit AMD EPYC-Prozessoren der 4. Generation finden Sie unter www.dell.com/servers/amd.

Weitere Informationen zu Lösungen von Dell und AMD

Kontakt zu Dell Technologies ExpertInnen

Weitere Ressourcen

Reden Sie mit: #PowerEdge

DELL Technologies

AMD together we advance_