Whitepaper

Beveiliging van de digitale grens: een kijkje achter de Zero Trust-aanpak van Dell en AMD

Bescherm uw organisatie met de end-to-end beveiliging van Dell en AMD

Inhoudsopgave

Inleiding

De apparaten die ons verbinden, maken ongelooflijke dingen mogelijk, maar deze verbindingen zorgen helaas ook voor extra kwetsbaarheden waar kwaadwillenden misbruik van kunnen maken. Sommige schattingen voorspellen zelfs dat organisaties in 2025 maar liefst 10,5 biljoen dollar kwijt zullen zijn als gevolg van cyberaanvallen.[1] Volgens een schatting duurt het herstellen van de schade van een cyberaanval zo'n 277 dagen.[2]

Hoewel nieuwere technologie zoals kunstmatige intelligentie (AI) voor veel organisaties verbeteringen biedt op het gebied van productiviteit en de bedrijfsvoering, wordt data hierdoor ook kwetsbaar voor geavanceerdere cyberaanvallen. Met elke technologische vooruitgang moeten leiders in de technologie-industrie hun strategieën aanpassen om cybercriminelen effectief te bestrijden, omdat ze steeds nieuwe manieren vinden om data te stelen en misbruiken. Om deze bedreigingen te voorkomen en data te beschermen, heeft elke component van het datacenter - van servers en storage tot netwerken, software en firmware - geïntegreerde bescherming nodig. Bescherming begint met het beperken van de kans op manipulatie van de leveringsketen op de productievloer en gaat door tijdens het transportproces en het gebruik door de klant. En aanvallen stoppen niet langer bij de muren van datacenters. Organisaties die actief zijn in de cloud staan voor extra uitdagingen bij het beveiligen van data.

Dell en AMD bieden samen een speciaal gebouwde cyberbestendige architectuur waarmee organisaties een Zero Trust-strategie kunnen toepassen. Centraal hierbij staat het idee dat elke systeemcomponent in elke schakel van de keten kwetsbaar is en daarom wordt op elk punt bescherming geboden. Bij een Zero Trust-strategie wordt gebruik gemaakt van een krachtig, op identiteiten gebaseerd beleid voor elke IT-asset en voor toegang worden 'least privilege'-principes toegepast. De cybertolerante architectuur van Dell heeft geavanceerde functies ten aanzien van opstartintegriteit en databescherming, evenals iDRAC-beveiligingsfuncties (Integrated Dell Remote Access Controller). Dell PowerEdge servers zijn vervaardigd op een op silicium gebaseerde Root of Trust (RoT) die een vertrouwensketen tot stand brengt voor cryptografische verificatie van hardware- en softwarecomponenten op de server. AMD Infinity Guard biedt een extra beveiligingslaag die het potentieel van aanvallen verlaagt wanneer software wordt gestart en uitgevoerd. AMD Infinity Guard telt verschillende extra beveiligingsfuncties, waaronder Platform Secure Boot en Platform Secure Processor, die ervoor zorgen dat PowerEdge servers in elke fase van hun levenscyclus zijn beschermd.

De cyberbestendige architectuur van Dell

In de cyberbestendige architectuur van Dell wordt gebruik gemaakt van PowerEdge beveiligingsfuncties die samenwerken om veerkracht te bieden en een Zero Trust-strategie mogelijk te maken. Beveiligingsfuncties moeten bescherming bieden tegen potentiële bedreigingen, verdachte activiteiten detecteren en snel herstellen in geval van een inbreuk. Tegelijkertijd moeten ze ook een "verify before trust"-aanpak volgen om uitvoering te geven aan een Zero Trust-benadering met "least privilege"-principes, waarbij gebruikers en apparaten alleen toegang krijgen tot wat ze nodig hebben om hun taken uit te voeren. Door samen te werken, bieden deze PowerEdge beveiligingscontroles een uitgebreide beveiligingsoplossing die veerkracht garandeert en tegelijkertijd een Zero Trust-aanpak afdwingt. Voor meer informatie over alle functies en services van de cyberbestendige architectuur van Dell, verwijzen wij u naar de whitepaper.

Zorgen voor opstartintegriteit

De pre-boot-omgeving wordt vaak over het hoofd gezien en kan, als er geen voorzorgsmaatregelen worden genomen, worden aangevallen. Als een kwaadwillende tijdens het opstarten het BIOS, de firmware of een driver in gevaar brengt, kan die mogelijk toegang tot het hele systeem krijgen. Zonder de juiste controles kan een aanvaller op elk moment het systeem binnendringen en zijn gewenste doel bereiken: uw data.

Om beveiligingslekken te beperken, moet de fabrikant van de server het BIOS beschermen, maar ook specifieke servercomponenten en firmware zoals geheugen en processors verifiëren en valideren. Fabrikanten van serverhardware moeten ervoor zorgen dat hun componenten volledig integreren in de serverarchitectuur om beveiligings- en validatiecontroles probleemloos te laten werken. Elke Dell PowerEdge server heeft meerdere beveiligingslagen om de opstartcyclus te beschermen: een op silicium gebaseerde RoT, UEFI Secure Boot en iDRAC-beveiligingsfuncties, waaronder Firmware Rollback en Rapid Operating System Recovery.

Naast deze Dell PowerEdge servergebaseerde beveiligingslagen zijn AMD-processors uitgerust met Platform Secure Boot (PSB) en Platform Security Processor (PSP) om data te beschermen die in gebruik zijn. Samen dekken Dell en AMD elk aspect van de opstartcyclus af om een veilige basis voor uw data en workloads te garanderen.

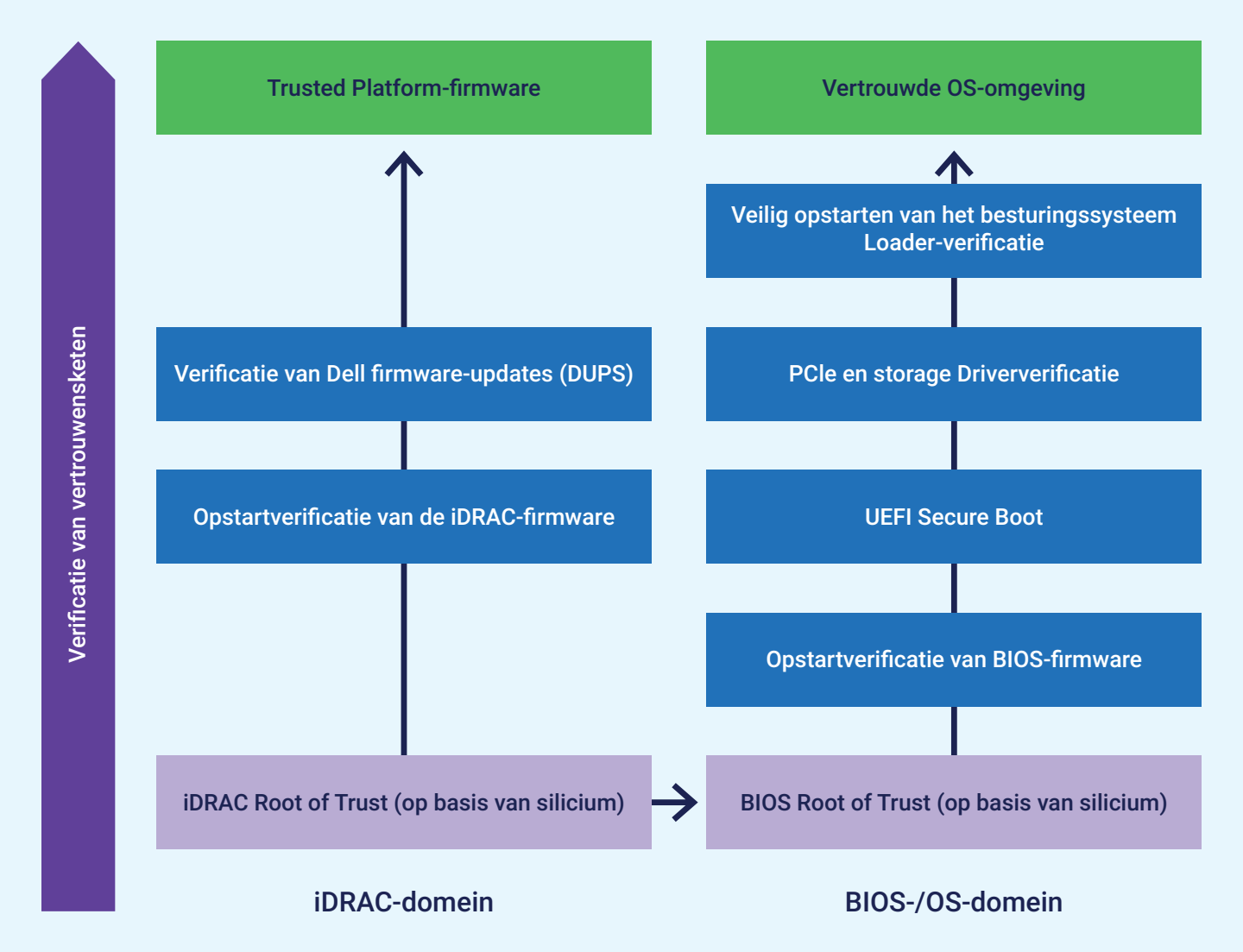
[1] Chuck Brooks, "Cybersecurity Trends & Statistics For 2023; What You Need to Know", geraadpleegd op 4 december 2023, https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=9885ce219dba.

[2] Ken Kizzee, "Cyber Attack Statistics to Know", geraadpleegd op 19 december 2023, https://parachute.cloud/cyber-attack-statistics-data-and-trends/.

Dell iDRAC en Root of Trust

Het RoT-concept gaat ervan uit dat als een systeem een bepaalde baseline als veilig heeft geverifieerd, alle daaropvolgende validaties en beveiligingscontroles worden verankerd in een continue vertrouwensketen. Stelt u zich een huis voor: Als de fundering instabiel is en begint af te brokkelen, doet de integriteit van de stenen muur er weinig toe. Hetzelfde principe geldt voor het BIOS van uw server. Als deze is gecompromitteerd, heeft het waarschijnlijk weinig zin om het serverbesturingssysteem te beveiligen.

De vertrouwensketen van PowerEdge servers biedt een naadloze cryptografische verificatie voor alle servercomponenten, van basis tot data. Dit zorgt ervoor dat de componenten van de systeemsoftwarestack (hypervisor, besturingssysteem, applicaties) kunnen vertrouwen op de onderliggende server wanneer de server operationeel is. Deze laag legt de basis van een vertrouwensketen binnen een server en zorgt voor een vertrouwd en veilig serverplatform. Dell servers maken gebruik van een unieke op silicium gebaseerde RoT die in elke server is gebrand. Deze zorgt voor cryptografische verificatie zodat veilig opstarten wordt gegarandeerd bij elke koude of warme opstart. Vanaf versie 4.10.10.10 biedt iDRAC een RoT-mechanisme om bij het opstarten de BIOS-image te verifiëren. De server staat opstarten pas toe nadat deze de BIOS-image heeft geverifieerd. Voor PowerEdge servers met AMD-processors maakt de geïntegreerde Dell Remote Access Controller (iDRAC) gebruik van AMD PSB-technologie om de BIOS-code te verifiëren voordat het besturingssysteem wordt geladen. AMD PSB onderzoekt de integriteit van het BIOS en communiceert met de primaire BIOS ROM en AMD Fusion Controller Hub (FCH) om een grondige RoT-verwerking uit te voeren. Deze minutieuze validatie strekt zich uit tot de bootloader van het besturingssysteem, waardoor een continue vertrouwensketen is gegarandeerd.



Afbeelding 1: Op silicium gebaseerde Root of Trust-domeinen in PowerEdge servers met iDRAC9.

Als de BIOS-validatie mislukt, sluit iDRAC de server onmiddellijk af en wordt de gebruiker hiervan op de hoogte gesteld, waardoor het opstarten van ongeautoriseerde firmware wordt voorkomen. iDRAC heeft ook een back-up- en herstelsysteem voor BIOS- en iDRAC-firmware, wat de betrouwbaarheid van de server versterkt en serveractiviteiten beschermt tegen mogelijke beschadiging van de firmware. Om extra bescherming te bieden, heeft iDRAC ook een live BIOS-scan die gebruikers op aanvraag kunnen uitvoeren of regelmatig kunnen plannen. Voor deze scan is de iDRAC Datacenter-licentie vereist en kunnen gebruikers mogelijke problemen opsporen voordat ze opnieuw opstarten, waardoor problemen proactief kunnen worden ingedamd.[3]

UEFI Secure Boot

Dell PowerEdge servers maken gebruik van de industriestandaard 'UEFI Secure Boot' om besturingssysteemspecifieke bootloaders te valideren, waardoor de integriteit van de OS-kernel en andere kritieke componenten wordt gewaarborgd. UEFI fungeert als een schild tegen malware en ransomware in pre-boot-omgevingen. Om interoperabiliteit te garanderen, moeten zowel fabrikanten van servers als componenten samenwerken om ervoor te zorgen dat voor UEFI geschikte BIOS driver- en firmwarehandtekeningen voor componenten worden herkend. Door cryptografische handtekeningen van UEFI-drivers en andere pre-OS-code te valideren, probeert 'UEFI Secure Boot' ervoor te zorgen dat code die tijdens het opstarten wordt geladen, vrij is van schadelijke inhoud.

Om de aanpasbaarheid van de beveiliging te verbeteren, kunnen beheerders aangepaste OS bootloader-ondertekeningscertificaten configureren voor UEFI Secure Boot. (Ga voor meer informatie over de aanpassingsopties voor UEFI Secure Boot naar https://infohub.delltechnologies.com/section-assets/direct-from-development-uefi-boot-enhanced-security-to-combat-threats.) Hierdoor wordt de uitvoering beperkt tot vertrouwde veilige OS-bootloaders, die de veilige opstartketen in stand houden doordat de kernel en het bestandssysteem van het besturingssysteem worden geverifieerd. Deze functie biedt extra flexibiliteit, met name voor Linux-beheerders die liever hun eigen OS-bootloaders ondertekenen in plaats van afhankelijk te zijn van standaard UEFI-certificeringsinstanties van derden. Beheerders kunnen via de iDRAC API aangepaste certificaten uploaden, waardoor de authenticatie van hun specifieke OS-bootloaders wordt verbeterd. Uniek is dat Dell PowerEdge servers volledige aanpassing van Secure Boot ondersteunen, waaronder de optie om alle standaardcertificaten van de certificeringsinstanties van Microsoft, VMware of UEFI te verwijderen.[4]

CPLD-validatie

Elke Dell PowerEdge server valideert het Complex Programmable Logic Device (CPLD) bij het opstarten. CPLD, een veelzijdig programmeerbaar logisch apparaat[5], bestaat uit meerdere eenvoudige PLD's die door een programmeerbare schakelmatrix met elkaar zijn verbonden. De firmware, die meestal wordt opgeslagen in EEPROM, flashgeheugen of SRAM, maakt aanpassingen aan de functies van de systeemkaart mogelijk die verder gaan dan de BIOS-mogelijkheden, waaronder de implementatie van specifieke logica voor interacties met apparaten op de systeemkaart. CPLD-validatie zorgt ervoor dat wijzigingen aan de systeemkaart geen schade toebrengen aan uw servers of data.

iDRAC-hardwarebeveiliging

iDRAC breidt de vertrouwensketen uit naar extra hardwarecomponenten en maakt gebruik van het Security Protocol and Data Model (SPDM), waarmee de manier wordt gestandaardiseerd waarop servers informatie over hun componenten verzamelen. De identiteits-, firmware- en configuratiegegevens van elke component worden versleuteld. iDRAC-hardwarebeveiliging maakt gebruik van geverifieerde sleuteluitwisselingen om de communicatielijnen tussen componenten en iDRAC te beveiligen. Met SPDM kan iDRAC de geldigheid van componenten zoals PowerEdge RAID-controllers (PERC)12 en netwerkinterfacekaarten (NIC's) verifiëren. Dit verbetert niet alleen de serverbeveiliging door de apparaatidentiteitscertificaten van componenten te verifiëren, maar waarschuwt gebruikers ook bij eventuele verificatiefouten.

[3] Dell, "Improved security with iDRAC9 using Root of Trust and BIOS Live Scanning", geraadpleegd op 19 december 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", geraadpleegd op 4 december 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", geraadpleegd op 4 december 2023, https://www.techopedia.com/definition/6655/complex-programmable-logic-device-cpld.

AMD Platform Secure Boot

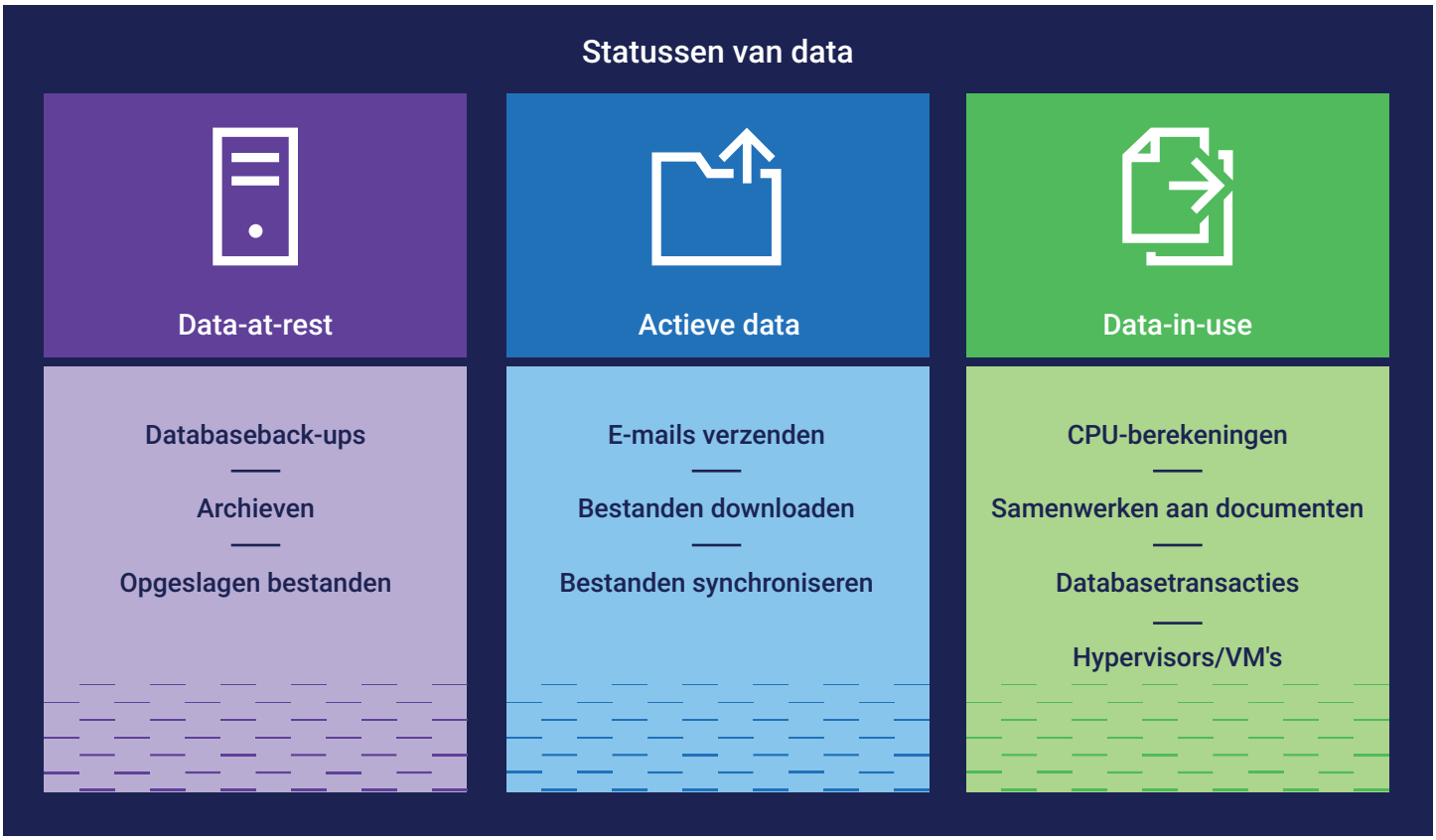
AMD-processors zijn uitgerust met AMD Platform Secure Boot (PSB) om een ander groeiend probleem in het huidige digitale landschap tegen te gaan: bedreigingen op firmwareniveau. PSB maakt gebruik van de AMD Silicon RoT en verifieert het opstartproces van de BIOS-code naar de OS Bootloader via UEFI Secure Boot.[6] Dell gebruikt AMD PSB-moederborden om alleen de cryptografisch ondertekende BIOS-code ervan uit te voeren. Bovendien bindt Dell elke AMD-processor aan een specifiek moederbord met eenmalige programmeerbare 'zekeringen' die de processor aan de ondertekeningssleutels van de Dell firmwarecode koppelen.[7] Ter bescherming tegen aanvallen die zijn gericht op het insluiten van malware in firmware, autoriseert PSB alleen firmware die door AMD Secure Processor is geverifieerd.[8]

Door de softwarestack cryptografisch te verifiëren, voegt AMD Platform Secure Boot een substantiële verdedigingslaag toe tegen onbevoegde indringing op verschillende platforms, met name in gevirtualiseerde omgevingen en in de cloud.

AMD Platform Secure Processor

Samen met PSB versterkt AMD Platform Secure Processor (PSP) het opstartproces van Dell PowerEdge servers. Wanneer een CPU voor het eerst wordt ingeschakeld in de fabriek van Dell, integreert de AMD Platform Secure Processor permanent een unieke Dell ID in de CPU. Deze ID koppelt de CPU aan de PowerEdge server, waardoor een veilige band ontstaat.[9]

Deze integratie betekent dat PSP voorkomt dat een PowerEdge server opstart als deze een CPU van een andere server detecteert. CPU-portabiliteit is echter nog steeds mogelijk na een eventuele hardwarestoring. De AMD-processor is vergrendeld op de ondertekeningssleutel van de leverancier in plaats van op het moederbord. Dit is een balans tussen beveiliging en mobiliteit van componenten.[10]



Afbeelding 2: Statussen van data

[6] AMD, "AMD Pro Security", geraadpleegd op 4 december 2023, https://www.amd.com/en/technologies/pro-security.
[7] AMD, "AMD Infinity Guard", geraadpleegd op 4 december 2023, https://www.amd.com/en/technologies/infinity-guard.
[8] AMD, "4 Ways AMD Infinity Guard Helps Protect Your Data", geraadpleegd op 4 december 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", geraadpleegd op 4 december 2023, https://infohub.delltechnologies.com/p/defense-in-depth-comprehensive-security-on-poweredge-amd-epyc-generation-2-rome-servers/.

Uw data beschermen

Hoewel aanvallers toegang krijgen tot systemen, is het einddoel altijd hetzelfde: uw data vinden en deze stelen, manipuleren, verkopen of vernietigen. De fysieke server is niet het enige zwakke punt. Kwaadwillenden kunnen netwerken aanvallen, IT-beleid kan fouten bevatten, eindgebruikers kunnen zwakke wachtwoorden hebben en IT-teams kunnen toegangsmachtigingen te ruim instellen. Aanvallers kunnen zich met phishingmails op gebruikers richten om malware te verspreiden.

Dell stelt klanten in staat om een Zero Trust-aanpak te hanteren die afhankelijk is van meerdere beveiligingslagen om tegen al deze kwetsbaarheden bescherming te bieden. Om diefstal en manipulatie te voorkomen, moet u data-at-rest, data-in-process, actieve data en de buitengebruikstelling van data beveiligen.[11] Met functies zoals versleuteling van data-at-rest, robuust versleutelingssleutelbeheer en geautomatiseerde certificaatverlenging zetten Dell PowerEdge servers zich in om schadelijke aanvallen na de eerste opstart te blokkeren, af te schrikken en te beperken. Dell PowerEdge servers met AMD-processors bieden extra functies om de beveiliging verder te versterken, waaronder AMD Secure Memory Encryption (SME) en Secure Encrypted Virtualization (SEV).

Data-at-rest

Om data-at-rest te beschermen, biedt Dell drie belangrijke beveiligingsfuncties: softwarematige versleuteling, sleutelbeheer op ondernemingsniveau en versleuteling van hardwareschijven. Met stations die Instant Secure Erase (ISE) ondersteunen, kunnen klanten van Dell alle data op zelfversleutelende schijven (SED's), ISE-schijven en NVM-apparaten zoals NVDIMM's cryptografisch wissen. SED's beschermen data tegen aanvallen in gevallen waarin een ontevreden werknemer of een andere kwaadwillende schijven fysiek van een server verwijdert. Omdat het wachtwoord van de vergrendelingssleutel van de versleutelde schijf deze koppelt aan de specifieke server en RAID-controller waar deze vandaan komt, heeft een andere server geen toegang tot de data. Voor verdere bescherming kan iDRAC Dell OpenManage Secure Enterprise Key Manager met lokaal sleutelbeheer (iLKM, LKM) gebruiken, dat samenwerkt met een externe sleutelbeheerder om de storagecontroller bij het opstarten te vergrendelen en te ontgrendelen. Als iemand de server opstart zonder de sleutelbeheerder, houdt iDRAC de storagecontroller vergrendeld, zodat de data die op het apparaat zijn opgeslagen, versleuteld blijven. Ga naar https://infohub.delltechnologies.com/section-assets/openmanage-sekm-storage-performance-infographic voor meer informatie over andere opties voor versleutelingssleutels.

Actieve data

Bij actieve data kunnen kwetsbaarheden in het netwerk en datatoegangscontrole aanvallers in staat stellen om data die via het netwerk worden verzonden, te onderscheppen of te wijzigen. De iDRAC-internetverbinding is een mogelijk kwetsbaar punt, dus Dell biedt verschillende opties om de verbinding te beveiligen met een TLS/SSL-certificaat, waardoor de kans op aanvallen wordt beperkt. Hoewel dit certificaat standaard zelfondertekend is, kunnen beheerders een aangepast certificaat maken of een certificaat kiezen dat is ondertekend door een vertrouwde certificeringsinstantie (CA). Met dit certificaat kunnen webbrowsers en tools zoals opdrachtregelhulpprogramma's veilig via de iDRAC-verbinding met de server communiceren.

iDRAC heeft ook verschillende besturingselementen voor gebruikers om strikte, beperkte toegangsregels aan te passen die SSH-toegang tot de server toestaan. Voor iDRAC-gebruikers met een licentie op datacenterniveau heeft iDRAC het Simple Certificate Enrollment Protocol (SCEP), dat webservercertificaten met automatische verlenging bijhoudt om te voorkomen dat de dekking per ongeluk vervalt. Uit onderzoek dat in 2020 door Principled Technologies is uitgevoerd, is gebleken dat deze automatische verlengingsfunctie ervoor zorgt dat servers veilig blijven en dat IT-personeel kostbare tijd bespaart, vooral als het gaat om het onderhouden van een vloot aan servercertificaten.[12]

Data-in-use

Om data-in-use te beschermen, beschikken Dell PowerEdge servers over vertrouwelijke AMD-rekenfuncties, waaronder AMD Secure Memory Encryption (SME) en Secure Encrypted Virtualization (SEV) om data te beschermen terwijl deze door het geheugen en verwerkingscomponenten stromen.

[11] Dell, "Reduce Your Risk of Unauthorized Server Data Access", geraadpleegd op 24 januari 2024, https://infohub.delltechnologies.com/section-assets/data-protection-infographic.

[12] Principled Technologies, "Reduce hands-on deployment times to near zero with iDRAC9 automation", geraadpleegd op 4 december 2023, https://www.principledtechnologies.com/Dell/iDRAC9-v6.10-provisioning-infographic-0323.pdf.

Secure Memory Encryption

AMD SME versleutelt alle data wanneer deze het geheugen binnenkomt, waardoor uw data nog beter zijn beveiligd. Zonder geheugenversleuteling zijn data kwetsbaar voor schadelijke software en andere indringers, vooral met nieuwere geheugentechnologie zoals NVDIMM's die geen data verliezen wanneer ze worden uitgeschakeld. Deze bescherming strekt zich uit tot het geheugen via krachtige versleutelingsengines die in de geheugenkanalen zijn geïntegreerd, waardoor zowel veiligheid als snelheid worden gegarandeerd. Omdat deze aanpak volledig transparant is voor het hostbesturingssysteem en de applicatielagen, realiseert AMD SME dit zonder dat er wijzigingen in de applicatiesoftware nodig zijn, wat een gebruiksvriendelijke benadering is om geheugen beter te beveiligen.[13]

AMD SME in-memory dataversleuteling wijkt af van oudere geheugenversleutelingsmethoden die waren afgestemd op specifieke gebruiksscenario's. Een belangrijk voordeel van AMD SME is de flexibiliteit, waardoor software er op verschillende manieren gebruik van kan maken: ofwel door alle DRAM te versleutelen voor een uitgebreide bescherming, ofwel door selectief specifieke regio's te versleutelen, zoals die worden gebruikt door gast-VM's (Virtuele Machines).[14]

AMD Secure Encrypted Virtualization

AMD SEV verbetert de versleuteling voor het geheugen en virtuele machines door een op virtuele machines gebaseerde TEE-omgeving (Trusted Execution Environment) te implementeren. AMD SEV integreert in de AMD-V-architectuur en versleutelt het geheugen van elke VM afzonderlijk, waardoor de VM's tegen elkaar en tegen de hypervisor worden beschermd. Deze aanpak maakt gebruik van cryptografie om code binnen een VM te beschermen tegen mogelijk kwetsbare code met hogere bevoegdheden, zoals de hypervisor. De extra beveiligingslaag is vooral cruciaal in cloudomgevingen. Deze methode zorgt voor betere bescherming van VM's, waardoor deze worden versterkt tegen kwetsbaarheden van buiten. De versleuteling vindt plaats bij de geheugencontroller, waar data wordt versleuteld en ontsleuteld zonder de verwerkingssnelheid te vertragen. Dit is te danken aan de AMD Secure Processor die alle versleutelingsdetails onzichtbaar verwerkt.[15]

Er zijn nog steeds enkele situaties waarin de data van een VM met andere VM's of met de hypervisor moeten communiceren. In deze gevallen staat AMD SEV de VM toe om te kiezen welke versleutelingssleutel moet worden toegepast op specifieke geheugenpagina's: een gastsleutel die de pagina privé houdt voor de VM of een hypervisorsleutel waarmee de hypervisor en andere VM's de pagina kunnen ontsleutelen. Deze flexibiliteit maakt beveiliging en communicatie mogelijk op basis van de behoeften van elke VM.[16]

AMD SEV biedt extra functies die de cryptografische isolatie van VM's uitbreiden: SEV-Encrypted State (SEV-ES) en SEV-Secure Nested Paging (SEV-SNP). SEV-ES isoleert VM's verder van elkaar en de hypervisor door CPU-registerinhoud te versleutelen wanneer een VM wordt uitgeschakeld, waardoor deze wordt beschermd tegen onbevoegde toegang via een naburige VM of de hypervisor. SEV-SNP bouwt voort op SEV en SEV-ES en voegt geheugenintegriteitsbescherming en optionele extra beveiligingsfuncties voor VM's toe. De verbetering van de geheugenintegriteit zorgt ervoor dat een VM alleen toegang heeft tot data in het geheugen als deze de laatste waarde kan lezen die is geschreven. Als een andere entiteit de data in het geheugen heeft gewijzigd, heeft de VM geen toegang tot de data. Dit beschermt de VM tegen het uitvoeren van gecompromitteerde data of code.

Versleuteling en versleutelingssleutels

AMD SEV maakt voor elke VM gebruik van een unieke versleutelingssleutel, waardoor VM's en de hypervisor cryptografisch worden geïsoleerd. Deze versleutelingsengine beveiligt data bij schrijfbewerkingen en ontsleutelt deze bij het lezen ervan. Elke VM ontvangt bij het maken een unieke sleutel, zodat elke ongeoorloofde poging om toegang te krijgen tot het geheugen resulteert in onbegrijpelijke data. Elke 4e generatie AMD EPYC™-processor biedt tot duizend versleutelingssleutels. Deze architectuur verandert niets aan applicaties binnen de VM. In plaats daarvan werkt de architectuur op het niveau van het besturingssysteem en wordt de databeveiliging naar een hoger niveau getild. De versleutelingshardware die is ingebouwd in de geheugencontroller, is ontworpen om data-in-use te beschermen, waaronder de inhoud van het geheugen, en beheert de versleuteling en ontsleuteling van VRAM-verkeer en versterkt de bescherming van data-in-use.[17]

[13] AMD, "AMD Infinity Guard".
[14] AMD, "AMD Memory Encryption", geraadpleegd op 4 december 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", geraadpleegd op 4 december 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".

Conclusie

Vanaf het moment dat u Dell PowerEdge servers met AMD-processors bestelt tot het moment dat u ze buiten gebruik stelt en elk moment daartussenin, bieden Dell en AMD talloze beveiligingslagen om uw data veilig te houden. Dankzij nauw geïntegreerde lagen van op silicium gebaseerde RoT en meerdere lagen aan opstartbescherming om verdachte drivers, firmware en BIOS-versies te verwijderen, zijn servercomponenten vanaf het moment van productie veilig. Door SED- en ISE-schijven te versleutelen, zijn bovendien uw data veilig, zelfs als kwaadwillende personen schijven of servers fysiek uit uw datacenter verwijderen. Dankzij andere beveiligingsfuncties, zoals processorgebaseerde AMD SME- en SEV-technologie, die data tijdens het proces beschermen, en geavanceerde softwarecontroles via iDRAC, zorgen Dell PowerEdge servers met AMD-processors er mede voor dat uw bedrijfsvoering probleemloos doorgaat, ongeacht welke nieuwe aanvalsmethoden cybercriminelen bedenken. Ga voor meer informatie over Dell PowerEdge servers met 4e generatie AMD EPYC processors naar www.dell.com/servers/amd.

Meer informatie over de oplossingen van Dell en AMD

Neem contact op met een Dell Technologies expert

Bekijk meer informatiebronnen

Neem deel aan het gesprek via #PowerEdge

DELL Technologies

AMD
together we advance_