Informationsdokument

Säkra den digitala gränsen: I Dells och AMD:s nollförtroendestrategi

Skydda din organisation med Dells och AMD:s heltäckande säkerhet

Innehållsförteckning

Inledning

Enheterna som kopplar samman oss gör otroliga saker möjliga, men de här anslutningarna ger också ytterligare sårbarhetspunkter som illvilliga aktörer kan utnyttja. Enligt vissa uppskattningar kommer cyberattacker att ha kostat organisationer så mycket som $ 10,5 biljoner år 2025.[1] Och enligt en uppskattning tar det cirka 277 dagar att återhämta sig efter skadorna från en cyberattack.[2]

Nyare teknik som artificiell intelligens (AI) möjliggör förbättringar av produktivitet och affärsverksamhet för många organisationer, men den gör även data sårbara för mer sofistikerade cyberattacker. Med varje teknikframsteg måste ledare inom teknikbranschen byta strategi för att effektivt motverka cyberbrottslingar som hittar nya sätt att komma åt och utnyttja data. För att motverka dessa hot och skydda data måste alla datacenterkomponenter – från servrar och lagring till nätverk, mjukvara och fast mjukvara – ha inbyggt skydd. Skyddet börjar med åtgärder för att minska manipulering av leverantörskedjan på tillverkningsgolvet och fortsätter genom transportprocessen och kundanvändningen. Och attackerna stannar inte längre vid datacentrets väggar. Organisationer som håller till i molnet står inför ytterligare utmaningar när det gäller att hålla data säkra.

Tillsammans tillhandahåller Dell och AMD en specialbyggd cyberelastisk arkitektur som hjälper organisationer att anta en nollförtroendestrategi som omfattar tanken på att systemkomponenter är sårbara vid varje länk i kedjan och erbjuder skydd vid varje punkt. En nollförtroendestrategi använder starka, identitetsbaserade policyer för varje IT-tillgång tillsammans med principer om ”lägsta behörighet” för åtkomst. Dells cyberelastiska arkitektur innehåller djupgående funktioner centrerade kring startintegritet och dataskydd samt säkerhetsfunktioner i Integrated Dell Remote Access Controller (iDRAC). Dell PowerEdge-servrar är förankrade med en kiselbaserad förtroenderot (RoT) som upprättar en förtroendekedja för kryptografisk verifiering av hårdvaru- och mjukvarukomponenter på servern. AMD Infinity Guard ger ytterligare ett säkerhetslager som minskar den potentiella attackytan när mjukvara startas och körs. AMD Infinity Guard omfattar flera ytterligare säkerhetsfunktioner, som till exempel Platform Secure Boot och Platform Secure Processor, som säkerställer att PowerEdge-servrar skyddas i varje steg av livscykeln.

Dell cyberelastisk arkitektur

Dells cyberelastiska arkitektur använder PowerEdge-säkerhetsfunktioner som samverkar för att både ge tålighet och möjliggöra en nollförtroendestrategi. Säkerhetsfunktionerna måste skydda mot potentiella hot, upptäcka misstänkt aktivitet och snabbt återställas vid intrång. Samtidigt måste de också upprätthålla en ”verifiera före förtroende”-attityd för en nollförtroendemetod med lägsta behörighet, där användare och enheter endast får åtkomst till det de behöver för att utföra sina uppgifter. Genom att arbeta tillsammans ger de här säkerhetsfunktionerna i PowerEdge en omfattande säkerhetslösning som garanterar tålighet samtidigt som nollförtroendet upprätthålls. Mer information om de fullständiga funktionerna och tjänsterna i Dells cyberelastiska arkitektur finns i informationsdokumentet.

Säkerställa startintegritet

Förstartsmiljön förbises ofta och kan, om skyddsåtgärder inte vidtas, vara öppen för angrepp. Om en illvillig aktör komprometterar BIOS, fast mjukvara eller en drivrutin under start kan hen potentiellt få åtkomst till hela systemet. Utan rätt kontroller på plats kan hen framgångsrikt infiltrera systemet när som helst och nå sitt önskade mål: dina data.

För att minimera sårbarheter måste serverleverantören skydda BIOS, men även verifiera och validera specifika serverkomponenter och fast mjukvara, till exempel minne och processorer. Tillverkare av serverhårdvara måste se till att deras komponenter integreras helt med serverarkitekturen för att säkerhets- och valideringskontroller ska fungera sömlöst. Varje Dell PowerEdge-server erbjuder flera säkerhetslager för att skydda startcykeln: en kiselbaserad förtroenderot, UEFI Secure Boot och iDRAC-säkerhetsfunktioner, som avveckling av fast mjukvara och snabb återställning av operativsystem.

Utöver dessa Dell PowerEdge-serverbaserade säkerhetslager har AMD-processorer PSB (Platform Secure Boot) och PSP (Platform Security Processor) för att skydda data som används. Tillsammans täcker Dell och AMD alla aspekter av startcykeln för att säkerställa en säker grund för dina data och din arbetsbelastning.

[1] Chuck Brooks, ”Cybersäkerhetstrender och statistik för 2023; allt du behöver veta”, hämtad 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, ”Statistik om cyberattacker du bör ha koll på” (på engelska), hämtad 19 december 2023, https://parachute.cloud/cyber-attack-statistics-data-and-trends/.

Dell iDRAC och förtroenderot

Förtroenderot-konceptet förutsätter att om ett system verifierar en grund eller baslinje som säker, är alla efterföljande valideringar och säkerhetskontroller förankrade i en kontinuerlig förtroendekedja. Föreställ dig ett hus: Om grunden är instabil och börjar smulas sönder spelar väggens integritet ingen större roll. På samma sätt är det om din servers BIOS äventyras, då kan det vara förgäves att skydda serverns operativsystem.

Förtroendekedjan för PowerEdge-servrar ger en smidig kryptografisk verifiering av alla serverkomponenter, från grund till data. Detta säkerställer att komponenterna i systemmjukvarustacken (hypervisor, OS, program) är medvetna om att de kan lita på den underliggande servern när servern är i drift. Det här lagret lägger grunden för en förtroendekedja inom en server och skapar en betrodd och säker serverplattform. Dell-servrar använder en unik kiselbaserad förtroenderot som bränns in i varje server för kryptografisk verifiering som säkerställer säker start vid varje kallstart eller A/C-cykel. Från och med version 4.10.10.10 tillhandahåller iDRAC (Integrated Dell Remote Access Controller) en förtroenderot-mekanism för att verifiera BIOS-bilden vid start och tillåter inte att servern startar förrän BIOS-bilden har verifierats. För PowerEdge-servrar med AMD-processorer använder iDRAC AMD PSB-teknik för att verifiera BIOS-koden innan operativsystemet läses in. AMD PSB granskar BIOS-integriteten och samverkar med BIOS-huvudsystemets ROM och AMD Fusion Controller Hub (FCH) för grundlig bearbetning av förtroenderoten. Denna noggranna validering sträcker sig upp till OS-starthanterare, vilket garanterar en kontinuerlig förtroendekedja.

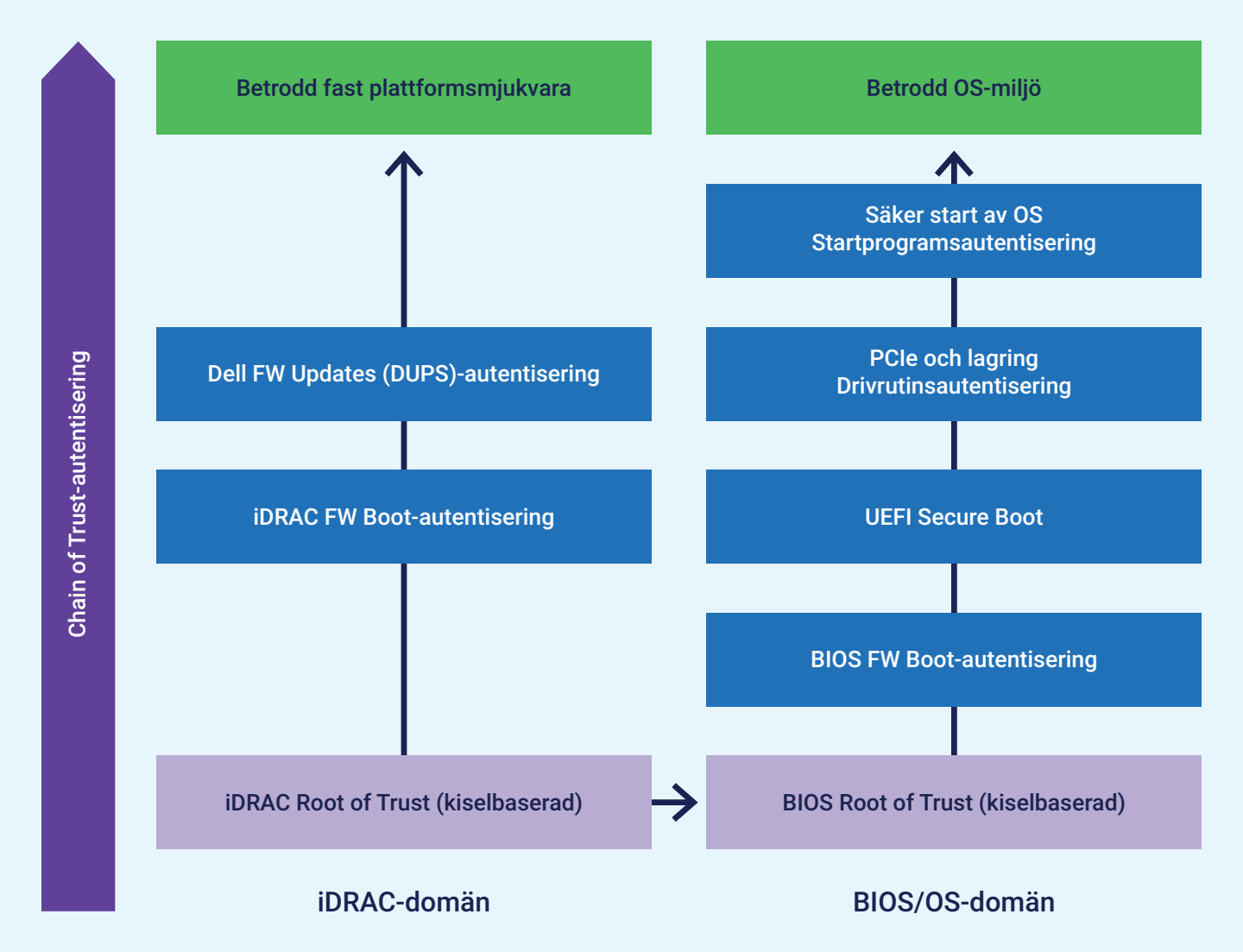

Bild 1: Kiselbaserade förtroenderot-domäner i PowerEdge-servrar med iDRAC9.

Om BIOS-valideringen misslyckas stänger iDRAC omedelbart av servern och meddelar användaren, vilket förhindrar att obehörig fast mjukvara startas. iDRAC innehåller även ett system för säkerhetskopiering och återställning för BIOS och fast iDRAC-mjukvara, vilket förstärker serverns pålitlighet och skyddar serverdriften mot potentiell skada på den fasta mjukvaran. För att ge ytterligare skydd erbjuder iDRAC även en BIOS-genomsökning i realtid som användare kan köra på begäran eller schemalägga att köra regelbundet. Den här genomsökningen kräver iDRAC Datacenter-licensen och gör det möjligt för användare att upptäcka potentiella problem innan de startar om, vilket möjliggör proaktiva åtgärder.[3]

UEFI Secure Boot

Dell PowerEdge-servrar använder UEFI Secure Boot som är branschstandard för att validera operativsystemsspecifika startprogram, vilket säkerställer integriteten hos OS-kärnan och andra viktiga komponenter. UEFI fungerar som en sköld mot skadliga program och utpressningsvirus i förstartsmiljöer. För att säkerställa interoperabilitet måste både server- och komponenttillverkare samarbeta för att säkerställa att det UEFI-aktiverade BIOS känner igen signaturer för drivrutiner och fast mjukvara för komponenter. Genom att validera kryptografiska signaturer för UEFI-drivrutiner och annan kod som föregår operativsystemet strävar UEFI Secure Boot efter att säkerställa att all kod som läses in under starten är fri från skadligt innehåll.

För att öka säkerhetsanpassningen kan administratörer konfigurera anpassade signeringscertifikat för OS-starthanterare för UEFI Secure Boot. (Om du vill ha mer information om anpassningsalternativen för UEFI Secure Boot går du till https://infohub.delltechnologies.com/section-assets/direct-from-development-uefi-boot-enhanced-security-to-combat-threats.) Detta begränsar körningen till betrodda säkra OS-starthanterare, som upprätthåller den säkra startkedjan genom att autentisera OS-kärnan och filsystemet. Den här funktionen ger ytterligare flexibilitet, särskilt för Linux-administratörer som föredrar att signera sina egna OS-starthanterare snarare än att vara beroende av standardiserade UEFI-certifieringsbehörigheter från tredje part. Administratörer kan ladda upp anpassade certifikat via iDRAC API, vilket förbättrar autentiseringen av deras specifika OS-starthanterare. Dell PowerEdge-servrar har unikt stöd för fullständig anpassning av Secure Boot, inklusive alternativet att ta bort alla standardcertifikat från Microsoft, VMware eller UEFI CA.[4]

CPLD-validering

Alla Dell PowerEdge-servrar validerar CPLD (Complex Programmable Logic Device) vid varje A/C-start. CPLD, en mångsidig programmerbar logikenhet,[5] består av flera enkla PLD:er som är anslutna med en programmerbar switchmatris. Den fasta mjukvaran, som vanligtvis lagras i EEPROM, flashminne eller SRAM, gör det möjligt att modifiera moderkortets funktioner utöver BIOS-kapaciteten, till exempel med implementering av specifik logik för interaktion med moderkortets enheter. CPLD-validering säkerställer att ändringar av moderkortet inte skadar dina servrar eller data.

iDRAC-hårdvarusäkerhet

För att utöka förtroendekedjan till ytterligare hårdvarukomponenter använder iDRAC säkerhetsprotokollet och datamodellen SPDM (Security Protocol and Data Model), som standardiserar hur servrar samlar in information om sina komponenter. Varje komponents identitet, fasta mjukvara och konfigurationsinformation krypteras. iDRAC-hårdvarusäkerhet använder autentiserade nyckelutbyten för att säkra kommunikationslinjerna mellan komponenter och iDRAC. Med SPDM kan iDRAC autentisera giltigheten för komponenter som PowerEdge RAID-kontroller (PERC)12 och nätverkskort (NIC), vilket inte bara förbättrar serversäkerheten genom att autentisera komponenternas enhetsidentitetscertifikat, utan även varnar användare om eventuella autentiseringsfel.

[3] Dell, ”Förbättrad säkerhet med iDRAC9 med hjälp av förtroenderot och BIOS Live Scanning” (på engelska), hämtad 19 december 2023, https://dl.dell.com/manuals/common/dell-emc-idrac9-security-root-of-trust-bios-live-scanning.pdf.

[4] Dell, ”Cyberelastisk säkerhet för Dell PowerEdge-servrar” (på engelska), hämtad 4 december 2023, https://www.delltechnologies.com/asset/en-us/products/servers/industry-market/cyber-resilient-security-with-poweredge-servers.pdf.

[5] Technopedia, ”Komplex programmerbar logikenhet” (på engelska), hämtad 4 december 2023, https://www.techopedia.com/definition/6655/complex-programmable-logic-device-cpld.

AMD Platform Secure Boot

AMD-processorer har AMD Platform Secure Boot (PSB) för att motverka ett annat växande problem i dagens digitala landskap: hot mot fast mjukvara. PSB utnyttjar AMD-kiselförtroenderoten och verifierar startprocessen från BIOS-koden till OS-starthanterare genom UEFI Secure Boot.[6] Dell använder AMD PSB-aktiverade moderkort för att endast tillåta körning av deras kryptografiskt signerade BIOS-kod. Dessutom binder Dell varje AMD-processor till ett specifikt moderkort med engångsprogrammerbara säkringar som kopplar processorn till Dells kodsigneringsnycklar för fast mjukvara.[7] För att skydda mot attacker som syftar till att bädda in skadliga program i fast mjukvara auktoriserar PSB endast fast mjukvara som autentiserats av AMD Secure Processor.[8]

Genom att kryptografiskt verifiera mjukvarustacken lägger AMD Platform Secure Boot till ett rejält lager av försvar mot obehörigt intrång på olika plattformar, särskilt i virtualiserade miljöer eller i molnet.

AMD Platform Secure Processor

Tillsammans med PSB förstärker AMD Platform Secure Processor (PSP) startprocessen för Dell PowerEdge-servrar. När en processor startas för första gången i Dell-fabriken bäddar AMD Platform Secure Processor in ett unikt Dell-ID permanent i processorn. Detta ID knyter effektivt processorn till PowerEdge-servern, vilket skapar en säker förbindelse.[9]

Den här integreringen innebär att PSP hindrar en PowerEdge-server från att starta om den upptäcker en processor från en annan server. Processor-portabilitet är dock fortfarande möjlig i händelse av ett hårdvarufel. AMD-processorn är låst till leverantörens signeringsnyckel istället för moderkortet, vilket ger en balans mellan säkerhet och komponentmobilitet.[10]

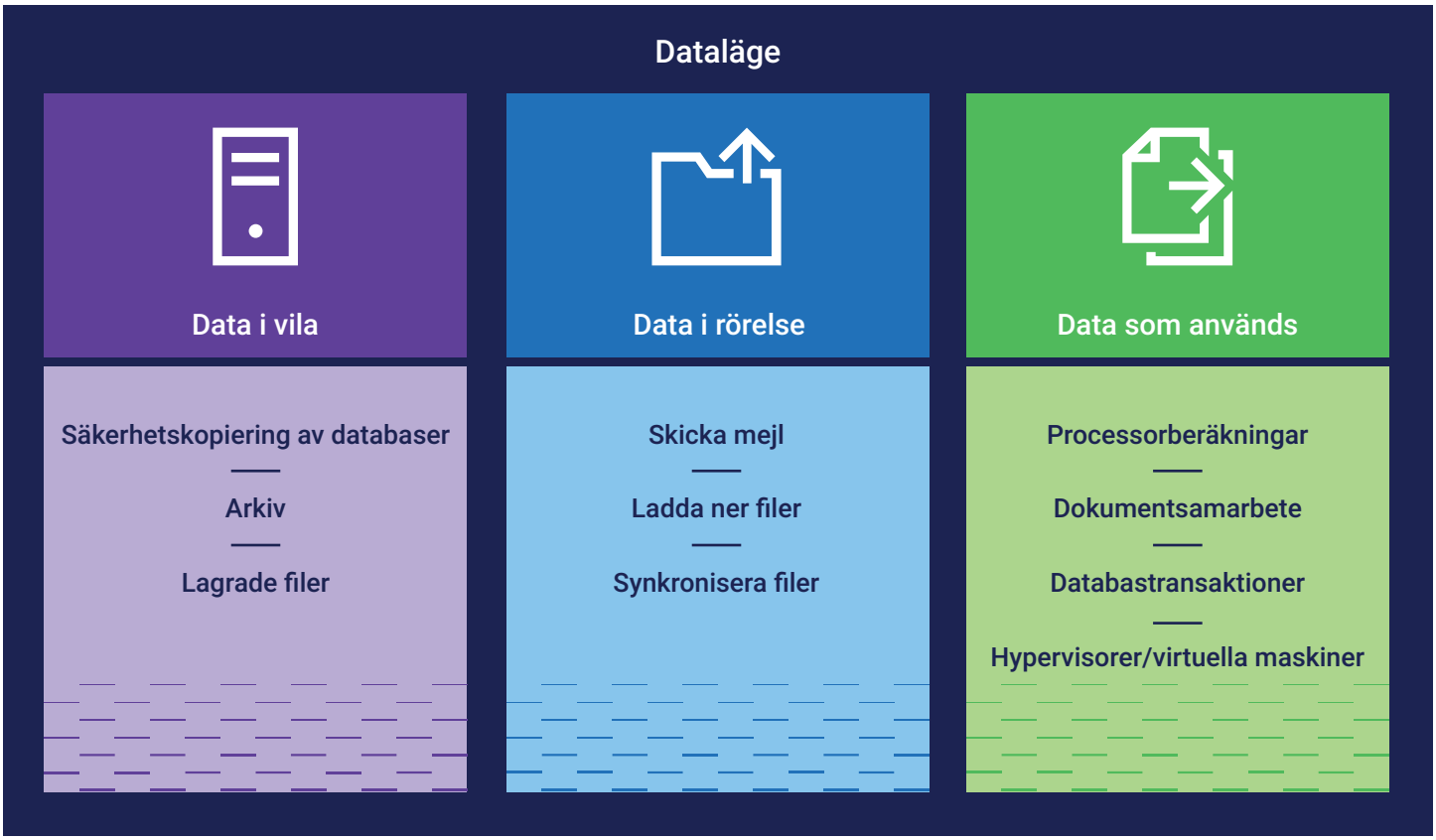

Bild 2: Dataläge

[6] AMD, ”AMD Pro Security”, hämtad 4 december 2023, https://www.amd.com/en/technologies/pro-security.
[7] AMD, ”AMD Infinity Guard”, hämtad 4 december 2023, https://www.amd.com/en/technologies/infinity-guard.
[8] AMD, ”4 sätt AMD Infinity Guard hjälper dig att skydda dina data” (på engelska), hämtad 4 december 2023, https://www.amd.com/system/files/documents/content-security-infographic.pdf.
[9] AMD, ”AMD Infinity Guard.”
[10] Dell, ”Djupgående försvar: Omfattande säkerhet på PowerEdge AMD EPYC Generation 2-servrar (Rome)” (på engelska), hämtad 4 december 2023, https://infohub.delltechnologies.com/p/defense-in-depth-comprehensive-security-on-poweredge-amd-epyc-generation-2-rome-servers/.

Skydda dina data

Även om angripare får åtkomst till systemen, är slutmålet alltid detsamma: att hitta dina data och stjäla, manipulera, sälja eller förstöra dem. Den fysiska servern är inte den enda sårbara punkten. Illvilliga aktörer kan attackera nätverk, IT-policyer kan innehålla fel, slutanvändare kan ha svaga lösenord och IT-team kan ange åtkomstbehörigheter för brett. Angripare kan rikta in sig på användare med nätfiske-meddelanden via mejl för att distribuera skadliga program.

Dell gör det möjligt för kunder att använda en metod med nollförtroende som bygger på flera säkerhetslager för att skydda mot alla dessa typer av sårbarheter. För att skydda dig mot stöld eller kompromettering måste du skydda vilande data, bearbetade data och in-flight data, fram till datainaktivering.[11] Med funktioner som kryptering vid vila, robust hantering av krypteringsnycklar och automatiserad förnyelse av certifikat arbetar Dell PowerEdge-servrar för att blockera, avskräcka och mildra skadliga attacker efter första start. Dell PowerEdge-servrar med AMD-processorer erbjuder ytterligare funktioner för att stärka säkerheten, såsom AMD Secure Memory Encryption (SME) och Secure Encrypted Virtualization (SEV).

Data i vila

För att skydda data i vila tillhandahåller Dell tre huvudsakliga säkerhetsfunktioner: mjukvarubaserad kryptering, Enterprise Key Management och kryptering av hårdvarudrivenhet. Med drivenheter som stöder omedelbar säker radering (Instant Secure Erase, ISE) kan Dell-kunder kryptografiskt radera alla data på självkrypterande enheter (SED), ISE-enheter och NVM-enheter som NVDIMM. Självkrypterande enheter skyddar data från attacker i fall där en missnöjd anställd eller annan illvillig aktör fysiskt tar bort drivenheter från en server. Eftersom den krypterade enhetens låsnyckellösenord knyter den till den specifika server- och RAID-kontrollern som den kom från, kan en annan server inte komma åt data. För ytterligare skydd kan iDRAC använda Dell OpenManage Secure Enterprise Key Manager med lokal nyckelhantering (iLKM, LKM) som fungerar tillsammans med en extern nyckelhanterare från tredje part för att låsa och låsa upp lagringsstyrenheten vid start. Om någon startar servern långt bort ifrån nyckelhanteraren håller iDRAC lagringsstyrenheten låst så att data som lagras på enheten förblir krypterade. Om du vill ha mer information om andra alternativ för krypteringsnycklar kan du besöka https://infohub.delltechnologies.com/section-assets/openmanage-sekm-storage-performance-infographic.

In-flight-data

Med In-flight-data kan sårbarheter i nätverket och dataåtkomstkontroll göra det möjligt för angripare att fånga upp eller ändra data som färdas över nätverket. iDRAC-webbanslutningen är en möjlig sårbar punkt, så Dell erbjuder flera alternativ för att säkra anslutningen med ett TLS/SSL-certifikat och därmed minska risken för angrepp. Även om det här certifikatet är självsignerat som standard kan administratörer skapa ett anpassat certifikat eller ett som är signerat av en betrodd certifieringsbehörighet (CA). Det här certifikatet möjliggör krypterade, säkra anslutningar så att webbläsare och verktyg, till exempel kommandoradsverktyg, kan interagera med servern på ett säkert sätt via iDRAC-anslutningen.

iDRAC tillhandahåller också flera kontroller som användare kan använda för att ändra strikta, smala åtkomstregler som tillåter SSH-åtkomst till servern. För iDRAC-användare med en licens på datacenternivå erbjuder iDRAC SCEP (Simple Certificate Enrollment Protocol), som underhåller webbservercertifikat med automatisk förnyelse för att undvika oavsiktliga avbrott i täckningen. En studie från 2020 av tredjepartsföretaget Principled Technologies visade att den här funktionen för automatisk förnyelse håller servrarna säkrare samtidigt som IT-personalen sparar värdefull tid – särskilt när det gäller att upprätthålla en uppsjö av servercertifikat.[12]

Data som används

För att skydda data som används aktiverar Dell PowerEdge-servrar AMD:s konfidentiella beräkningsfunktioner, som AMD Secure Memory Encryption (SME) och Secure Encrypted Virtualization (SEV) för att skydda data när de flödar genom minnes- och bearbetningskomponenter.

[11] Dell, ”Minska din risk för obehörig åtkomst till serverdata” (på engelska), hämtad 24 januari 2024, https://infohub.delltechnologies.com/section-assets/data-protection-infographichttps.

[12] Principled Technologies, ”Minska praktisk driftsättningstid till nästan noll med iDRAC9 automatisering” (på engelska), hämtad 4 december 2023, https://www.principledtechnologies.com/Dell/iDRAC9-v6.10-provisioning-infographic-0323.pdf.

Secure Memory Encryption (SME)

AMD SME krypterar alla data när de kommer in i minnet och skyddar dina data ytterligare. Utan minneskryptering är data sårbara för skadlig mjukvara och andra intrång, särskilt med nyare minnesteknik som NVDIMM-moduler som inte förlorar data när de stängs av. Skyddet sträcker sig till minnet via högpresterande krypteringsmotorer som är integrerade i minneskanalerna, vilket garanterar både säkerhet och hastighet. Eftersom det är helt transparent för värdoperativsystemet och applikationslagren, åstadkommer AMD SME detta utan att kräva några ändringar i applikationsmjukvaran, vilket ger en användarvänlig metod för förbättrad minnessäkerhet.[13]

AMD SME-datakryptering i minnet skiljer sig från äldre minneskrypteringsmetoder som var skräddarsydda för specifika användningsfall. En viktig fördel med AMD SME är dess flexibilitet, som gör att mjukvaran kan använda den på olika sätt: antingen genom att kryptera hela DRAM-minnet för omfattande skydd eller selektivt kryptera specifika regioner, till exempel de som används av virtuella gästmaskiner (VM).[14]

AMD Secure Encrypted Virtualization (SEV)

AMD SEV förbättrar krypteringen för minne och virtuella maskiner genom att implementera en virtuell maskinbaserad betrodd körningsmiljö (TEE). AMD SEV integreras med AMD-V-arkitekturen och krypterar minnet för varje virtuell maskin separat, vilket skyddar de virtuella maskinerna från varandra och från hypervisor. Den här metoden använder kryptografi för att skydda kod på en virtuell maskin från potentiellt sårbar kod med högre privilegier, till exempel hypervisor-programmet. Det extra säkerhetslagret är särskilt viktigt i molnmiljöer. Den här metoden säkerställer förbättrat skydd för virtuella maskiner och stärker dem mot externa sårbarheter. Krypteringen sker direkt vid minnesstyrenheten, där den krypterar och dekrypterar data utan att sänka bearbetningshastigheten – tack vare att AMD Secure Processor hanterar alla krypteringsdetaljer osynligt.[15]

Det finns fortfarande vissa situationer när en virtuell maskins data behöver kommunicera med andra virtuella maskiner eller med hypervisor-programmet. I dessa fall tillåter AMD SEV att den virtuella maskinen väljer vilken krypteringsnyckel som ska tillämpas på specifika minnessidor: en gästnyckel som håller sidan privat för den virtuella maskinen eller en hypervisor-nyckel som gör att hypervisor-programmet och andra virtuella maskiner kan dekryptera sidan. Den här flexibiliteten möjliggör säkerhet och kommunikation baserat på behoven för varje virtuell maskin.[16]

AMD SEV erbjuder ytterligare funktioner som utökar den kryptografiska isoleringen av virtuella maskiner: SEV-Encrypted State (SEV-ES) och SEV-Secure Nested Paging (SEV-SNP). SEV-ES isolerar ytterligare virtuella maskiner från varandra och hypervisorn genom att kryptera processorns registrerade innehåll när en virtuell maskin stängs av, vilket skyddar den från obehörig åtkomst via en närliggande virtuell maskin eller hypervisor. SEV-SNP bygger på SEV och SEV-ES och lägger till minnesintegritetsskydd och ytterligare säkerhetsfunktioner som tillval för virtuella maskiner. Förbättringen av minnesintegriteten gör att en virtuell maskin endast kan komma åt data i minnet om den kan läsa det senaste värdet som den skrev. Om en annan entitet har ändrat data i minnet kan den virtuella maskinen inte komma åt data. Detta skyddar den virtuella maskinen från att köra komprometterade data eller komprometterad kod.

Kryptering och krypteringsnycklar

AMD SEV använder en unik krypteringsnyckel för varje virtuell maskin, vilket kryptografiskt isolerar virtuella maskiner och hypervisor-programmet. Den här krypteringsmotorn skyddar data vid skrivning och dekrypterar dem vid läsning. Varje virtuell maskin får en unik nyckel när den skapas, vilket säkerställer att alla obehöriga försök att komma åt dess minne resulterar i obegripliga data. Varje 4:e generations AMD EPYC-processor™ erbjuder upp till tusen krypteringsnycklar. Den här arkitekturen ändrar inte program på den virtuella maskinen utan fungerar istället på operativsystemnivå och höjer datasäkerheten. Krypteringshårdvaran som är inbyggd i minnesstyrenheten är utformad för att skydda data som används, inklusive minnesinnehåll, och hanterar VRAM-trafikkryptering och -dekryptering, vilket stärker skyddet av data som används.[17]

[13] AMD, ”AMD Infinity Guard.”
[14] AMD, ”AMD Memory Encryption”, hämtad 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”, hämtad 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.”

Slutsats

Från det att du beställer Dell PowerEdge-servrar med AMD-processorer till det att du kasserar dem och varje ögonblick däremellan erbjuder Dell och AMD många säkerhetslager för att skydda dina data. Serverkomponenterna är säkra redan från tillverkningen, med tätt integrerade lager av kiselbaserad förtroenderot och flera lager av startskydd för att sålla bort misstänkta drivrutiner, fast mjukvara och BIOS-versioner. Genom att kryptera SED- och ISE-enheter är dina data dessutom säkra även om illvilliga aktörer fysiskt tar bort diskar eller servrar från ditt datacenter. Tack vare andra säkerhetsfunktioner, som processorbaserad AMD SME- och SEV-teknik som skyddar bearbetade data och toppmoderna mjukvarukontroller via iDRAC, kan Dell PowerEdge-servrar med AMD-processorer se till att verksamheten fortsätter utan problem – oavsett vilka nya angreppsmetoder cyberbrottslingar hittar på. Om du vill ha mer information om Dell PowerEdge-servrar med fjärde generationens AMD EPYC-processorer kan du besöka www.dell.com/servers/amd.

Mer information om Dell- och AMD-lösningar

Kontakta en Dell Technologies-expert

Visa fler resurser

Delta i samtalet med #PowerEdge

DELL Technologies

AMD
together we advance_

Publicerat i USA 1/24 informationsdokument