Handleiding voor passieve SED op Adaptec® Storage Adapters

Nieuwe passieve SED-ondersteuning voor SAS- en SATA-apparatuur is nu beschikbaar voor Smart Storage-adapters ter bescherming van gegevens in gebruik en in rust

Het belang van gegevensbeveiliging neemt snel toe naarmate de dreiging van cyberaanvallen in datacenters en de cloud computing-industrie toeneemt. Gegevensencryptie is nu een beveiligingsvereiste voor de gezondheidszorg, de financiële sector en de verzekeringssector, met overheidsmandaten voor beveiliging en privacy met betrekking tot gegevens in rust.

De Adaptec® storage adapters van Microchip bieden twee encryptiemogelijkheden. De eerste is Controller-Based Encrypton (CBE) en de tweede is Self-Encrypting Drive (SED) ondersteuning. Controller-Based Encrypton (CBE) is een uitgebreide encryptieoplossing die wordt aangeboden op de meeste Adaptec RAID-adapters, maar we bieden nu ook SED aan als het huidige systeem niet compatibel is met een Adaptec® maxCrypto™ CBE-enabled adapter of als er behoefte is aan een HBA encryptieoplossing. De passieve SED-ondersteuning voor SAS- en SATA-apparaten is beschikbaar in de meeste SmartRAID 3100- en SmartHBA 2100-modellen (in HBA-modus) en HBA 1100-modellen met firmwareversie 4.11 en hoger evenals in de meeste modellen van de nieuwe SmartRAID 3200, SmartHBA 2200 (in HBA-modus) en HBA 1200.

Wat is een zelfversleutelende schijf?

Een Self-Encrypting Drive (SED) is een hardwarematige versleutelingsmethode voor HDD's en SSD's die de gegevens automatisch versleutelt en ontsleutelt, onafhankelijk van externe versleutelingsprocessoren of besturingssystemen. SED's bieden bescherming van gegevens in rust en halen de cryptografische verwerking weg van de host-CPU, met weinig tot geen impact op latentie en I/O-prestaties.

Hoe werkt een zelfversleutelende schijf?

Het coderingsproces wordt uitgevoerd met behulp van een unieke en willekeurige Data Encryption Key (DEK) die de schijf gebruikt om de gegevens te coderen en te decoderen. Wanneer gegevens naar de schijf worden geschreven, worden ze eerst gecodeerd volgens de DEK. Evenzo worden gegevens die van de schijf worden gelezen, eerst met dezelfde DEK gedecodeerd voordat ze naar de rest van het systeem worden verzonden. Deze op hardware gebaseerde encryptie biedt extra

beveiliging tegen cyberaanvallen, omdat de sleutel niet toegankelijk is via een aanval op softwareniveau. De DEK is bovendien nuttig omdat hij door de gebruiker kan worden beheerd als hij gecompromitteerd is en moet worden bijgewerkt, of de gegevens veilig moeten worden gewist, in welk geval de DEK kan worden gewist. Naast de DEK moet een Authenticatiesleutel, of AK, worden geconfigureerd om gegevens in rust te beschermen. Deze AK vergrendelt de versleutelde gegevens van de SED wanneer de schijven worden uitgeschakeld, waardoor toegang tot de schijfgegevens bij diefstal of intern openen wordt voorkomen.

Passive SED op Adaptec-adapters biedt het Trusted Computing Group Security Protocol (TCG) dat nodig is om te communiceren en toegang te krijgen tot de volledige functieset van elk SED-apparaat. In Passive SED ondersteunt de adapter Level 0 discovery header om te bepalen of het een SED-apparaat is, of het TCG-beveiligingsprotocol Enterprise of Opal is en of het apparaat vergrendeld of ontgrendeld is. Wanneer het SED-apparaat op een HBA of RAID-adapter is aangesloten, communiceert het met het besturingssysteem uitsluitend als een SCSI-doel. Het gebruik van SED's in RAID-volumes wordt niet aanbevolen. Eenmaal aangesloten, gebruikt het besturingssysteem een hulpprogramma van derden om met het TCG beveiligingsprotocol te communiceren met de SED via de fysieke SCSI passthrough interface van de Adaptec controller. De passieve SED-basiscode van Adaptec ondersteunt SAS- en SATA-interfaceversies van het TCG-beveiligingsprotocol.

Wat zijn de voordelen van een SED?

Als u overweegt een SED aan te schaffen, houd dan rekening met de onderstaande punten:

- SED's hebben een verwaarloosbare invloed op de prestatiesnelheid en -latentie. Het versleutelingsproces is volledig geïntegreerd, zodat er geen andere systeemcomponenten nodig zijn om in te grijpen en veel werk te verzetten.
- Naast CBE-adapters zijn SED's een van de sterkste beveiligingsmiddelen die voor geld te koop zijn. Ze zijn onafhankelijk van het besturingssysteem, dus zelfs als een hacker een computer aanvalt, is het vrijwel onmogelijk toegang te krijgen tot de SED (en de daarin opgeslagen versleutelingscodes) wanneer de computer is uitgeschakeld.
- Eenmaal gekoppeld aan software van derden voor het beheer van versleutelingscodes is het gebruik van een SED eenvoudig. De software optimaliseert de ontsleutelings- en versleutelingsfuncties van de SED en het sleutelbeheer, waardoor de gebruiker geen actief SED-beheer meer hoeft uit te voeren.
- SED's zijn goedkoop in gebruik en onderhoud. SED's coderen op het moment dat ze van de lopende band komen. Beheersoftware doet de rest en zorgt ervoor dat SED's hun werk doen zonder menselijke tussenkomst, wat tijd en geld bespaart

Conclusie

Indien een Adaptec maxCrypto™ CBE-controller geen optie is, maar er toch een solide bescherming tegen cyberaanvallen op bedrijfs- en/of klantgegevens moet worden geïmplementeerd, vormen SED's een uitstekende oplossing. Het gebruik van SED's isoleert beveiligingsgegevens van aanvallen op softwareniveau en minimaliseert menselijke fouten in het beveiligingsprotocol.