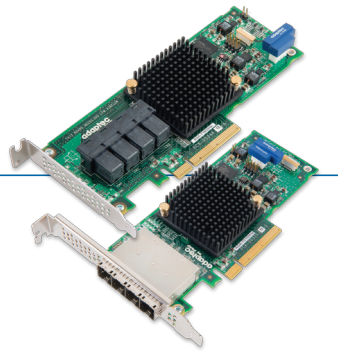
Überragende on-the-fly Datenverschlüsselung in Leitungsgeschwindigkeit



Die Themenstellung

In Rechenzentren und Cloud Computing-Umgebungen genießt die Datensicherheit mittlerweile höchste Priorität. Unternehmen sind bestrebt, Kundendaten, vertrauliche Geschäftsdokumente und die geschäftliche Kommunikation sowie Finanzdaten, Gehaltsdaten der Mitarbeiter und andere vertrauliche Daten zu schützen.

Leiter von Rechenzentren müssen sich der doppelten Herausforderung stellen, zum einen die Daten zu schützen, zum andern aber auch immer höheren Leistungsanforderungen für umfangreiche Anwendungen wie Web-Server, Dateiserver, Datenbanken, OLTP (Online-Transaktionsverarbeitung), Microsoft Exchange Server und HPC (High Performance Computing) gerecht zu werden.

Gefahren für die Datensicherheit

Bei den Sicherheitsbemühungen steht bislang vor allem der Schutz der Daten vor Angriffen aus dem Internet im Mittelpunkt. Doch in Rechenzentren können die Sicherheitsgefahren, denen die Hardware in unterschiedlichen Szenarien direkt ausgesetzt ist, nicht länger ignoriert werden.

Entsorgung von Speicherlaufwerken

Bevor Speicherlaufwerke ausgemustert werden, müssen die darauf gespeicherten Daten für Unbefugte, die z. B. in Abfallcontainern wühlen, unzugänglich gemacht werden. Dies kann auf zwei Arten erreicht werden. Die erste Möglichkeit ist die Komplettlöschung der Daten. Bei dieser Methode wird das komplette Laufwerk mit Datenmüll beschrieben, sodass die Nutzdaten überschrieben werden. Bei dem Datenmüll handelt es sich in der Regel um eine Reihe von Nullen oder um verschiedene nach dem Zufallsprinzip erzeugte Zeichenmuster. Je nach Kapazität und Geschwindigkeit des Speicherlaufwerks kann dieser Vorgang mehrere Stunden in Anspruch nehmen. Wenn ein kompletter Server ausgemustert wird, kann es tagelang dauern, bis die Daten aller angeschlossenen Laufwerke komplett gelöscht sind.

Zudem kann der Fall eintreten, dass für unterschiedliche Laufwerkstypen wie etwa Festplatten und SSD-Laufwerke (Solid State Drives) unterschiedliche Tools und Methoden für die Komplettlöschung der Daten erforderlich sind. Als zweite Möglichkeit kann das Laufwerk mit einem Hammer, einem Shredder oder anderen geeigneten Werkzeugen zerstört werden. Auch dieses Verfahren ist u. U. zeitaufwändig. Zudem bleiben möglicherweise weiterverwendbare Teile zurück, wenn die Arbeit nicht gründlich erledigt wurde. Gewiefte Hacker könnten daraus noch Daten auslesen.

Austausch defekter Laufwerke

Vertrauliche Daten sollten von einem Speicherlaufwerk entfernt werden, wenn es wegen eines Ausfalls zum Austausch an den Lieferanten zurückgesendet werden muss.

Auch hier gelten dieselben Herausforderungen wie bei der Entsorgung von Laufwerken. Die zusätzliche Schwierigkeit besteht darin, Daten von einem funktionsunfähigen Laufwerk zu löschen.

Diebstahl

Firewalls und andere Tools für die Netzwerksicherheit sind erstaunlich effizient, wenn es darum geht, Daten vor Hackern zu schützen. Doch was nützen diese schon, wenn die Gefahr besteht, dass Unbefugte die Speicherlaufwerke selbst, also die Hardware an sich, entwenden?

Für alle oben genannten Situationen wäre eine Manipulation der Daten auf dem eigentlichen Laufwerk die ideale Lösung. Die Daten wären dadurch unlesbar bzw. unbrauchbar, wenn Unbefugte auf diese zugreifen möchten.

Datenverschlüsselung

Die Verschlüsselung ist eine Codierung von Daten, die bewirkt, dass diese nur von befugten Personen genutzt werden können. Die Informationen werden mit einem Schlüssel codiert und sind ohne den Schlüssel nicht lesbar. Es gibt zwei Arten der Verschlüsselung: die symmetrische und die asymmetrische Verschlüsselung.

Bei der symmetrischen Kryptographie wird derselbe Schlüssel für die Verschlüsselung und die Entschlüsselung genutzt. Wenn der Schlüssel manipuliert wird, ist die Sicherheit nicht mehr gewährleistet. Deshalb ist die Verwaltung der Schlüssel bei diesem Verfahren ein entscheidender, komplexer Vorgang.

Bei der asymmetrischen Kryptographie wird ein Schlüssel für die Verschlüsselung und ein zweiter Schlüssel für die Entschlüsselung genutzt.

Der Schlüssel für die Verschlüsselung kann per Softwareimplementierung öffentlich bereitgestellt werden. Der Schlüssel für die Entschlüsselung verbleibt jedoch als privater Schlüssel in der Hardware. Dieses Verfahren bietet höhere Sicherheit als die asymmetrische Kryptographie.

Die eigentliche Verschlüsselung kann software- oder hardwaregestützt sein. Bei der softwaregestützten Verschlüsselung liefert der Prozessor die nötige Rechenleistung. Bei der hardwaregestützten Verschlüsselung kommt hingegen ein separater Chipsatz zum Einsatz, das sich im Laufwerk selbst oder im Hostbusadapter (HBA) befindet.

Highlights

Adaptec maxCrypto Datenverschlüsselung für Festplatten und SSDs

Verfügbar bei Adaptec Hostbusadaptern (HBAs) der Serie 7He mit 6 Gbit/s

- Ein HBA kann mehrere Laufwerke verschlüsseln. Das senkt die Investitionskosten und vereinfacht die Implementierung
- Kompatibel mit der vorhandenen Infrastruktur von Rechenzentren sowie mit Festplatten und SSD-Laufwerken aller Hersteller
- Rechenzentren sind damit in der Lage, eine einheitliche, skalierbare Verschlüsselungsstrategie im ganzen Unternehmen einzuführen

On-the-fly hardwarebasierte Verschlüsselung

- Leitungsgeschwindigkeit mit minimalen Auswirkungen auf die Latenz
- Erfordert keine Software zur Schlüsselverwaltung
- Der Encryption-Schlüssel ist vom Betriebssystem unabhängig, wodurch keine Gefahren durch Viren oder andere Angriffe drohen

Überlegene Kryptographie und Funktionalität

- Branchenführender Authentifizierungs-Chip Infineon SLE95050
- AES-Verschlüsselung mit 256 Bit
- Innovativer ECC-Logarithmus (Elliptic Curve Cryptography)
- Asymmetrische Schlüsselauthentifizierung

Datengröße und Datenstruktur auf dem Laufwerk bleiben erhalten

- Keine Beeinträchtigung der Nutzungskapazität oder der Wartungstechnologien

Überragende on-the-fly Datenverschlüsselung in Leitungsgeschwindigkeit

Softwaregestützte Verschlüsselung

Die softwaregestützte Verschlüsselung wird vom Betriebssystem gesteuert. Dabei werden die Daten mit einer Anwendung verschlüsselt und entschlüsselt, wenn diese auf den Laufwerken gespeichert bzw. von diesen gelesen werden.

Vorteile der softwaregestützten Verschlüsselung

- in der Regel die kostengünstigste Datenverschlüsselungsmethode
- Software-Anwendungen sind für die gängigen Betriebssysteme erhältlich und funktionieren mit Festplatten und SSDs der meisten Hersteller

Nachteile der softwaregestützten Verschlüsselung

- Da die Verschlüsselung und Entschlüsselung auf der Prozessorebene stattfinden, steigt die Latenz der Speichersysteme
- Das Betriebssystem, unter dem die Software-Verschlüsselung läuft, ist für Viren, Abstürze und andere Bedrohungen anfällig

Hardwaregestütztes Self-Encrypting Drive (SED)

Bei einer selbst verschlüsselnden SSD oder Festplatte (kurz SED) erfolgen Verschlüsselung und Entschlüsselung unabhängig von Prozessor und Betriebssystem über einen Chipsatz, in dem ein Schlüssel für die Verschlüsselung und Entschlüsselung integriert ist.

Vorteile von SEDs

- Der Schlüssel für die Verschlüsselung ist vom Betriebssystem unabhängig, wodurch keine Gefahren durch Viren oder andere Angriffe drohen.
- Für die Verschlüsselung sorgt dedizierte Hardware, sodass keine spürbaren Auswirkungen auf die Latenz oder die E/A-Leistung auftreten.

Nachteile von SEDs

- Neue SEDs müssen (in der Regel zu höheren Preisen als herkömmliche Laufwerke) beschafft und implementiert werden.
- Zur Absicherung kompletter Systeme ist der Austausch aller vorhandenen Festplatten und SSD-Laufwerke durch SEDs erforderlich.
- Derzeit ist die Auswahl bei den Anbietern von Festplatten und SSD-Laufwerken noch relativ gering.
- Die vorhandenen Daten müssen von den bislang nicht verschlüsselten Laufwerken auf die neuen SEDs übertragen werden.
- Die Verwaltung mehrerer SEDs erfordert eine integrierte Softwarelösung für die Schlüsselverwaltung.
- Einige SEDs verfügen über einen nicht entfernbaren Schlüssel. Dadurch sind die Daten ungeschützt, wenn das Laufwerk entsorgt oder an den Lieferanten zurückgesendet wird.

HBAs mit hardwaregestützter Verschlüsselung

Ebenso wie SEDs verfügen auch HBAs mit hardwaregestützter Verschlüsselung über ein integriertes Chipset für die Verschlüsselung und Entschlüsselung.

Vorteile von HBAs mit hardwaregestützter Verschlüsselung

- Der Schlüssel für die Verschlüsselung ist vom Betriebssystem unabhängig, wodurch keine Gefahren durch Viren oder andere Angriffe drohen.
- Für die Verschlüsselung sorgt dedizierte Hardware, sodass keine spürbaren Auswirkungen auf die Latenz oder die E/A-Leistung auftreten.
- Kompatibel mit der vorhandenen Infrastruktur von Rechenzentren sowie mit Festplatten und SSDs aller Hersteller. Daher müssen die bisherigen Laufwerke nicht durch SEDs nur eines Anbieters ersetzt werden.
- Ein HBA kann mehrere Laufwerke verschlüsseln. Das senkt die Investitionskosten und vereinfacht die Implementierung.
- HBAs haben in der Regel eine höhere Lebensdauer als Festplatten und SSDs und müssen daher nicht so häufig ausgetauscht werden, was ebenfalls die Investitionskosten senkt.
- Erfordert keine integrierte Softwarelösung für die Schlüsselverwaltung.

Nachteile von HBAs mit hardwaregestützter Verschlüsselung:

- Vorhandene HBAs müssen durch verschlüsselungsfähige HBAs ersetzt werden.
- Beim Einschalten der Verschlüsselung werden alle Daten auf dem Laufwerk gelöscht. Sollen diese Daten aufbewahrt werden, muß vor der Encryption ein Backup durchgeführt werden.

Adaptec maxCrypto

Die 6 Gb/s Adaptec Hostbusadapter der Serie 7He mit bereits integrierter Adaptec maxCrypto Encryption liefern on-the-fly Ver- und Entschlüsselung auf höchstem Niveau in Leitungsgeschwindigkeit und mit minimaler Auswirkung auf die Latenz.

Adaptec maxCrypto ist mit dem branchenführenden Authentifizierungs-Chip Infineon SLE95050 ausgestattet, der den innovativen Elliptische-Kurven-Kryptographiealgorithmus (ECC) sowie eine asymmetrische Schlüsselauthentifizierung für überlegene Kryptographie und Funktionalität nutzt.

Es ist keine Softwarelösung für die Schlüsselverwaltung erforderlich. Somit sind Rechenzentren in der Lage, eine einheitliche, skalierbare Verschlüsselungsstrategie im ganzen Unternehmen einzuführen.

Da maxCrypto auf HBAs basiert, ist die Lösung mit den vorhandenen Speicherinfrastrukturen kompatibel; es müssen also keine neuen Festplatten oder SSD-Laufwerke erworben werden. Der Adaptec 7He verschlüsselt jedoch keine Daten auf Bandlaufwerken oder auf anderen Laufwerken ohne Direktzugriff. Der HBA unterstützt Bandlaufwerke, wenn der Encryption-Schlüssel entfernt wird. Auch Multi-LUN Support für RBOD ist bisher noch nicht verfügbar. Die Verschlüsselung funktioniert jedoch bei LUN0 eines RBOD und bei allen anderen Laufwerken mit Direktzugriff.

Adaptec maxCrypto verändert weder die Größe der Daten auf einem Laufwerk noch deren Struktur. Deshalb kommt es zu keiner Beeinträchtigung der Nutzungskapazität oder der Wartungstechnologien wie etwa Dedupe.

Einsatzgebiete des Adaptec maxCrypto Schlüssels

Jeder maxCrypto Key wird mit einem einzigartigen Encryption-Schlüssel hergestellt. Adaptec HBAs der Serie 7He sind mit einem speziellen Steckplatz für diesen Key ausgerüstet.

Durch das Einstecken des Schlüssels in den Steckplatz bzw. durch dessen Erkennung wird die Verschlüsselung ausgelöst. Alle angeschlossenen Laufwerke haben denselben Verschlüsselungsstatus – es sind entweder alle oder keines der Laufwerke verschlüsselt. Das BIOS des HBA zeigt an, ob die Verschlüsselung aktiviert oder deaktiviert ist. Auf diese Weise kann der Verschlüsselungsstatus geprüft werden, ohne dass direkt am HBA nachgeschaut werden muss, ob der Schlüssel steckt.

Überragende on-the-fly Datenverschlüsselung in Leitungsgeschwindigkeit

Die folgende Tabelle zeigt die Ergebnisse nach dem Einstecken, Entfernen und erneuten Anbringen des maxCrypto Schlüssels in verschiedenen Szenarien.

Da die Daten auf Festplatten und SSDs, die mit maxCrypto verschlüsselt wurden, ohne Schlüssel nicht genutzt werden können, stellt maxCrypto ein wirksames Mittel gegen die zuvor in diesem Dokument genannten Gefahren für die unmittelbare Sicherheit der Hardware dar: ausgemusterte Laufwerke können ohne zeitaufwändige Komplettdatenlöschung entsorgt werden; ein defektes Laufwerk kann an den Hersteller zurückgesendet werden, ohne dass die Datenintegrität gefährdet ist. Selbst wenn ein Laufwerk gestohlen wird, hält der Dieb damit nur die Hardware in Händen – nicht jedoch die wertvollen Daten, die darauf gespeichert sind.

Fazit

Rechenzentren sehen sich immer stärker in der Verantwortung, vertrauliche Daten wie etwa die Identität der Kunden, die geschäftliche Kommunikation sowie Finanzdaten zu schützen. Dabei dürfen sie nicht nur an den Schutz der Daten vor Angriffen aus dem Internet denken, sondern müssen darüber hinaus auch Sicherheitsgefahren entgegentreten, denen die Festplatten und SSDs in unterschiedlichen Szenarien unmittelbar ausgesetzt sind.

Die Datenintegrität ist gefährdet, wenn ein ausgefallenes Laufwerk vom Rechenzentrum an den Lieferanten zurückgesendet wird, wenn Laufwerke ohne zeitaufwändige Komplettdatenlöschung ausgemustert werden oder wenn die Laufwerke diebstahlgefährdet sind. Werden die Daten jedoch gleich bei deren Speicherung verschlüsselt, hat das Rechenzentrum Gewissheit, dass keine Unbefugten auf diese Daten zugreifen können, selbst dann nicht, wenn sie sich das Laufwerk angeeignet haben, auf dem die Daten gespeichert sind.

Die Software-Verschlüsselung ist eine kostengünstige Lösung, verursacht jedoch Leistungsprobleme und ist anfällig für Viren und Betriebssystemabstürze. Self-Encrypting Drives (SEDs) stellen eine leistungsfähige hardwaregestützte Lösung dar, erfordern jedoch beträchtliche Investitionen und erheblichen Verwaltungsaufwand.

Die Platzierung der Verschlüsselung im HBA bietet bei geringerem Kapitaleinsatz alle Vorteile der hardwaregestützten Verschlüsselung und zudem eine einfachere Verwaltung als bei SEDs.

Bei den Adaptec 6 Gb/s Hostbusadaptern (HBAs) der Serie 7He ist die hardwarebasierte Verschlüsselungslösung Adaptec maxCrypto bereits integriert. Diese Lösung ermöglicht eine optimale Datenverschlüsselung/-entschlüsselung bei minimalen Auswirkungen auf die Latenz. Sie lässt sich nahtlos in vorhandene Speicherinfrastrukturen integrieren. Damit sind Rechenzentren in der Lage, eine einheitliche, skalierbare Verschlüsselungsstrategie im ganzen Unternehmen einzuführen.

Ursprünglicher Zustand	Daten verschlüsselt?	Aktion	Ergebnis
HBA ohne maxCrypto Schlüssel	nein	maxCrypto Schlüssel einstecken	Vorhandene Daten werden gelöscht*, neue Daten werden verschlüsselt
HBA ohne maxCrypto Schlüssel	nein	HBA ohne maxCrypto Schlüssel austauschen	Daten werden nicht verschlüsselt
HBA ohne maxCrypto Schlüssel	nein	HBA mit maxCrypto Schlüssel austauschen	Vorhandene Daten werden gelöscht*, neue Daten werden nicht verschlüsselt
HBA ohne maxCrypto Schlüssel	nein	HBA durch HBA eines anderen Anbieters austauschen	Daten werden nicht verschlüsselt
HBA mit maxCrypto Schlüssel	ja	maxCrypto Schlüssel entfernen	Vorhandene Daten werden gelöscht*, neue Daten werden nicht verschlüsselt
HBA mit maxCrypto Schlüssel	ja	Ausfall des maxCrypto Schlüssels	Vorhandene Daten werden gelöscht*, neue Daten werden nicht verschlüsselt
HBA mit maxCrypto Schlüssel	ja	Schlüssel durch neuen maxCrypto Schlüssel ersetzen	Vorhandene Daten werden gelöscht*, neue Daten werden verschlüsselt
HBA mit maxCrypto Schlüssel	ja	HBA mit vorhandenem maxCrypto Schlüssel austauschen	Die Daten bleiben intakt und verschlüsselt
HBA mit maxCrypto Schlüssel	ja	HBA mit maxCrypto Schlüssel austauschen	Vorhandene Daten werden gelöscht*, neue Daten werden verschlüsselt
HBA mit maxCrypto Schlüssel	ja	HBA durch HBA eines anderen Anbieters austauschen	Vorhandene Daten werden gelöscht*, neue Daten werden nicht verschlüsselt

** nach Bestätigung durch den Benutzer*

adaptec by PMC

PMC-Sierra, Inc.
1380 Bordeaux Dr.
Sunnyvale, CA 94089 USA
Tel: +1 (408) 239-8000

Im Internet unter: www.adaptec.com
Kundenservice vor dem Verkauf:
USA und Kanada: Tel.: +1 (800) 442-7274 oder Tel.: +1 (408) 957-7274 oder per E-Mail an adaptecsales@pmcs.com
Deutschland: Tel.: +49-89-45640621 oder per E-Mail an adaptecsales.germany@pmcs.com
Großbritannien: Tel.: +44-845 2668773 oder per E-Mail an uk_sales@pmcs.com
Australien: Tel.: +61-2-90116787
Singapur: Tel.: +65-92351044