Sicheres automatisches Schlüsselmanagement mit TDE und HSMs

Mario Galatovic
Senior Systems Engineer Central Europe
Thales eSecurity Ltd.
Frankfurt

Schlüsselworte:

Hardware Security Module, HSM, Encryption, Verschlüsselung, Schlüssel, Keys, Masterkey, Transparent Data Encryption, TDE, Key Management, Compliance

Einleitung:

Der Druck auf Unternehmen und Behörden, ihre Daten zu schützen, nimmt ständig zu. Gesetze wie die BDSG Novelle 2 stellen klare Bedingungen an den Datenschutz. Spätestens durch die letzten Datenpannen in Deutschland und der Schweiz ist klar, dass Unternehmen mehr als nur Firewalls und Virenschutzprogramme einsetzen müssen. Dieser Vortrag stellt die Möglichkeiten dar, wie Daten in Oracle-Datenbanken mit Oracle-eigenen Mitteln verschlüsselt werden können. Er zeigt auf, was Unternehmen bei der Schlüsselverwaltung beachten sollten und wie durch Einsatz von sogenannten Hardware Security Modulen eine hochsichere Lösung entsteht, die Unternehmen klare Vorteile bei der Erfüllung der gesetzlichen Vorgaben gibt und weitestgehenden Schutz ihrer Unternehmens- und Kundendaten bietet.
Teilnehmer lernen: Was ist Oracle Transparent Data Encryption und wie wird diese eingesetzt. Was sind die Unterschiede zwischen Column- und Tablespace-Verschlüsselung? Was muss ich bei der Schlüsselverwaltung beachten? Was ist ein Hardware Security Module (HSM) und welche Unterschiede gibt es? Wie binde ich ein HSM in die Oracle Datenbank ein? Wie hilft mir dies bei der Erreichung der rechtlichen Vorgaben und Audits?

Transparent Database Encryption

Um den steigenden Sicherheitsanforderungen gerecht zu werden, wird mittlerweile an vielen Stellen eine Verschlüsselung eingesetzt. Nicht nur im Zahlungsverkehr oder bei E-Mails, sondern auch vermehrt bei der Verwendung und Speicherung von Daten. Das geistige Eigentum eines Unternehmens sowie Daten der Mitarbeiter und Kunden sind heute das wichtigste -und somit schützenswerteste- Gut geworden. Dabei sind nicht nur Produktions-, personenbezogene und Finanzdaten schützenswert, sondern alles, was nicht morgen in der Zeitung stehen soll.
Daten können auf vielfältige Weise in die falschen Hände geraten. Sie befinden sich z.B. auf verlorenen oder gestohlenen Laptops, auf Backup-Tapes, die sich auf dem Weg zu ihrem Bestimmungsort verirren, oder werden von enttäuschten Mitarbeitern missbraucht, um sich einen persönlichen Vorteil zu verschaffen oder dem Unternehmen zu schaden. Dies sind nur ein paar Beispiele aus dem täglichen Leben und viele dieser Fälle tauchen leider immer wieder in den Medien auf.
Mit wachsenden Datenmengen und der Weiterentwicklung der Computersysteme steigt das Bedrohungspotential, dem sich Unternehmen stellen müssen.

Eine optimale Möglichkeit, sensible und wichtige Daten zu schützen, ist die Verschlüsselung dieser Daten. Oracle bietet, neben vielen anderen Funktionen, auch den Einsatz einer Verschlüsselung an. Viele Bedrohungen verschwinden, wenn die Daten verschlüsselt sind. Allerdings müssen nicht immer alle Daten eines Unternehmens so geschützt werden, sondern nur gezielt Informationen, die zum Beispiel Finanzdaten enthalten.

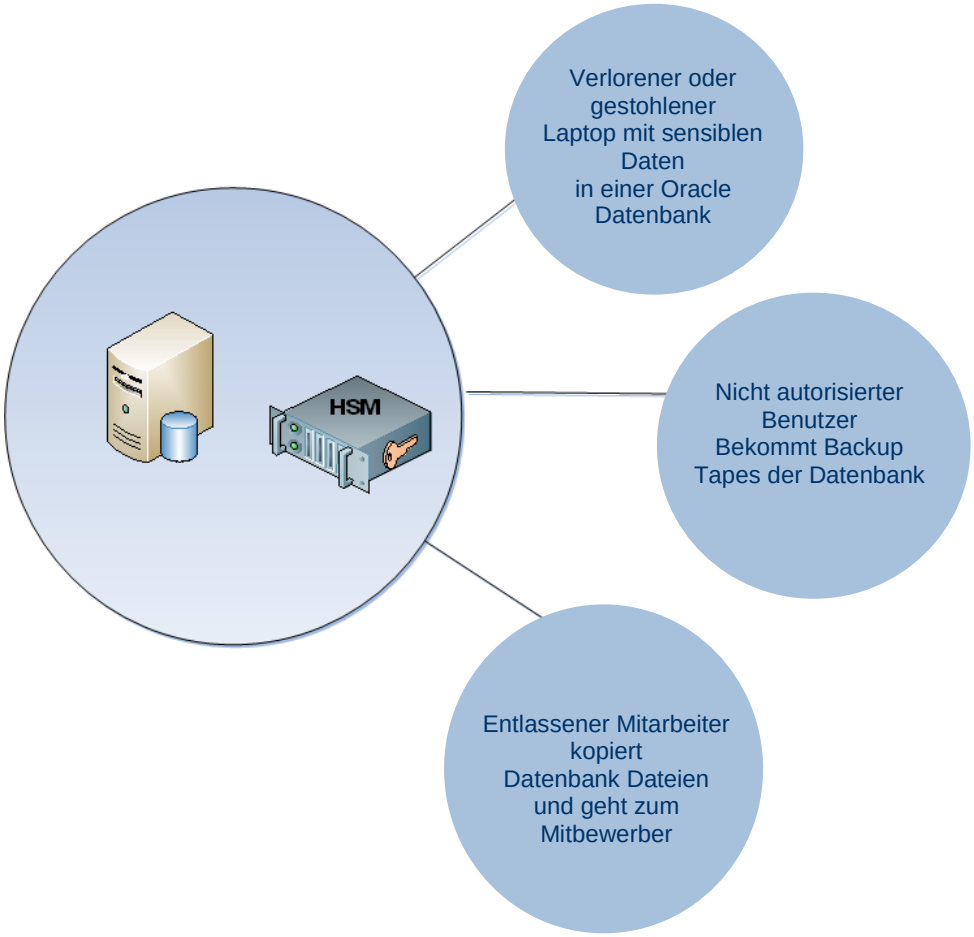

Abb. 1: Bedrohungen der Informationen

Um diesem Umstand gerecht zu werden, hat Oracle die Transparent Database Encryption, auch TDE genannt, eingeführt.
TDE bietet die Möglichkeit, einen Teil Ihre Daten zu verschlüsseln. Sie haben die Wahl, einzelne Tabellen oder auch innerhalb einer Tabelle z.B. einzelne Spalten oder Felder mit sensiblen Informationen zu schützen. Stellen Sie sich vor, Sie speichern Kundendaten und Informationen zu den Käufen dieser Kunden. Innerhalb dieser Informationen sollten die Kundendaten und eventuell auch die Preise gesondert gesichert sein. Der Teil, der Ihre Produkte beschreibt, ist möglicherweise nicht besonders schützenswert, wenn diese Informationen im Internet frei zugänglich sind. Mit der Transparent Database Encryption haben Sie genau diese Möglichkeit. Sie entscheiden, welche Teile Sie schützen möchten.
Auch gesetzliche Vorgaben spielen hier eine Rolle. Zum Beispiel können das Datenschutzgesetz, PCI/DSS (Payment Card Industry / Data Security Standard) oder andere Auflagen vorschreiben, dass bestimmte Informationen verschlüsselt gespeichert werden müssen.

Hardware Security Module

Die Transparent Database Encryption bringt Sie auf dem Weg zur sicheren Datenhaltung ein gutes Stück nach vorne. Um aber die Sicherheit auf ein höheres Level zu heben, muss man die Schlüssel, die für diese Verschlüsselung verwendet werden, näher betrachten. Selbst die beste Verschlüsselung der Welt ist nutzlos, wenn der Schlüssel hierzu zugänglich ist.
Aus diesem Grund bietet es sich an, ein Hardware Security Modul (HSM) zu verwenden. Mit den verschiedenen HSMs der Firma Thales werden diese Schlüssel, die von der Oracle Datenbank, bzw. der TDE verwendet werden, von der Datenbank separiert. Die Schlüssel werden nicht mehr auf dem Server gespeichert, sondern in einem von Oracle zertifiziertem hochsicheren Hardware Security Modul.
Stellen Sie sich vor, jemand bekommt Zugang zu den Backup-Daten. Die sensiblen Teile dieses Backups sind über TDE verschlüsselt. Sollte aber auch der Schlüssel dazu in diesem Backup vorhanden sein, besteht nun die Gefahr, diese unternehmenskritischen Daten zu entschlüsseln. Liegen die Schlüssel zu diesen Informationen in einem Hardware Security Modul besteht keine Möglichkeit mehr, an die Informationen zu gelangen. Die FIPS- und Common Criteria-zertifizierte Hardware, die zusätzlich durch SmartCards geschützt ist, bietet Ihnen somit einen zusätzlichen Schutz, der Ihnen hilft, die gesetzlichen oder von der Industrie vorgegebenen Auflagen zu erfüllen.
Der Installationsaufwand für ein (oder mehrere) Hardware Security Modul(e) ist gering. Die Vorteile, die sich durch die Installation bieten, sind enorm. Neben dem zusätzlichen Schutz Ihrer wertvollen Informationen erfüllen Sie so Sicherheitsvorgaben und erleichtern wesentlich Audits und Revision. Dieser Vorteil übertrifft bei weitem den Aufwand der nötig ist.
Für die Benutzer der Datenbank oder anderer Applikationen ist dieser Vorgang natürlich vollkommen transparent.

Weitere Funktionalitäten der Hardware Security Module

Ein Hardware Security Modul bietet noch andere, über die reine Schlüsselhaltung hinausgehende Vorteile: von der Schlüsselgenerierung über symmetrische und asymmetrische Verschlüsselungen, bis hin zu digitalen Signaturen, Authentifizierungen und einem Schlüssel-Management. Die revisionssichere Speicherung und die Fähigkeit, den kompletten Lebenszyklus Ihrer Schlüssel, von Generierung über Nutzung und Speicherung, bis hin zur Löschung, zu begleiten, gibt Ihnen die Möglichkeit die vorhandenen Gesetze und Auflagen auf einfache Weise zu erfüllen.
Durch eine Vielzahl von Schnittstellen können Sie Hardware Security Module nicht nur schnell und einfach mit Ihrer Oracle Datenbank verbinden, sondern auch mit Ihren anderen geschäftskritischen Applikationen nutzen. Die verschiedenen HSMs können mit Ihren selbst entwickelten Applikationen agieren oder diese sogar innerhalb dieser Hardware laufen zu lassen, um sie so gegen Attacken zu schützen.

In größeren Netzwerken sind auch Funktionalitäten wie Fail-Over, Load-Balancing oder ein Remote-Zugriff auf die HSMs wichtig.
Thales bietet Hardware Security Module in vielen verschiedenen Bauformen und Geschwindigkeiten. Vom USB-Gerät, das zum Beispiel zum Testen verwendet werden kann über PCI- oder PCI-Express-Steckkarten für Server bis hin zu Netzwerkgeräten oder jeder denkbaren Kombination daraus. Wir haben das passende Gerät für Ihr Einsatzgebiet im Portfolio.

Abb. 2: Verschiedene Bauformen der Hardware Security Module

Ergänzt werden die Hardware Security Module durch andere Hardware-Komponenten aus unserem Haus, die sich den Themen Schlüssel-Management für Storage (TEMS), Tape-Verschlüsselung, SSL Beschleunigung, Zeitstempel, Leitungsverschlüsselung oder Authentifizierung in heterogenen Umgebungen annehmen.

Unsere Security Lösungen schützen mittelständische Unternehmen, internationale Konzerne und öffentliche Institutionen. So setzten vier von fünf der größten Energieanbieter und Luftfahrtunternehmen auf die Thales Lösungen. Sie werden in 22 NATO-Ländern eingesetzt und schützen weltweit über 80 % der Zahlungstransaktionen.

Kontaktadresse:

Mario Galatovic
Thales eSecurity Ltd.
Herriot Str. 1
D-60528 Frankfurt am Main

Telefon: +49 (0) 7252 / 84113
E-Mail: mario.galatovic@thales-esecurity.com
Internet: http://iss.thalesgroup.com/