PCI/DSS
Security Compliance im Zahlungsverkehr mit HSMs

Jochen Belke
Thales eSecurity Ltd
Frankfurt

Schlüsselworte:

Hardware Security Module, HSM, PCI/DSS, Verschlüsselung, Schlüssel, Keys, Masterkey, Key Management, Zahlungsverkehr, e-banking, Sicherheit, Encryption, Banken, Compliance, Security, Kreditkartendaten, sicheres Online Banking

Einleitung:

Jeder Bankenkunde erwartet, dass seine Kundendaten und Transaktionen über online Banking, Kredit- oder EC-Karte sicher sind und nicht von Unbefugten eingesehen oder manipuliert werden können. Doch wie sicher ist sicher? Haben Sie alles getan?
Regulierungen wie der Payment Card Industry Data Security Standard (PCI/DSS) setzen hier klare Bedingungen für den Datenschutz.

Sie erhalten Antworten auf folgende Fragen und wie Sie die Anforderungen des PCI/DSS Standards umsetzen:
Wie erreichen Sie diesen Schutz und PCI/DSS Compliance?
Wie verbessern Sie den Schutz Ihrer sensiblen Kundendaten?
Was sind hierbei die wichtigsten Anforderungen an Key-Management, Sicherheit und Reporting?
Welche Appliances sind verfügbar, um Daten in Banken-Applikationen, Datenbanken und im Backup zu sichern?
Wie reduzieren Sie Aufwand und Kosten durch ein automatisches Schlüsselmanagement und dedizierte Hardware Security Module?

Verschlüsselung im Unternehmen

Verschlüsselungen werden mittlerweile an vielen Stellen im Unternehmen eingesetzt. Auch, wenn die Ziele dieser Verschlüsselungen verschieden sein können, sind die Kernanforderungen in den meisten Unternehmen und Institutionen der Schutz persönlicher Daten, die Integrität von Daten und eine starke Authentifizierung
Für jeden dieser Punkte gibt es heute verschiedene Lösungsansätze. Man kann Daten mit Software verschlüsseln, Datenbanken wie Oracle können intern verschlüsseln, Tape-Drives – oder Storage-Devices allgemein - bieten die Möglichkeit zu verschlüsseln und Notebooks haben eine integrierte Lösung, um die Daten vor fremdem Zugriff zu schützen. Diese Ansätze lassen sich beliebig fortführen, wenn man nur an E-Mails und Internet denkt.
Alle diese Lösungen funktionieren – für sich betrachtet. Doch was passiert mit den Schlüsseln dieser Insellösungen? Jede Verschlüsselung benötigt Schlüssel und jeder Schlüssel muss verwaltet werden. Die Schlüssel sind der zentrale und kritische Punkt in jedem Unternehmen. Sobald sich eine unbefugte Person Zugang zu den Schlüsseln verschaffen kann, hat diese Person Zugang zu sämtlichen Daten. Das bedeutet, die Schlüssel müssen nicht nur erzeugt und verwendet werden, sondern sie müssen über ihren kompletten Lebenszyklus geschützt und betreut werden.

Der Weg und die Kosten

In vielen Unternehmen stellt sich die Frage, wo man am besten anfangen soll und welchen Weg man einschlägt. Dabei spielen viele Faktoren eine Rolle. Wie sieht die Infrastruktur aus, welche

Applikationen und Datenbanken werden betrieben, welche Daten werden gespeichert? Zusätzlich müssen die gesetzlichen Vorgaben eingehalten werden und je nach Daten und Verwendungszweck kommen Vorgaben der Industrie zum Tragen. PCI/DSS, eine Vorgabe der Kreditkartenunternehmen, ist für ein Unternehmen, das Kreditkarteninformationen verarbeitet und speichert, eine der wichtigsten Vorgaben.

In der Praxis sieht man recht häufig, dass mit der Absicherung bei den Web-Servern begonnen wird. Über diese Server hat ein Kunde möglicherweise den ersten Online-Kontakt mit einem Unternehmen, das zur Absicherung der Kommunikationsverbindung dort eine SSL-Verschlüsselung nutzt. Der nächste Schritt wäre die Frage nach den Backups der Web-Server. Auch dort sollen die Daten verschlüsselt gespeichert werden. Entscheidend wird es bei Online-Shops, die meist eine direkte Verbindung zu einer Oracle-Datenbank haben. Sobald es um Zahlungsabwicklung geht, greifen die Regularien des PCI/DSS. Sensible Daten müssen sowohl auf der Leitung als auch im gespeicherten Zustand verschlüsselt sein, außerdem verlangt die interne oder externe Revision ein entsprechendes Reporting. Eingesetzte Lösungen sind möglicherweise über verschiedene Rechenzentren an mehreren Standorten verteilt und müssen hochverfügbar sein.

Verschlüsselung ist ein essentieller Bestandteil dieser Überlegungen. In dieser Kette wird an vielen Stellen verschlüsselt und viele Schlüssel werden verwendet. Um nur einige zu nennen:
Web-Server Zertifikate, Datenbankschlüssel, PCI-Schlüssel und Backup-Schlüssel. Für jeden dieser Punkte stellt sich die Frage nach Erneuerung, Backup, Logs, Prüfung, Verfügbarkeit und Ausfallsicherheit.
Wenn keine zentrale Verwaltung aller dieser Komponenten vorhanden ist, können verschiedene teure oder unternehmenskritische Szenarien eintreten. Ein nicht vorhandenes Web-Zertifikat kann dazu führen, dass die Web-Server über Stunden nicht verfügbar sind und Kunden keine Transaktionen durchführen können. Durch nicht automatisierte Prozesse besteht die Gefahr, dass auf Backups der letzten Jahre nicht mehr zugegriffen werden kann. Nicht dokumentierte Schlüsselwechsel können bewirken, dass die Revisionsprüfung nicht bestanden wird und teilweise sehr hohe Strafen zu zahlen sind.
Aus diesen Gründen ist ein zentrales Schlüssel-Management ein Kernpunkt der Überlegungen auf dem Weg zur Compliance mit PCI/DSS. Wenn Schlüssel nicht vorhanden sind, dann sind es die Daten auch nicht.

Abb. 1: Schlüsselverwaltung heute

PCI/DSS – Payment Card Industry / Data Security Standard

PCI/DSS ist ein Regelwerk, das alle wichtigen Kreditkartenorganisationen unterstützen. Handelsunternehmen und Dienstleister, die Kreditkarten-Transaktionen speichern, übermitteln oder abwickeln, müssen die Anforderungen erfüllen. Halten sie sich nicht daran, können Strafgebühren verhängt, Einschränkungen ausgesprochen oder ihnen letztlich die Akzeptanz von Kreditkarten untersagt werden.

Das Regelwerk umfasst 12 Bereiche, die in Unterpunkten genauer definiert sind. Ein Beispiel aus diesen Punkten sieht so aus:

PCI-Anforderung 3: Schützen der Daten des Karteninhabers

PCI-Anforderung 3.5: “Schützen der Schlüssel, die für die Verschlüsselung der Daten des Karteninhabers verwendet werden gegen Offenlegung und Missbrauch.”

3.5.1 “Zugriff auf Schlüssel an möglichst wenige Verwalter geben.”

3.5.2 “Speicherung der Schlüssel an möglichst wenigen Plätzen und in möglichst wenigen Formen.”

PCI-Anforderung 3.6 “Volle Dokumentation aller Key-Management-Prozesse und Prozeduren.”

3.6.1 Generierung starker Schlüssel

3.6.2 Sichere Schlüsselverteilung

3.6.3 Sichere Schlüsselspeicherung

3.6.4 Periodischer Schlüsseltausch

3.6.5 Zerstörung alter Schlüssel

3.6.6 Geteiltes Wissen und Erstellung von doppelter Kontrolle der Schlüssel

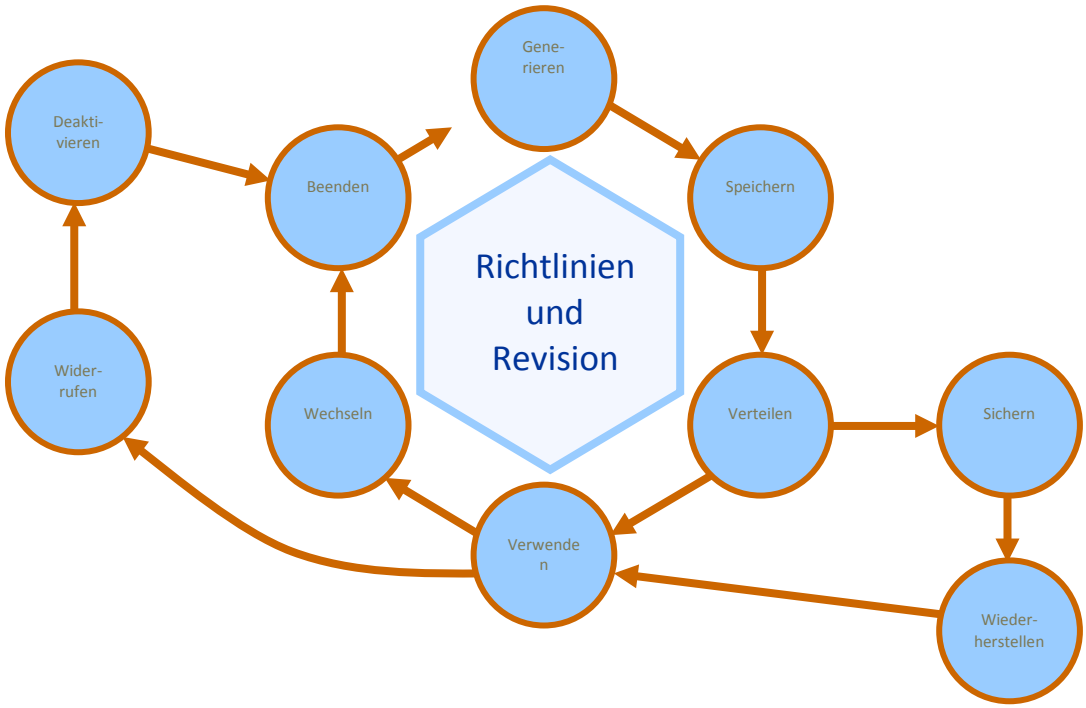

Abb. 2.: Lebenszyklus der Schlüssel

Hardware Security Module

Um die Anforderungen von PCI/DSS zu erfüllen, müssen verschiede Komponenten eingesetzt werden. Eine zentrale Komponente ist ein Hardware Security Modul (HSM). Mit den verschiedenen HSMs der Firma Thales können die Schlüssel, die von der Oracle Datenbank, bzw. der TDE, des Web-Servers und der anderen Komponenten der Infrastruktur nicht nur sicher gespeichert, sondern auch verwaltet werden. Die Schlüssel werden dann nicht mehr auf dem Server gespeichert, sondern in einem von Oracle zertifiziertem, hochsicheren Hardware Security Modul. Die FIPS- und Common Criteria-zertifizierte Hardware, die zusätzlich durch SmartCards geschützt ist, bietet Ihnen den Schutz, die gesetzlichen oder von der Industrie vorgegebenen Auflagen, wie PCI/DSS, zu erfüllen.

Der Installationsaufwand für ein (oder mehrere) Hardware Security Modul ist gering. Die Vorteile, die Sie durch die Installation haben sind enorm. Nicht nur der zusätzliche Schutz Ihrer wertvollen Informationen, sondern auch die Vorteile mit HSMs den Anforderungen der Revision oder den Regularien gerecht zu werden, übertreffen bei weitem den Aufwand der nötig ist.
Für die Benutzer der Datenbank oder anderer Applikationen ist dieser Vorgang vollkommen transparent.

Weitere Funktionalitäten der Hardware Security Module

Natürlich bietet ein Hardware Security Modul auch noch andere, über die reine Schlüsselhaltung weit hinausgehende Möglichkeiten: von der Schlüsselgenerierung über symmetrische und asymmetrische Verschlüsselungen, bis hin zu digitalen Signaturen, Authentifizierungen und einem Schlüssel-Management. Die revisionssichere Speicherung und die Möglichkeit, den kompletten Lebenszyklus Ihrer Schlüssel, von Generierung über Nutzung und Speicherung, bis hin zur Löschung, zu begleiten, erlaubt Ihnen, 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 der Fa. Thales bieten die Möglichkeit, mit Ihren selbst entwickelten Applikationen zu agieren oder diese Applikationen sogar innerhalb dieser Hardware laufen zu lassen, um sie 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 Ihnen Hardware Security Module in vielen verschiedenen Bauformen und Geschwindigkeiten. Vom USB-Gerät, das zum Beispiel für Testzwecke verwendet werden kann über PCI oder PCI-Express-Steckkarten für den Server bis hin zu Netzwerkgeräten oder jeder denkbaren Kombination daraus. Wir haben das passende Gerät für Ihr Einsatzgebiet im Portfolio.

Abb. 3: Verschiedene Bauformen der Hardware Security Module

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

Unsere Hardware Security Module schützen, im Mittelstand bis hin zu den weltgrößten Unternehmen, öffentlichen Institutionen und Militär, sensible Daten rund um den Globus.

Auch im Zahlungsverkehr, sei es bei Banken oder bei Online-Transaktionen nimmt Thales eine führende Stellung ein und unterstützt bei der Einhaltung der PCI/DSS Richtlinien.

Kontaktadresse:

Jochen Belke
Thales eSecurity Ltd.
Herriot Str. 1
D-60528 Frankfurt am Main

Telefon: +49 (0) 69 / 6773 3166
E-Mail Jochen.Belke@thales-esecurity.com
Internet: http://iss.thalesgroup.com/