Informationssicherheit ist wichtiger denn je, um Kundenvertrauen zu erhalten und erfolgreich zu sein. Compliance und Verschlüsselungstechnologien sind Termini, die für Unternehmen stetig wichtiger werden. Sie müssen ihre vertraulichen Daten von Mitarbeitern und Kunden beziehungsweise Lieferanten schützen und diesen Schutz im Zweifelsfall auch nachweisen können. Dieser Artikel zeigt auf, wie Auditoren diese Herausforderung bewerten und wo Unternehmen heute stehen.

Was Auditoren über Compliance und Verschlüsselungstechnologien denken

Mario Galatovic, Thales e-Security

Der Schutz von persönlichen Daten wird immer wichtiger, wie in jüngster Vergangenheit auch in der Presse zu verfolgen war. Im Jahr 2009 verabschiedete der Deutsche Bundestag die Novelle II des Bundesdatenschutzgesetzes (BDSG), wodurch Unternehmen verpflichtet wurden, sich öffentlich zu Datenpannen zu bekennen. Ähnliche Gesetzgebungen wie die California Senate Bill 1386 in den USA oder der Data Protection Act im Vereinigten Königreich führten zu einer deutlichen Straffung der Sicherheitsmaßnahmen von Unternehmen und Behörden. Mit der Änderung des BDSGs wird dieser Trend auch in Deutschland spürbar. Auditoren weisen ausdrücklich darauf hin, dass Verschlüsselung hilft, Compliance gegenüber dem BDSG zu erreichen und Geschäftsabläufe vor Risiken zu schützen. Darüber hinaus sind Unternehmen nicht verpflichtet, Datenpannen zu melden, wenn die kompromittierten Daten über entsprechende Mechanismen verschlüsselt und damit unlesbar sind. Aus diesem Grund betrachten Auditoren entsprechende Systeme sehr genau.

Sicherheits-Audit

In der Regel verfügen Auditoren, die Unternehmen prüfen, über einen tiefen Wissensschatz und eine langjährige Erfahrung. Sie sind in der Lage, sowohl die eingesetzten Praktiken zum Erreichen von Compliance als auch den Einsatz von Verschlüsselungslösungen für dieses Ziel zu analysieren. Diese Auditoren nehmen die Nutzung von Verschlüsselungstechnologien wie beispielsweise einer Public-Key-Infrastruktur sehr positiv an. Dies belegt die Studie „What Auditors think about Crypto“, die im Mai 2011 vom Ponemon Institute durchgeführt wurde (siehe Abbildung 1). Ein Compliance-Audit oder Assessment wird in der Regel durchgeführt, um Risiken und Sicherheitslücken zu identifizieren oder die Compliance mit Regularien und Vorschriften zu bestätigen. Es bleibt die Frage, wer das Obligo und das Budget für die entsprechende Umsetzung trägt.

Compliance-Budget und Verantwortung

Unternehmen, die sich der Gefahr bewusst sind, Daten zu verlieren und dadurch einen Imageverlust zu erleiden, müssen das entsprechende Budget für die Implementierung sicherer Technologien zur Verfügung stellen. Auditoren sind laut der früheren Studie „PCI DSS Trends 2010“, die vom Ponemon Institut erstellt wurde, der Meinung, dass die Entscheidungshoheit für das Compliance-Budget in der Regel im Aufgabengebiet des Business Unit Managers liegt. Dieser hat damit auch die Entscheidungsfähigkeit, das Sicherheits-Budget an die wachsenden Anforderungen anzupassen und eine strategische Ausrichtung zu beschließen. Die Verantwortlichkeit für das Einhalten diverser Compliance-Anforderungen wie der Payment Card Industry Data Security Standard (PCI DSS), der Health Insurance Portability and Accountability Act (HIPAA) oder das BDSG liegt allerdings häufig in speziellen „Compliance & Audit“-Teams, wel-

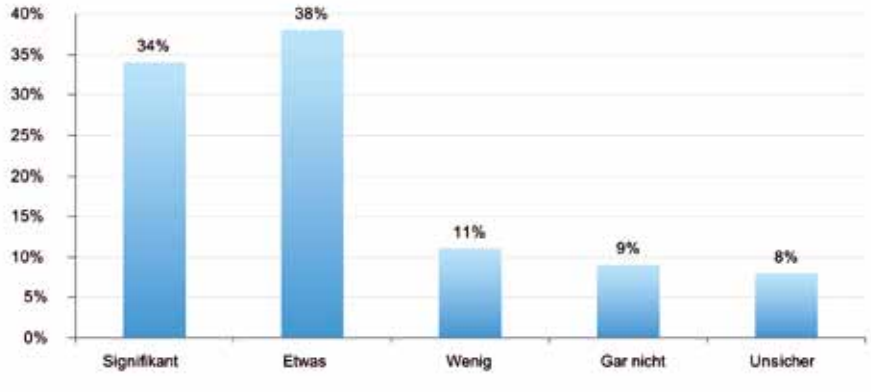

Abbildung 1: Wie die Nutzung von Verschlüsselungslösungen die Wahrnehmung der Auditoren positiv beeinflusst (Quelle: What Auditors think about Crypto, May 2011, Ponemon Institut)

che gegebenenfalls dediziert für diese Aufgabe gebildet werden.

Gefahren und Risiken für Compliance

Datensicherheit und damit auch Compliance ist am meisten bei Applikationen, externen Mitarbeitern, mobilen Geräten, Laptops und externen Geschäftspartnern gefährdet. Dies sind häufig auch die Bereiche, in denen die Compliance-Anforderungen versagen (siehe Abbildung 2). Laut der Studie „What Auditors think about Crypto“ sind Cloud-Computing-Anbieter das größte Risiko für Unternehmen. Diesen folgen das Outsourcen von Dienstleistungen und Cloud-Computing-Dienste für Plattform-Dienste. Ein weiterer entscheidender Faktor bei der Analyse der wachsenden Anforderungen und steigenden Risiken ist, dass die notwendigen Budgets nicht vorhanden sind, um die richtigen technischen Hilfsmittel zu implementieren.

Technische Hilfsmittel und Compliance

Die Compliance-Anforderungen lassen sich durch völlig unterschiedliche Hilfsmittel erfüllen. Diese reichen vom sogenannten „Need-To-Know-Prinzip“ über die Installation und Wartung von Firewalls bis hin zur Verschlüsselung unterschiedlicher Daten. Verschlüsselungstechnologien werden als essenzielles und bestes Werkzeug angesehen, um die Informationssicherheit auf ein akzeptables Niveau zu heben. Verschlüsselung kann auf unterschiedlichen Ebenen des Datenflusses erfolgen. Sie kann in öffentlichen Netzwerken, Datenbanken, in Storage Area Networks (SANs) oder externen Speichermedien, in Datenbanken, aber auch auf mobilen Endgeräten eingesetzt werden. Verschlüsselung der Information ist jedoch nur die halbe Miete, denn Verschlüsselung ist nur so gut wie das Management und die Sicherung der verwendeten Schlüssel. Werden bei einer Datenpanne zusätzlich zu den verschlüsselten Daten auch die verwendeten Schlüssel kompromittiert, ist der Schutz unwirksam, da die Daten entschlüsselt werden können. Durch diese Resultate bleibt die Frage, wo Unternehmen sich heute befinden und wohin der Weg führt.

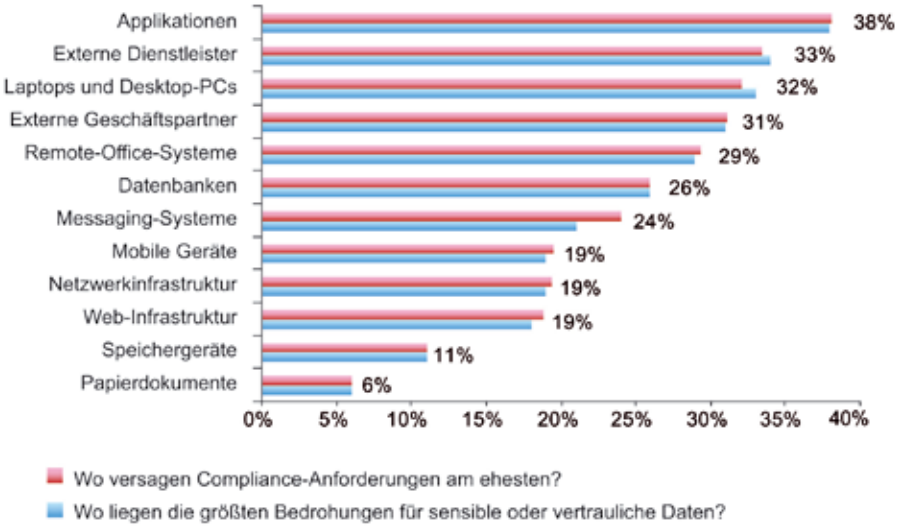

Abbildung 2: Wo Compliance-Anforderungen versagen und wo die größten Gefahren liegen (Quelle: What Auditors think about Crypto, May 2011, Ponemon Institut)

Wo stehen Unternehmen heute?

Nicht nur durch die zuletzt bekannt gewordenen Angriffe auf Unternehmen wie RSA, Sony oder die CIA wächst die Angst von Unternehmen, sensible Daten ungewollt zu veröffentlichen (siehe Abbildung 3).

Hinzu kommt, dass Themen wie Datenschutz und Datensicherheit zunehmend in den Fokus drängen und sich mittlerweile die Vertrauenswürdigkeit eines Unternehmens durch diese kennzeichnet. Dies lässt ableiten, dass ohne entsprechenden Schutz für Informationen die Kundenbasis verloren geht und einem Unternehmen raue Zeiten bevorstehen können. Daher werden diese Themen von seriös geführten Unternehmen sehr ernst genommen und entsprechende Schutzmaßnahmen bereits eingeleitet. In aller Regel setzen Unterneh-

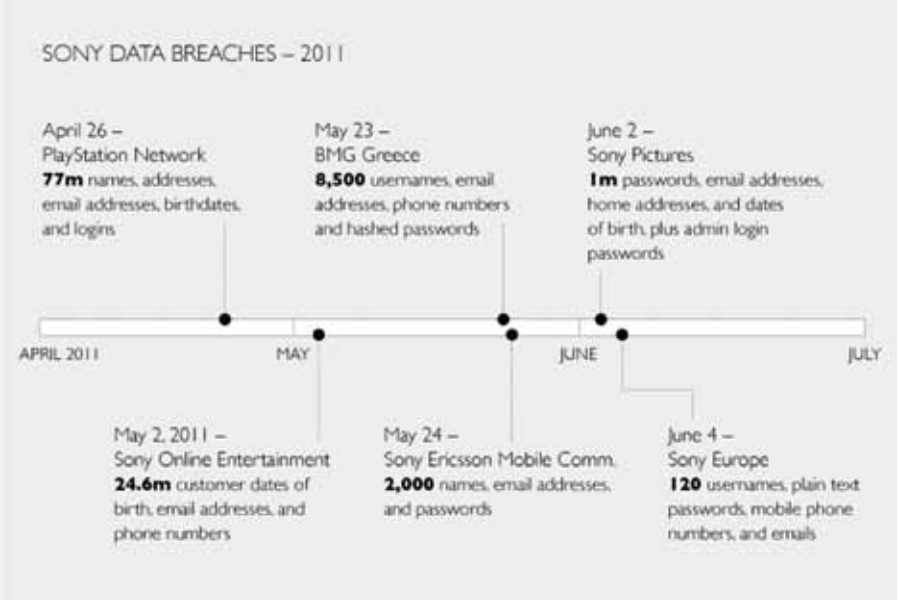

Abbildung 3: Timeline der bekannten Datenverluste von Sony (Quelle: http://flowingdata.com)

men dabei die höchste Priorität auf die Einhaltung regulatorischer Vorgaben sowohl des Gesetzgebers als auch interner Policies. Dabei stehen Unternehmen häufig vor dem Problem, die lückenlose Erfüllung der Compliance-Anforderungen zu bewerkstelligen, ohne dabei das vorhandene Budget für Sicherheit zu überlasten. Als Quintessenz lässt sich aus diesen Umständen ableiten, dass vor allem der Einsatz von bereits zertifizierten Hardware-Security-Modulen mit entsprechender Verschlüsselung die Compliance erhöht und dabei die Kosten auf Dauer reduziert werden.

Welche Empfehlungen lassen sich ableiten?

Aus den beschriebenen Entwicklungen lassen sich die abzuleitenden Empfehlungen am besten an einem Beispiel nachvollziehen. Nehmen wir hierzu eine Oracle-Datenbank mit Transparent Data Encryption (TDE) als Teil der Advanced-Security-Option. Damit ist es möglich, Daten transparent für Applikationen zu verschlüsseln. Jedoch stellen die Verwaltung und Aufbewahrung des Schlüsselmaterials ein entscheidendes Kriterium für den Erfolg dieser Verschlüsselungslösung dar. Hardware-Sicherheitsmodule (HSM) sind eine Kernkomponente dessen und bieten große Vorteile im Betrieb, bei Sicherheit und Compliance-Audits. Durch den Einsatz von HSMs wird das Management von Schlüsselmaterial auf dedizierten Geräten zusammengeführt, zentralisiert und automatisiert, wodurch die operativen Kosten reduziert werden. Systeme werden beliebig skalierbar, da HSMs die Möglichkeiten bieten, Hunderte Datenbanken auf einmal zu verwalten, und eine kurz- und langfristige Wiederherstellung von Daten erst dadurch sicher erreichbar ist.

Die IT-Sicherheit wird durch HSMs erhöht, da sie die Hauptschlüssel durch nicht angreifbare Hardware schützen und besonders sensible Anwendungen innerhalb einer HSM ablaufen können. Dadurch liefern sie eine wartungsfreie, deutlich höhere Sicherheit als softwarebasierte Lösungen (siehe Abbildung 4). Erst HSMs ermöglichen die Trennung von Zuständigkeiten oder die Einführung eines Mehr-Augen-Prinzips für sicherheitskritische Tätigkeiten und verbessern dadurch die betrieblichen Kontrollmöglichkeiten beziehungsweise reduzieren das Risiko von Missbrauch.

HSMs sind als Best Practice für Sicherheit anerkannt. Sie unterstützen eine automatische, zentrale Schlüsselverwaltung, beschleunigen den Schlüsselwechsel und vereinfachen eine Revision. Dadurch reduzieren sie Aufwendungen von Governance, Risk und Compliance (GRC).

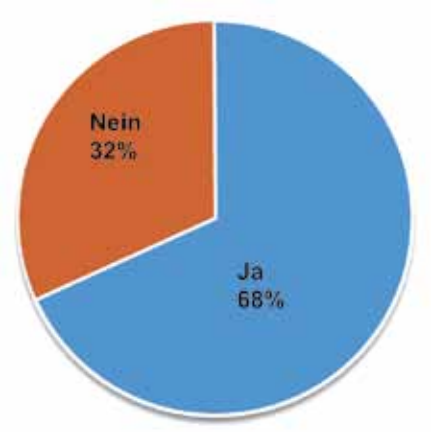

Abbildung 4: Verringert der Gebrauch von Hardware-Security-Modulen zur Verschlüsselung und Schlüsselverwaltung den Zeitaufwand, um Compliance nachzuweisen? (Quelle: What Auditors think about Crypto, May 2011, Ponemon Institut)

Fazit

HSMs können eine Lösung mit internationalen Sicherheits-Zertifizierungen wie „FIPS 140-2“ und „Common Criteria“ ausstatten. Gerade deswegen bewerten Auditoren den Einsatz von HSMs – und dadurch ein kontrollierbares Management von Schlüsseln – als entscheidend für das Erreichen von Compliance-Anforderungen wie BDSG oder PCI DSS.

Mario Galatovic
Thales e-Security
mario.galatovic@thales-esecurity.com