

**Nachrichten über Datendiebstahl erscheinen immer häufiger in den Medien. Bei einer US-Kreditkartenabrechnungsfirma sind rund 40 Millionen Karteninhaber von einem Datendiebstahl betroffen, in Europa sind in jüngster Vergangenheit bei einer Edelbekleidungs-Marke 180.000 Kreditkartennummern aufgrund von IT-Sicherheitslücken entwendet worden. Vorfälle dieser Art häufen sich zunehmend, und Angriffe kommen nicht nur von aussen.**

Aus diesem Grund haben bereits die Kreditkartengesellschaften mit verschärften Sicherheitsrichtlinien reagiert. Master Card und VISA haben gemeinsam den "Payment Card Industry Data Security Standard" (PCI) adaptiert, um Händler, Issuer, Acquirer und Prozessoren zu mehr Sicherheit zu verpflichten. Im Gegensatz zur Standards wie 3D Secure oder SPA/UCAF, die sich mit dem Sichern von Zahlungs-Transaktionen befassen, liegt der Fokus von PCI auf der internen IT-Infrastruktur und deren Sicherheit.

Traditionelle IT Sicherheitsmassnahmen haben ihren Fokus auf der Zugriffskontrolle von Netzwerken, Betriebssystemen und Datenbanken. Jedoch sind traditionelle Maßnahmen oft unzureichend, um sensiblen Daten Schutz gegen Attacks und Entwendungen bieten zu können. Oft sind es kleine Sicherheitslücken in Betriebssystem oder Datenbank, die es ermöglichen, einen unbefugten, uneingeschränkten Zugriff auf die Systeme zu bekommen.

Aus diesem Grund ist die Verschlüsselung der gespeicherten Karteninformationen ein wichtiger Bestandteil der PCI Standards. Dies soll verhindern, dass lesbare Kreditkarteninformationen an Dritte gelangen können, z.B. durch Diebstahl von Sicherungsmedien oder Infiltration (Einhacken) in ein Datenbank System.

Das Verschlüsseln von Daten erfordert einen gut durchdachten Mechanismus zur Speicherung von Schlüsseln. Wenn ein Schlüssel gestohlen wird, sind sensible Daten nicht mehr sicher. Nach dem Motto "Wie sicher ist Ihr Haus, wenn der Schlüssel unter der Fussmatte liegt?" ist es verständlich, dass besondere Aufmerksamkeit von PCI auf der sicheren Verwaltung von Schlüsseln liegt. Zudem ist eine lückenlose Nachvollziehbarkeit sämtlicher kryptografischer und administrativer Operationen notwendig, um schnell eventuellen Missbrauch entdecken zu können.

Für die Anforderung, die PCI an die IT Infrastruktur stellt, ist die DataSecure Plattform von Ingrian Networks die optimale Lösung. DataSecure ist eine Netzwerk Appliance, die eine kryptografische Engine, Schlüsselverwaltung und Auditing in einer einbruchssicheren Plattform zentralisiert. CPU-intensive Ver- und Entschlüsselungsvorgänge werden auf die DataSecure Plattform ausgelagert. Somit sind oftmals notwendige Anwendungs- und

Datenbankserver Hardware Upgrades überflüssig.

Die flexible Architektur der DataSecure Plattform ermöglicht eine Implementierung, die optimal auf die jeweilige Architektur und die zur Verfügung stehenden Ressourcen abgestimmt ist. Die Verschlüsselung kann vom Web- oder Application-Server vor dem Speichern in der Datenbank angestossen werden. Alternativ dazu kann die Verschlüsselung direkt vom Datenbank Server aus durchgeführt werden. Dies hat den Vorteil, dass keine Änderung der Anwendungen notwendig ist, um eine PCI-konforme Verschlüsselung zu implementieren.

Für eine komplette technologische Umsetzung der PCI Richtlinien bietet DataSecure eine hocheffiziente Lösung, die genannten Verschlüsselungs- und Key-Management Anforderungen mit einem geringen Implementierungs-Aufwand auf bereits bestehenden Systemen zu erfüllen. Da die verwendeten Schlüssel besonders geschützt werden und die Appliance nicht verlassen, ist eine komplexe verteilte Key-Management Infrastruktur nicht notwendig. Ebenfalls ist die Bereitstellung von Hardware Security Modulen (HSMs) zum sicheren Schutz der Schlüssel nicht erforderlich.



Abb. 2: DataSecure i311 Plattform

Für eine schnelle Integration bietet die DataSecure Plattform ein leicht bedienbares Interface zur Schlüsselverwaltung, Datenbank-Feldverschlüsselung, Schlüsselaustausch (Key Rotation) und Benutzerverwaltung. Gesichert durch mehrstufige Authentifizierung, SSL und Auditing wird ein Missbrauch verhindert

Durch Load Balancing und automatische Failover Funktionalität ist ein skalierbarer und ausfallsicherer Betrieb gesichert. Eine einzige DataSecure Appliance führt bis zur 45.000 Ver- oder Entschlüsselungsoperationen pro Sekunde durch. Durch Einbinden mehrerer Appliances in einen Cluster wird der Durchsatz noch erhöht. Somit unterstützt die DataSecure Plattform ebenfalls mehrere Anwendungen mit unterschiedlichen Anforderungen problemlos.

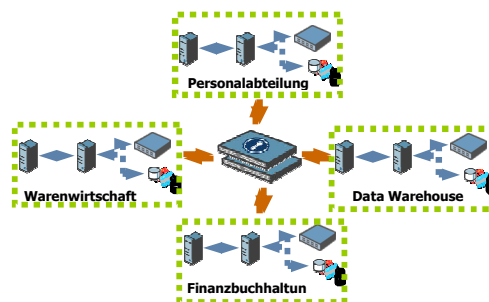


Abb. 3: Unterstützung unterschiedlicher Verschlüsselungsanforderungen

Die flexible Architektur erlaubt eine schlanke und effektive Implementierung im Vergleich zu anderen Lösungen. So bietet z.B. Storage Level Encryption (Dateisystemverschlüsselung) lediglich Schutz bei Diebstahl von Festplatten und Sicherungsbändern. Ebenfalls leiden softwarebasierte Lösungen unter Performanz-Problemen; zudem hängt die Sicherheit und Stabilität des Systems von dem darunterliegenden Betriebssystem ab.

Somit ist DataSecure die ideale Lösung, um den Verschlüsselungs- und Schlüsselverwaltungsanforderungen sicherheitsbewusster Unternehmen gerecht zu werden. Umfangreiche Änderungen an bestehenden Soft- und Hardwaresystemen sind nicht notwendig. Zudem garantiert die flexible Architektur, intuitive Administration und geprüfte Sicherheit eine standardskonforme und kosteneffektive Implementierung.

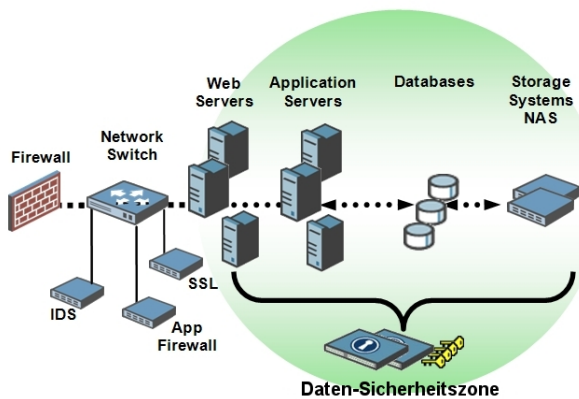


Abb. 1: DataSecure Zone