

SICHERHEIT FÜR SENSIBLE DATENBANKINHALTE

VON KARL FRIEDRICH KÄMPFNER | sandra.gerbich@informationweek.de

Kreditkartendaten müssen umfassend vor Missbrauch geschützt werden. Die Hamburger Albis Zahlungsdienste implementierten daher ein Verschlüsselungssystem, das die Daten ihrer Kreditkartenkunden nahezu unausspähbar macht.



Foto: Albis

Die Albis Zahlungsdienste sind sicherheitstechnisch gut gerüstet.

Zu Beginn dieses Jahres wurde von führenden Kreditunternehmen wie Visa und Mastercard der Payment Card Industry Data Security Standard, kurz PCI, entwickelt. Dieses Regelwerk für den Zahlungsverkehr wird von allen wichtigen Kreditkartenorganisationen unterstützt und muss von Unternehmen, die Kreditkartentransaktionen abwickeln, eingehalten werden.

Die Hamburger Albis Zahlungsdienste, Anbieter von Lösungen für Internet-gestützte Bezahlvorgänge,

Kredit- und Leasingverträge, suchte im Rahmen der laufenden PCI-Zertifizierung nach einem Verschlüsselungssystem, das ein Maximum an Sicherheit und die Zentralisierung aller kryptographischen Prozesse garantiert. Mit der DataSecure-Appliance von Ingrian Networks wurde eine Lösung gefunden, die nicht nur dem PCI-Standard gerecht wird, sondern auch für weitergehende eigene und kundenspezifische Anforderungen gerüstet ist.

Vor der Implementierung von DataSecure durch den deutschen Partner

Clearnote Solutions waren Kreditkartennummern bei Albis unter anderem dadurch geschützt, dass sie nur mit den ersten drei Ziffern angezeigt und ansonsten automatisch unkenntlich gemacht wurden, also »ausge-X-t« erschien – im Normalfall eine ausreichende Lösung, aber keine echte Verschlüsselung. »Visa und Master Card sind in ihren Beiträgen zur Entwicklung der Industriestandards von Extremfällen ausgegangen«, erläutert Michael Hülsiggensen, Geschäftsführer der Albis Zahlungsdienste. »Selbst wenn jemand ins Rechenzentrum einbrechen und die Rechner hinaustragen würde, dürfte er nicht an die Kreditkartendaten kommen. Das bedeutet, der Missbrauchsschutz muss gleichermaßen nach innen wie nach außen gewährleistet sein.« Weitere Forderungen der PCI sind beispielsweise die getrennte Speicherung der Schlüssel sowie deren regelmäßiger Austausch.

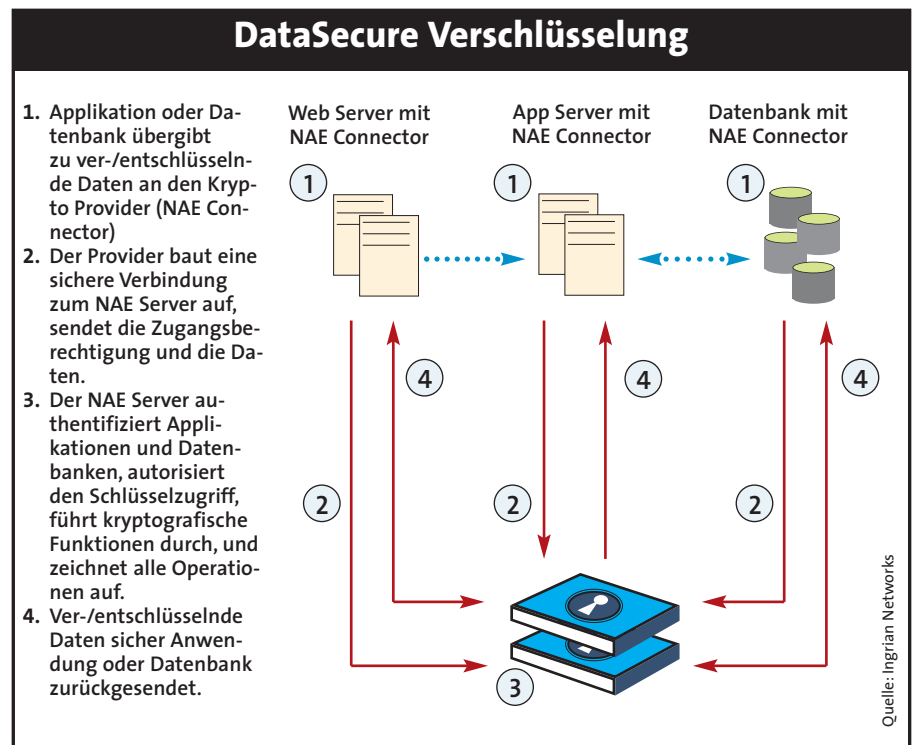
SCHUTZ VOR INTERNEN WIE EXTERNEN BEDROHUNGEN

Bei der Suche nach einer durchgängigen Kryptographie-Lösung war zunächst eine Eigenentwicklung in der Diskussion, aber sehr schnell wurde klar, dass die DataSecure-Appliance die Anforderungen mit weit geringerem internen Aufwand optimal bedienen könnte. Das Produkt besteht aus drei Komponenten: dem DataSecure-Rechner, einem dedizierten Hardware-System, dem Network Attached Encryption Server (NAE), der auf der DataSecure-Hardware läuft, und dem NAE

Connector, einer Software, die auf dem Web-, Applikations- oder Datenbank-Server installiert ist. Das System bietet eine auf Applikations Ebene angesiedelte Verschlüsselung, die sensible Daten nicht nur gegen externe, sondern ebenso gegen interne Bedrohungen schützt. Als applikationsbezogene Lösung verschlüsselt DataSecure nicht das gesamte File-System oder ganze Speichereinheiten, sondern nur die ausgewählten Anwendungsdaten. Durch diese Fokussierung können gerade interne Missbrauchsattacken erfolgreich verhindert werden.

»Die DataSecure-Appliance unterstützt umfassend die Anforderungen an die Datenverschlüsselung und das Key Management nach dem PCI Data Security Standard«, sagt Ralph Wörn, Leiter PCI Audit Services von Excelsis, die das PCI-Assessment bei der Albis Zahlungsdienste durchgeführt hat.

Bei Albis sind eine i311 und eine i321 DataSecure-Appliance im Einsatz, beides Server mit 2,8-GHz-Intel-Xeon-Prozessor und integrierter ASIC-Architektur. Die i321 verfügt zusätzlich über eine zweite CPU, RAID-1-Mirroring, redundante Netzteile und Lüfter sowie Gigabit-Ethernet-Schnittstellen. Eine DataSecure-Appliance arbeitet bis zu 45 000 kryptografische Operationen pro



Sekunde ab, bei weniger als 0,3 ms Latenzzeit.

Albis arbeitet mit einer 4D-Datenbank (4th Dimension) und Applikationen, die in der 4D-Entwicklungsumgebung erstellt wurden: ClickPay, ein modulares Zahlungssystem mit Prüfschlei-

fen und Riskmanagement, ClickLoan, ein Modul für den Raten- und Finanzkauf, ClickCards, ein Zahlungssystem für das elektronische Lastschriftverfahren und das Kreditkarten-Clearing, ClickCollect für das Forderungsmanagement, das Leasing-Modul ClickLea- →



Foto: Ingrian Networks

Eine DataSecure-Appliance arbeitet bis zu 45 000 kryptografische Operationen pro Sekunde ab.

se, das Risk-Management-System Click-Safe und ClickWire für Online-Überweisungen im E-Commerce. Der NAE Connector wurde auf dem 4D-Datenbank-Server installiert, und der NAE-Server verschlüsselt über diese Verbindung jedes einzelne Datenbankfeld mit personalisierten Daten von der Kartennummer bis hin zu den Adresdaten. Auf diese Weise ist die Verschlüsselung in den Workflow integriert. Eine Aufhebung der Entschlüsselung für Händler, die ihre Kreditkartentransaktionen über Albis abwickeln, erfolgt nur im Falle eines berechtigten Interesses, etwa wenn ein Kunde eine Gutschrift erhalten soll. Da der Händler die Kundendaten nicht speichern darf, bekommt er sie in einem solchen Fall von Albis.

Ein wesentlicher Bestandteil der Sicherheitslösung ist die Verwaltung der Schlüssel. Die gesamte Administration von Schlüsseln, Benutzern, Berechtigun-

gen wird innerhalb der geschlossenen Umgebung von DataSecure vorgenommen. Zu keinem Zeitpunkt müssen Schlüssel auf Servern oder Clients vorgehalten werden, was einem unberechtigten Zugriff wirkungsvoll vorbeugt. Ein sehr wichtiges Argument bei der Entscheidung für die Lösung war für Albis, dass DataSecure die Möglichkeit einer so genannten automatisierten Key-Rotation bietet; dies ist eine PCI-Anforderung und wird bei Albis im neunmonatigen Turnus durchgeführt.

ZUKUNFTSSICHERE LÖSUNG

»Die Anwendung der Lösung wird sich nicht auf die Kreditkartenverschlüsselung beschränken«, erläutert Gerald Schildger, Leiter Support bei Clearnote Solutions. »Da Albis sechs Auskunftsteilen, darunter Schufa und Bürgel, als Service Provider dient, gibt es neben den PCI-Anforderungen weitere strenge hausinterne Datenschutzbestimmungen, die eingehalten werden müssen. Die Kunden bekommen mit der Implementierung von DataSecure die Möglichkeit, über Remote-Zugriff eigene Daten zu verschlüsseln und benötigen somit keine eigene Lösung. Es hat sich gezeigt, dass sich mit diesem System problemlos kundenspezifische Kryptographie-Routinen einrichten lassen.«

Die Integration von DataSecure gestaltete sich erstaunlich unproblematisch. Die Installation der Server im Netzwerk dauerte weniger als eine Stunde, und die Anpassung der Applikationen kostete höchstens ein bis zwei Mannwochen Arbeitsaufwand. Die jet-

zige Konfiguration ist dabei so leistungsfähig, dass sämtliche nach Abschluss des PCI-Audits geplanten Kryptographie-Einsatzfelder, wie zum Beispiel das erwähnte Verwalten von Wirtschaftsinformationen für Auskunftsteilen, ohne Erweiterungen der Hardwareplattform integriert werden können.

Michael Hülsiggensen sagt: »DataSecure hat unser erstes Projekt, die Zertifizierung gemäß der PCI-Sicherheitsanforderungen durch VISA und Mastercard, auch dank der reibungslosen Implementierung problemlos unterstützt. In Zukunft kommt DataSecure für unsere unternehmensweiten Anwendungen zum Einsatz. Das gibt unseren Kunden ein sehr hohes Maß an Sicherheit für ihre Daten.«

Durch gezielte Verschlüsselung von Datenbankinhalten auf Feldebene und die Trennung der Verschlüsselung von der Anwendung können parallel verschiedene kunden- beziehungsweise workflowspezifische Anforderungen bedient werden. Die problemlose Integration von Anwendungen und Datenbanken macht die Lösung modular. An eine zentrale Schlüssel- und Sicherheitsadministration können beliebige Anwendungen auf unterschiedlichsten Plattformen angeschlossen werden.

»Auch wenn die PCI-Anforderungen der Anlass für die Anschaffung des Systems waren, wird die Anwendung weit darüber hinausgehen. Ich sehe PCI in einer Vorreiterrolle für den Datenschutz. Da der so genannte Identitätsklau eine große Bedrohung der Internetswirtschaft darstellt, wird es mit Sicherheit weitere Datenschutz-Anforderungen geben, für die wir uns aber mit unserer zentralen Kryptografie-lösung gut gerüstet fühlen«, sagt Michael Hülsiggensen. »Sicher ist die Einführung eines solchen Systems ein großer Schritt. Und das dafür notwendige Budget zu erstreiten, ist für die IT-Verantwortlichen wohl schwieriger als die Implementierung selbst, aber ich kann Unternehmen und Organisationen mit ähnlichen Sicherheitsanforderungen nur empfehlen, die Einführung zu evaluieren.«

* **KARL FRIEDRICH KÄMPFNER** ist Geschäftsführer der Clearnote Solutions GmbH

Anzeige

TECHNOLOGY TOUR 2006
KONGRESS UND AUSSTELLUNG

**network
Computing**
technology
tour

21.11.06 Leipzig
22.11.06 Frankfurt
23.11.06 Stuttgart

Anmeldung unter
www.networkcomputing.de/technology-tour