



SUCCESS STORY

Deutsche Lufthansa AG

Komplettlösung für das Management von PKI-Zertifikaten

Die Lösung im Überblick

Branche
Luftfahrt

Herausforderung

Bereitstellung einer umfassenden Lösung zur Administration von Server-Zertifikaten für den Aufbau sicherer Internet-Portale; einfache und kosten-günstige Beschaffung und Verwaltung von SSL-Zertifikaten

Lösung

VeriSign® Managed PKI für SSL (MPKI für SSL) bietet der Lufthansa eine schnelle, effiziente und kostengünstige Methode zur Bestellung und Inbetriebnahme von SSL-Server-Zertifikaten

Resultate

- Zeitaufwand für die SSL-Zertifizierung und -Installation von fünf Arbeitstagen auf weniger als eine Stunde reduziert

Mit Internet-Portalen wie Lufthansa.com und miles-and-more.com nutzt die Deutsche Lufthansa AG neue Medien zur umfassenden Betreuung ihrer Kunden. Beide Portale sind für die Lufthansa besonders wichtig — als Teil der Vertriebsstrategie ebenso wie als Werkzeug für die Kundenbindung und das Kundenmanagement.

Mehr als acht Millionen Zugriffe werden auf den Seiten der Lufthansa Internet-Portale täglich verzeichnet: Informationen aus dem Flugplan, der Kontostand bei Miles and More und natürlich Online-Buchungen sind darunter die am häufigsten genutzten Service-Angebote. Vor allem sind über die Internet-Portale besonders günstige Flüge und attraktive Web-Services zu finden — Leistungen, die die Beziehung zum Kunden weiter intensivieren.

Die Deutsche Lufthansa AG — eines der bedeutendsten Unternehmen in Deutschland und weltweit renommierte Luftfahrtgesellschaft, hat sich vor allem durch Pünktlichkeit, Zuverlässigkeit und Sicherheit einen Namen gemacht.

Qualität und Sicherheit sind bei der Lufthansa oberstes Gebot. Das gilt vor allem für die Flugzeuge, aber ebenso für die Online-Präsenz des Unternehmens. Nicht zuletzt, weil sensible, personenbezogene Daten genutzt werden, die gesondert zu schützen sind. Verantwortlich für die Sicherheitsmaßnahmen und für den reibungslosen Betrieb der Portale ist das E-Commerce and Direct Sales Department (IE/E) in Frankfurt am Main.

Die Herausforderung bei dieser anspruchsvollen Aufgabe besteht nicht allein in der Administration der hohen Anzahl von Zugriffen und in der Beherrschung der aus zahllosen Servern bestehenden, komplexen IT-Landschaft. Ein wesentlicher Punkt ist vor allem auch, dass die Web-Seiten so prominenter Unternehmen wie der Lufthansa Hacker regelrecht anziehen und attraktive Ziele für mutwillige Störungen und



Where it all comes together.™

- Sicherheit durch Eliminierung von einander überschneidenden oder verfallenen Zertifikaten
- Kostensenkung pro SSL-Zertifikat um 20 bis 25 Prozent gesenkt
- Effiziente Administration der Zertifikate über die gesamte Gültigkeitsdauer, beispielsweise durch übersichtliche Reports, die mit wenigen Mausklicks generiert werden können

kriminelle Angriffe darstellen. Sicherheit ist deshalb ein unumgängliches Gebot für Harald Mansmann, den Web Master der Deutschen Lufthansa AG.

+ Sicherheit ist aufwändig

Seit dem Start der Internet-Portale 1996 wurde SSL (Secure Socket Layer) als Verschlüsselungsverfahren für den gesamten webbasierten Datenaustausch verwendet. Mit SSL wurden die Server-seitigen Applikationen ebenso wie sensible Kundendaten, z.B. die Kreditkarteninformationen, geschützt. Diese hohen Sicherheitsvorkehrungen erforderten einen entsprechend hohen administrativen Aufwand.

Die wichtigste Frage dabei ist, wie man SSL-Zertifikate für mehrere Server an unterschiedlichen Standorten möglichst effizient managen kann. Oft werden noch kostentreibende, eigenständige Zertifizierungsstellen eingerichtet und betrieben. Auch die Lufthansa musste zunächst die zur Absicherung der Portale benötigten SSL-Server-Zertifikate bei verschiedenen öffentlichen Zertifizierungsstellen einholen. Das wiederum setzte eine manuelle Pflege der Zertifikate voraus, beispielsweise über Listen für den Gültigkeitszeitraum der Zertifikate. Die Zertifikate mussten also einzeln beantragt und installiert werden — und lösten so jeweils einen eigenen Vorgang in Einkauf und Rechnungswesen aus. Weder ein schneller Überblick über die eingesetzten Zertifikate noch eine durchgängige Kostenkontrolle waren auf manuelle Weise möglich.

„Wir hatten zwar eine Lösung, die dem hohen Sicherheitsbedarf der Lufthansa entsprach, aber wir hatten nicht die vollständige und notwendige Kontrolle“, erläutert Harald Mansmann, Web Master der Deutschen Lufthansa AG. Schon der Bestellprozess war vielschichtig und schwer zu steuern. Mitunter dauerte es mehr als fünf Tage, bis ein neues Zertifikat eingesetzt werden konnte.

Dadurch zeigten sich schnell echte Engpässe im bislang gültigen Konzept für den Erwerb und die Inbetriebnahme von Server-Zertifikaten. Es entstanden sogar Situationen, die ein konsequentes, fachmännisches Durchgreifen der Lufthansa IT-Spezialisten erforderten, damit sie nicht eskalieren. Mit dem Ziel, die Ressourcen dieser wichtigen Fachleute wirkungsvoller zu nutzen, suchte die Lufthansa daher eine einfachere Lösung zur Verwaltung der Sicherheits-Zertifikate.

+ VeriSign® MPKI für SSL:

Zertifikate kostengünstig und effizient verwalten

Die Entscheidung fiel auf die Managed Public Key Infrastructure für SSL (MPKI für SSL) von VeriSign. Diese Unternehmenslösung für den Erwerb, die Inbetriebnahme, die Administration und die Abrechnung von SSL-Zertifikaten beschleunigt und vereinfacht die Absicherung von Web-Servern ganz erheblich. Durch die reibungslose Umstellung auf diese Lösung kann die Lufthansa inzwischen über einen viel einfacheren, flexibleren Bestellprozess schnell und bequem so viele Zertifikate wie erforderlich bestellen. Der Aufwand ist dadurch gegenüber der Einzelbestellung und -verwaltung von SSL-Zertifikaten drastisch gesunken. Die Zertifikate sind in wenigen Minuten installiert, wodurch der Bestell- und Installationsvorgang, der einmal fünf Tage in Anspruch nahm, auf weniger als eine Stunde verringert werden konnte.

VeriSign MPKI für SSL liefert dem Sicherheitsverantwortlichen darüber hinaus detaillierte Reports über alle im Einsatz befindlichen Zertifikate. Dafür genügen wenige Mausklicks und es ist keine zusätzliche Software erforderlich, denn die VeriSign-Lösung wird über eine SSL-gesicherte Webapplikation bedient.

„Wir hatten eine schwierig zu behandelnde Situation, die wir mit Hilfe von VeriSign beheben konnten. Schnell und unproblematisch mit einem zentralisierten Ansatz ist MPKI für SSL genau das, wonach wir gesucht haben. Und VeriSign hat uns in allen Belangen umfassend unterstützt.“

Harald Mansmann
Web Master
Deutsche Lufthansa AG

Ein weiteres wichtiges Entscheidungskriterium für MPKI für SSL war die Tatsache, dass VeriSign der einzige Anbieter ist, der für seine Zertifikate eine Absicherung gegen finanzielle Schäden offeriert und deren Zertifizierungsprozess darüber hinaus einmal im Jahr durch die renommierten Wirtschaftsprüfer von KPMG geprüft wird.

„Wir suchten nicht nur einfach einen Anbieter, der nur die von uns bestellten Produkte liefert“, erläutert Volker Machulski, Senior Manager Operations eCommerce und Online Sales, Deutsche Lufthansa AG, „sondern wir suchten einen Partner, dessen Know-how und dessen Expertise uns dabei hilft, die beste Sicherheits-Infrastruktur aufzusetzen und der uns in allen Belangen umfassend unterstützt. VeriSign hat sich durch Kompetenz und Professionalität als zuverlässiger Partner qualifiziert.“

MPKI für SSL von VeriSign hat die Erwartungen der Lufthansa damit mehr als erfüllt — nicht nur unter den Aspekten Sicherheit und Administrierbarkeit, sondern vor allem auch unter dem Kostenaspekt. Harald Mansmann schätzt, dass die Anschaffungs- und Verwaltungskosten pro Server-Zertifikat um 20 bis 25 Prozent reduziert werden konnten. Darüber hinaus wurde das gesamte Sicherheitskonzept der Lufthansa nachhaltig verbessert, da unsichere Systemzustände durch verfallene Zertifikate ausgeschlossen sind. „Unsere Kunden können deshalb ihre persönlichen Informationen vertrauensvoll übertragen, denn sie sind umfassend gegen unberechtigte Zugriffe geschützt“, ergänzt Mansmann.

Bitte besuchen Sie uns unter www.verisign.de.