

be informed



Liebe Leserin, lieber Leser,
herzlich willkommen zur aktuellen Ausgabe
unseres Newsletters **be informed**.

Als Sicherheitsspezialisten können wir zwar nicht verhindern, dass Sie Ziel von Angriffen durch Datenräuber im Netz werden, aber wir können die Sicherheit Ihres Netzwerkes und Ihrer Anwendung im Hinblick auf Angriffe untersuchen und Ihnen wertvolle Hinweise zur Abwehr von Angriffen aufzeigen. Ein mächtiges Verteidigungswerkzeug ist die Datenverschlüsselung. Richtig eingesetzt stehen die Chancen mehr als gut, mit einer guten Verschlüsselung einen Angriff auf Ihre Daten unbeschadet zu überstehen. Daher beschäftigen wir uns in unserer heutigen Ausgabe des Acertigo Newsletters schwerpunktmäßig mit diesem Thema. Interessante Neuigkeiten gibt es auch in unserer Rubrik News Ticker. Schauen Sie einmal hinein, es hat sich Einiges in den letzten Wochen getan.

Wir wünschen Ihnen viel Spaß beim Lesen!

Herzliche Grüße



Ralph Wörn - Vorstand

Vereinbaren Sie einen Termin und treffen Sie uns auf den folgenden Events:

- Deutscher Versandhandelskongress & Fachmesse Mail Order World
29./30.09. 2010, Wiesbaden
- PCI Europe
12.10.2010 Frankfurt/Main
- EHI Technologie-Tage 2010
03./04.11.2010, Köln

Datenverschlüsselung muss mehr als ein ‚notwendiges Übel‘ sein

Christian Matt



Grundsätzlich sollte sich jeder Administrator mit dem Thema Verschlüsselung befassen, die Grundbegriffe und Standardverfahren verstehen und bei vertraulichen und geschäftskritischen Daten einsetzen. Für die PCI DSS-Konformität muss die Verschlüsselung zudem Mindeststandards erfüllen, über die unser Fachartikel informiert.

Grundsätzlich ist zwischen der Verschlüsselung von Kommunikation im Netzwerk und der Verschlüsselung von Daten selbst auf den Festplatten zu unterscheiden, zwei Verschlüsselungsarten, die sich in ihrer Funktionsweise ergänzen.

Warum man das Eine tun, das Andere aber nicht lassen sollte, ist leicht zu erklären: Datensicherheit besteht aus vielen Schichten und wird daher zu Recht im Aufbau oft wie eine Zwiebel mit ihren verschiedenen Häuten dargestellt. Der illegale Weg zu schützenswerten Daten führt nach dem

Durchdringen der äußeren Schutzschichten der Netzwerke im Inneren der Systeme entweder über die verwendete Applikation oder durch einen direkten Zugriff auf die Datenträger, welche die gespeicherten Daten enthalten. Daher ist es sinnvoll und wichtig, sowohl eine Zwei-Wege-Authentifizierung für die Applikation als auch eine Datenverschlüsselung auf dem Datenträger einzusetzen. Letztere gibt zudem die erforderliche Sicherheit bei physischem Diebstahl des Datenträgers samt Inhalt.

Auf einen Blick:

Grundlagen für PCI DSS konforme Verschlüsselung von Daten auf Datenträgern:

- Einsatz einer starken Kryptographie-Lösung für das Speichern von sensiblen Daten, z.B. AES mit 128 bit Schlüssellänge, 3DES mit mindestens 112 bit Schlüssellänge, oder asymmetrische RSA Schlüssel mit einer Länge von jeweils 1024 bit.
- Einsatz von entweder Feld-, Tabellenverschlüsselung oder Festplattenverschlüsselung.
- Aufbewahrung der Schlüssel getrennt vom Betriebssystem.
- Sichere Aufbewahrung der Schlüssel mit eigenem Schutzmechanismus.
- Beschränkung des Zugriffs auf die Schlüssel auf die notwendigen Personen.
- Schlüsselverwaltung auf mehrere Personen aufteilen, so dass Schlüssel nur von mehreren Personen rekonstruiert werden können.
- Verantwortliche Personen müssen um die Wichtigkeit ihrer Tätigkeit wissen.
- Erstellung von sicheren Schlüsseln muss gewährleistet sein.
- Vergabe von Schlüsseln auf sicherem Wege muss gewährleistet sein.
- Prozedur zur periodischen Änderung der Schlüssel muss definiert und in Anwendung sein (mind. jährlich).
- Auslagerung, Aufbewahrung, Widerruf und/oder Vernichtung von alten Schlüsseln auf sicherem Wege.
- Prozeduren zum Austausch von kompromittierten oder als kompromittiert verdächtigten Schlüsseln müssen vorhanden sein.
- Prozeduren zum Verhindern der Ausgabe oder Erstellung von Ersatzschlüsseln müssen vorhanden sein.

Es kann also nicht verwundern, dass PCI DSS den Einsatz beider Systeme in mehreren Anforderungen zwingend vorschreibt. Damit wird ein Sicherheitslevel für die Verarbeitung von Kreditkartendaten vorgeschrieben, der den Betreibern von Zahlungssystemen und deren Kunden eine sinnvolle und vertrauenswürdige Sicherheit sensibler Daten in betroffenen Netzwerksegmenten ermöglicht.

Unter den verschiedenen Arten für Verschlüsselung gibt es natürlich einen Standard, wobei die Verschlüsselung selbst noch keinen Standard darstellt. Die Anbieterlandschaft und die von ihr angebotenen Systeme sind vielfältig. Im Sinne des PCI DSS gilt es jedoch einiges zu beachten, denn nicht alle Systeme erfüllen die strengen Vorgaben. So steht beispielsweise das integrierte Microsoft-System EFS/NTFS im Konflikt zu Anforderung 3.4.1, denn der Schlüssel wird im Benutzerkonto gespeichert. Hingegen kann Software (wie zum Beispiel Windows 7 BITLOCKER, PGP oder SafeGuard Enterprise) in Hinblick auf oben genannte Anforderung in Frage kommen, da die Aufbewahrung des Schlüssels getrennt vom Benutzerkonto erfolgt. Insgesamt gilt es natürlich, alle Kriterien der für PCI DSS konformen Verschlüsselung von Daten auf Datenträgern zu erfüllen, so dass bei der Auswahl nicht eine Anforderung isoliert betrachtet werden kann.

Ganz Allgemein gilt, dass die Verschlüsselung mit den unterschiedlichsten Technologien umgesetzt werden kann. Dies kann durch softwaretechnische Maßnahmen erfolgen, bei dem eine Encryption-Library in die eigene Applikation integriert wird, oder durch den Einsatz von HSM-Cryptokarten die

über eine API in die jeweilige Applikation mit eingebunden werden. Eine weitere Möglichkeit besteht durch die bei vielen Datenbank-Managementsystemen verfügbare Verschlüsselungsoptionen. Auch der Einsatz sogenannter Crypto-Appliances als separate Hardware-Komponenten bietet sich an. Sie ermöglichen eine transparente Verschlüsselung, so dass weder die Applikation noch die Datenbanken angepasst werden müssen.

Unabhängig von den Anforderungen und Einsatzgebieten spielen bei der Entscheidungsfindung für die richtige Lösung, d.h. das zum eigenen Unternehmen passende Verschlüsselungssystem die Punkte Wartbarkeit, Geschwindigkeit, Sicherheit und Bedienungskomfort in der Regel die größte Rolle. Da durch die Verschlüsselung das System gezwungen ist, praktisch bei jedem Datenzugriff zunächst die Entschlüsselung durchzuführen, sind Bedenken über die Beeinträchtigung der Performance, also der Geschwindigkeit, durchaus verständlich. Einbußen sind allerdings erst dann objektiv spürbar, wenn ein Zugriff auf größere Dateien und damit große Datenmengen erfolgt. Die Bedenken einiger Administratoren und IT-Verantwortlicher ist daher oftmals unbegründet, die Performance-Nachteile sind eher subjektiv. In jedem Fall ist es jedoch ratsam, vor der Entscheidung für ein bestimmtes Produkt entsprechende Tests durchzuführen und die tatsächliche, d.h. die messbare Beeinträchtigung zu bestimmen. Ein Plus an Sicherheit muss nicht automatisch mit einem Minus an Performance und Bedienkomfort einhergehen.

Über den Auditor

Christian Matt ist als Auditor für PCI DSS und PA DSS bei der Acertigo AG tätig. Der diplomierte Informatiker arbeitete als Business Consultant bei der EXCELSIS Business Solutions AG, bevor er bei der Acertigo AG seine Auditorentätigkeit begann. Christian Matt arbeitet im PCI DSS Umfeld seit 2009.



Aus der Praxis:

Michael Hülsiggensen, EOS Payment Solutions

Herr Hülsiggensen, nach welchen Kriterien haben Sie seinerzeit das von Ihnen verwendete Verschlüsselungssystem von Ingrian ausgesucht?

Maßgeblich für uns waren drei Aspekte: Zunächst und an erster Stelle steht ein Maximum an Sicherheit für unsere Daten, d.h. ein Missbrauchsschutz, der nach innen wie nach außen gewährleistet ist.

Darüber hinaus haben wir nach einem System gesucht, das die Zentralisierung aller kryptographischer Prozesse garantiert. Und nicht zuletzt musste das System die Anforderungen des PCI DSS unterstützen und uns ermöglichen, diese vollumfänglich zu erfüllen. Diese Voraussetzungen hat die DataSecure-Appliance von Ingrian erfüllt.

Welche Erfahrungen haben Sie mit DataSecure in den letzten vier Jahren gemacht?

Wir haben ausgesprochen positive Erfahrungen gemacht. Das System ist hoch performant und extrem flexibel nutzbar. Es entspricht genau unseren Erwartungen.

Sie haben die PCI-Anforderungen als Anlass für die Anschaffung des Systems genannt. Haben sich weitere Datenschutz-Anforderungen ergeben, die DataSecure ebenfalls abdeckt?

Da EOS acht Auskunfteien, darunter Bürgel und Schufa, als Service Provider dient, gibt es neben den PCI Anforderungen weitere strenge hausinterne Datenschutzbestimmungen, die eingehalten werden müssen. Unsere 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 kundenspezifische Kryptographie-Routinen einrichten lassen.

Was raten Sie Unternehmen, die sich aktuell mit der Frage der Einführung eines Verschlüsselungssystems beschäftigen?

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.

Herr Hülsiggensen, vielen Dank für das Gespräch!
Die Fragen stellte Christina Wolf.

Über den Interviewpartner

Michael Hülsiggensen ist Geschäftsführer der EOS Payment Solutions GmbH. Nach seinem Studium der Rechtswissenschaften begann Michael Hülsiggensen seine berufliche Laufbahn im Jahr 1990 als Bereichsleiter Logistik, allgemeine Verwaltung EDV bei der TMI Top Music International Vertriebs GmbH. 1994 wechselte er als stellvertretender EDV-Leiter zur Ernst Brinkmann KG. Nachdem er dort von 1996-2001 eine Geschäftsführertätigkeit im Versandhandel ausübte, wechselte er im Jahr 2001 in die Geschäftsführung der Albis Zahlungsdienste GmbH & Co. AG. Im Zuge der Übernahme (2007) des Unternehmens durch die EOS Gruppe (www.eos-solutions.com) firmierte das Unternehmen in EOS Payment Solutions um.



EOS Payment Solutions GmbH

EOS Payment Solutions GmbH bietet seinen derzeit 2500 Kunden aus dem Bereich Handel seit 2007 Lösungen für den elektronischen Zahlungsverkehr und die elektronische Risikooptimierung. Bereits seit 1999 ist das Unternehmen als Albis Zahlungsdienste GmbH am Markt aktiv. EOS Payment verarbeitet die Zahlarten Kredit- und Debitkarten weltweit, elektronischen Lastschriftinzug, giro pay, iDEAL (Niederlande) sowie eps Online-Überweisungen (Österreich), bietet besicherte Zahlungen und übernimmt Risikoprüfungen. Das Unternehmen erfüllt den Payment Card Industry Data Security Standard (PCI-DSS) von Visa und MasterCard.



Die Kompetenzen im Bereich der automatisierten Zahlungslösungen verbindet EOS Payment Solutions mit dem fundierten Know-how der Bereiche Forderungsmanagement, Marketing-Informationen und Risiko-Informationen der EOS Gruppe. Mehr unter www.eos-payment.com

Gastartikel

Unternehmensweites Daten-Sicherheits-Management

von Peter Schulz, Protegrity

Die Erreichung der Konformität mit dem „Payment Card Industry Data Security Standard“ (kurz „PCI DSS“) stellt für viele Unternehmen die Motivation dar, das Thema Daten-Sicherheits-Management im Gesamtkontext aufzugreifen. Im Fokus von PCI DSS steht der Schutz der Kreditkarteninformation.

Technisch betrachtet ist der Schutz der Kreditkarteninformation durch Anwendung eines Verschlüsselungsalgorithmus simpel. Herausforderungen sind jedoch das Key Management, die Gewährleistung einer stetigen Funktionssicherheit der Lösung und die durch die Implementierung entstehenden Zeitaufwände und Kosten.

PCI DSS fordert den Schutz der sensiblen Daten während des gesamten Lebenszyklus im Unternehmen – in allen betroffenen Systemen. Typisch ist hier der Fluss der Daten über unterschiedlichste Systeme – am Beispiel eines Händlers von der Kasse über den Filialserver, hin in das Rechenzentrum und dort in verschiedene Systeme, bis die Daten schließlich archiviert und geordnet vernichtet werden. Diese gesamte Kette unterschiedlichster Plattformen gilt es abzudecken. Zu berücksichtigen sind auch die Datenflüsse zwischen diesen Systemen.

Der Grundgedanke von PCI DSS ist der Schutz der Daten auch bei internen Zugriffen. Die Umsetzung dieser geschäftlichen Anforderung in den einzelnen Systemen bedeutet eine Abbildung dieser Regularien in die technische Implementierung der einzelnen Systeme. Auch typische „Super User“ wie Administratoren und Entwickler sind zu berücksichtigen.

Die Maximen der Trennung des Zugriffs nach geschäftlichem Informationsbedarf und der Einfachheit der Implementierung kann durch die Einführung eines zusätzlichen „Interpretations-Layers“ auf Datenbank und/oder Dateisystem Ebene erreicht werden. Die physischen Zugriffsberechtigungen bleiben unverändert – inklusive der „Super User“ Administratoren-Gruppe. Appli-

kationen sollen nicht geändert werden müssen. Ausschließlich die Interpretierbarkeit der sensiblen Daten wird gesteuert. Das Management der Lösung erfolgt zentral und unabhängig von den anderen IT Systemen, dennoch soll diese zentrale Instanz keinen „Single Point of Failure“ darstellen. Die Bedienung soll geschäftlich orientiert sein und kein technisches Wissen über die einzelnen angeschlossenen Systeme bedingen. Mitarbeiterinformationen sollen aus einem Unternehmens-Verzeichnis übernommen werden – insbesondere wichtig ist hier die Möglichkeit der zeitnahen Deaktivierung von Mitarbeiterkonten die das Unternehmen verlassen oder den Aufgabenbereich wechseln. Aktivitätsdaten sollen zu dieser zentralen Instanz im Normalbetrieb online übertragen werden. Reporting und Alarmierung sollen von diesem System gesteuert werden. Weiterhin sollen hier die kryptographischen Schlüssel erzeugt und verteilt werden – als Voraussetzung für eine Schlüssel-Rotation, insbesondere im Falle der Kompromittierung.

Die Lösung von Protegrity kann Daten auf den Ebenen Dateisystem, Datenbank und Applikation schützen – eine sehr große Anzahl unterschiedlicher Hersteller dieser Systeme wird unterstützt. Der Schutz der Daten während des gesamten Lebenszyklus im Unternehmen wird damit gewährleistet. Weiterhin wird das Management der Berechtigungen, der kryptographischen Schlüssel und das Reporting und Alarmierung zentral zur Verfügung gestellt. Vorgefertigte Standard-Reports erfüllen die Anforderungen des PCI DSS. Diese Lösung wird weltweit von mehr als 150 Großunternehmen zum Schutz sensibler Daten und Erfüllung von regulatorischen und gesetzlichen Anforderungen eingesetzt. Eine große Zahl der Kunden unterliegt ebenfalls den Anforderungen des PCI DSS. Die Lösung unterstützt hierbei die Erfüllung folgender Bereiche im PCI Standard:

Requirement 3: Schutz gespeicherter Karteninhaberdaten

Requirement 6: Entwicklung und Wartung sicherer Systeme und Anwendungen

Requirement 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach geschäftlichem Informationsbedarf

Requirement 10: Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten

Requirement 12: Befolgung einer IS-Richtlinie für Mitarbeiter und Subunternehmer

Die Protegrity Plattform ist unter dem Gesichtspunkt „Risk Adjusted Data Security“ aufgebaut. Dies bedeutet, mit der gleichen Plattform, dem gleichen zentralen Management und Reporting, für alle unterstützten Hersteller, gibt es eine Auswahl unterschiedlicher Schutzmechanismen. Für die Erreichung des PCI DSS Compliance sind hiervon nur „starke Kryptographie“ und „Tokenization“ interessant, aber mit dem gleichen System lassen sich später auch andere sensible

Daten, mit eventuell anderen Methoden, schützen. Einen Überblick über die unterschiedlichen Schutzmechanismen und deren Vergleich in Bezug auf Performance-Auswirkung, Speicherplatz-Auswirkung, Sicherheits-Level und Transparenz gegenüber den Applikationen zeigt nachfolgende Abbildung.

Schutz-Methode	Performance-Auswirkung	Speicherplatz-Auswirkung	Sicherheits-Level	Transparenz gegenüber Applikationen
Monitor in Clear (agent)	●	●	○	●
Monitor + Blocking + Masking	●	●	○	●
Format Controlling Encryption	●	●	○	●
Partial Encryption (Mask)	●	●	○	●
Strong Encryption	●	●	●	○
Tokens	○	●	●	○
Hash	●	○	●	○

höchste ● ○ niedrigste

Dieser kurze Artikel kann nur einen Überblick über die Schutz-Optionen und die Lösung selbst geben. Ausführliche Informationen erhalten Sie gerne von uns.

Über den Autor

Peter Schulz verantwortet bei Protegrity den Sales-Bereich DACH, Osteuropa und Afrika. Sein Büro ist im Frankfurter Raum angesiedelt. Er hat umfangreiche Erfahrung im Design und der Implementierung von Unternehmenslösungen und der Durchführung von PCI DSS Projekten.



Protegrity Corporation

5 High Ridge Park
Stamford, CT-06905, USA
+1 203 326 7200 main
+49 6173 977397 direct
+49 176 23945650 mobile
peter.schulz@protegrity.com
www.protegrity.com

Weitere Informationen: www.protegrity.com



News Ticker

Unser News Ticker in dieser Ausgabe gestaltet sich etwas umfangreicher als Üblich, da es einiges Neues aus den letzten Wochen zu berichten gibt. Wir sind der Überzeugung, dass auch für Sie Interessantes dabei ist.

+++ Erweiterung des Life Cycle von PCI DSS auf 3 Jahre erweitert +++

Wie das PCI Council (PCI SSC) vor Kurzem mitgeteilt hat, wird der Life Cycle für PCI DSS auf 3 Jahre erweitert. Hierdurch will das PCI Council eine für Händler und Service Provider verbesserte

Dokument Erweiterung Life Cycle: https://www.pcisecuritystandards.org/pdfs/pr_100622_lifecycle.pdf

Planungssicherheit ermöglichen, da die jeweils gültigen PCI-Anforderungen für 1 Jahr länger ihre Gültigkeit behalten. Sie finden die Mitteilung unter nachfolgendem Link:

+++ Angriffe auf Händler-Webseiten mit PSP-Anbindung +++

Visa Europe hat einen sogenannten „Security Alert“ veröffentlicht, welcher Angriffe auf Webseiten von Händlern beschreibt, die Kartendaten über eine PSP-Anbindung verarbeiten lassen (Hosted Payment Pages). Hierbei wird direkt das Händlersystem manipuliert oder angegriffen, indem der dort in der Regel vom Händler eingebauter „redirect“ auf die Seiten des PSP vom Angreifer manipuliert wird.

Da an die Webseiten des Händlers seitens PCI DSS keine verpflichtende Sicherheitsanforderungen bestehen, werden solche Manipulationsversuche häufig weder erkannt noch verhindert. Wie wir bereits in der Vergangenheit häufig in Gesprächen mit den Verantwortlichen und Marktteilnehmern darauf hingewiesen haben, ist diese Situation absehbar gewesen, da das Händlersystem das

Dokument Hosted Payment Pages: http://www2.visaeurope.com/documents/ais/hosted_payment_page_security_alert1.pdf

schwächste Glied in der Kette wird und damit ein ideales Angriffsziel für Hacker und Kriminelle darstellt. Wir empfehlen daher seit langem, dass sich der Betreiber von Web-Shops im Eigeninteresse die entsprechenden Sicherheitsmaßnahmen aus PCI zunutze machen und diese freiwillig anwendet. Hierzu gehört neben der Erkennung von Veränderungen der Webseitenprogrammierung oder des html-Codes auch eine regelmäßige Durchführung von Schwachstellen-Scans, um die Systeme und damit die Sicherheit zu verbessern. Diese einfachen Mittel erschweren dadurch den Angreifern die Manipulation und beugen dem Missbrauch vor. Interessierten Kunden helfen wir diesbezüglich gerne weiter. Den „Security Alert“ von Visa Europe finden Sie unter folgendem Link:

+++ Neue Version 1.2 des PCI DSS Program Guide +++

Das PCI Council hat eine neue Version des PCI DSS Program Guide vorgestellt. Der Program Guide legt die Richtlinien für die Durchführung von externen Schwachstellen-Scans für die PCI-relevanten IP-Adressen fest, wie sie ein Approved Scanning Vendor (ASV) wie die Acertigo einhalten muss. Der Program Guide ist damit auch für unsere Scan-Kunden (Händler und Service Provider) wichtig, da hierin unter anderem festgelegt ist, welche IP-Adressen unsere Kunden scannen

lassen müssen. Wesentliche Änderungen hat es bei der Aufbereitung der Scanberichte, sowie der Umstellung der bisherigen fünfstufigen Einteilung einer Schwachstelle auf eine dreistufige gegeben.

Wie gewohnt werden wir Ihnen hierzu in einem unserer folgenden Newsletter oder NewsFlashes einen ausführlichen Artikel zur Verfügung stellen, welcher aller Änderungen im Einzelnen beschreibt.

+++ Ratschläge zu Passwortsicherheit und SQL Injection von Visa Europe +++

Visa Europe hat auf seiner Webseite zwei Dokumente publiziert, welche Informationen und Ratschläge für den Umgang mit Benutzerkonten/Passwörtern und einer der oft vorkommenden

Dokument SQL Injection: http://www2.visaeurope.com/documents/ais/sql_factsheet.pdf

Dokument Passwortsicherheit: http://www2.visaeurope.com/documents/ais/ds_factsheet.pdf

Angriffsvarianten auf Web-Applikationen, der sogenannten SQL Injection beinhalten. Die beiden Dokumente können Sie über den nachfolgenden Link herunterladen.

+++ Zertifizierung von DLL's als Payment Applikationen +++

Wie das PCI Council in einem seiner letzten Klarstellungen festgelegt hat, ist eine Zertifizierung von nicht eigenständig lauffähigen Applikationen, wie z.B. DLL's (Dynamic Link Libraries) oder sonstigen Programmkomponenten im Rahmen einer PA-DSS Zertifizierung (Payment Applikation Zertifizierung) nicht möglich. Begründet wird dies damit, dass eine DLL nur ein Teil einer gesamten Paymentapplikation ist. Nachfolgend ein Auszug aus der Begründung:

"This decision is based on the fact that libraries are unable to be tested independently as they are not stand-alone,

functional applications, and the implementation of a particular library into a payment application could vary from one application developer to another. Additionally, functional evaluation of a DLL would only be possible if the library was evaluated as part of a payment application in which the DLL is called."

Ausdrücklich wird vom PCI Council darauf hingewiesen, dass diese Regelung nicht für eine Middleware oder deren Komponenten zutrifft, da diese unabhängig von einem User-Interface funktionieren und separat getestet werden können.

+++ Einstellung des Supports für Microsoft Windows 2000 und XP SP2 +++

Microsoft hat mitgeteilt das zum 13.07.2010 der Extended Support für Windows 2000 und XP SP2 ausläuft. Damit werden diese Versionen hinsichtlich PCI DSS als ein nicht einsetzbares Betriebssystem herabgestuft, da zukünftig unter anderem nicht mehr die Bedingungen für regelmäßige Sicherheitsupdates und -patches vorliegen. Händler und Service Provider sollten ihre Systeme dementsprechend mit neueren Versionen des Betriebssystems aufrüsten.

+++ Payment Application Mandates +++

Die Kartenorganisationen Visa und MasterCard haben Deadlines für die Verwendung von Payment Applikation durch Händler und Service Provider bekanntgegeben. Visa legt fest, dass Händler ab 31.12.2012 nur noch PA-DSS-zertifizierte Payment Applikationen eines Herstellers einsetzen. MasterCard legt dies ab dem 1.7.2012 sowohl für Händler als auch Service Provider fest.

Impressum

Acertigo AG
Wilhelmsplatz 8
70182 Stuttgart (Germany)
+49 (0)7 11/6 20 30-300
Sitz Stuttgart
HRB 724100, Amtsgericht Stuttgart
Umsatzsteuer-Identifikationsnummer
gemäß § 27 a Umsatzsteuergesetz:
DE 813211856

Vorstand

Ralph Wörn
Dr. Stephan Engelke

Redaktion und Kontakt:

Christina Wolf
christina.wolf@acertigo.com



Rechtliche Hinweise

Informationen im Newsletter werden nach sorgfältiger Überprüfung veröffentlicht. Trotzdem kann keine Gewähr für die Fehlerfreiheit und Genauigkeit der enthaltenen Informationen übernommen werden. Jegliche Haftung für Schäden, die direkt oder indirekt aus der Benutzung des Newsletters entstehen, wird ausgeschlossen. Im Falle von Verlinkungen zu Drittanbietern, übernimmt Acertigo keine Verantwortung für diese Webseiten. Acertigo übernimmt keinerlei Gewährleistung oder Garantie für Informationen, Software oder andere Produkte, die von diesen Webseiten heruntergeladen werden können.

Hinweise zum Copyright

Die Inhalte dieser Publikation sind urheberrechtlich geschützt. Ohne schriftliche Genehmigung der Acertigo AG dürfen sie in keiner Form verarbeitet oder vervielfältigt werden. Alle Rechte, auch die der Übersetzung, sind vorbehalten.