ERNW Newsletter 14 / Februar 2007

Liebe Partner, liebe Kollegen,

willkommen zur vierzehnten Ausgabe des ERNW-Newsletters mit dem Thema:

PCI_Compliance

Version 1.0 vom 09.03.2007

von:

Enno Rey (erey@ernw.de)

Abstract:
Der von Visa und MasterCard initiierte Payment Card Industry Data Security Standard (PCI DSS) beschreibt Massnahmen und Werkzeuge zur sicheren Verarbeitung von Kreditkarten-Daten. Online-Händler (aber etwa auch Entwickler von Software im Bankenbereich) sind - je nach Anzahl der jährlich abgewickelten Transaktionen - zum Nachweis ihrer "Compliance" zum PCI DSS verpflichtet und werden mittlerweile bei Verstössen sogar mit Bussgeldern belegt. Dieser Newsletter stellt den Standard und die Prüf-Methodik vor.

Der Terminus *Compliance* wird ja durchaus seit einiger Zeit schwer strapaziert; hier soll daher auf eine umfangreiche Diskussion und Klärung verzichtet werden. Als Arbeitsdefinition genügt es, gemäss ISO 17799:2005 § 15 von „Einhaltung gesetzlicher, satzungsmässiger, behördlicher oder vertraglicher Verpflichtungen“ auszugehen. „PCI Compliance“ bezeichnet mithin einfach die Einhaltung der Vorschriften des „PCI DSS“.

„PCI DSS“ steht für „Payment Card Industry Data Security Standard“ und stellt den aktuellen De-facto Standard zur IT-Sicherheit bei der Verarbeitung von Kreditkarten-Daten dar. Er basiert im wesentlichen auf den *Visa Account Information Security* (AIS) und *Mastercard Site Data Protection* (SDP) Programmen, wird aber auch von allen anderen grossen Karten-Unternehmen (*Amex*, *Diners*, *JCB*, *Discover*) angewandt. Der Standard trat (mit einer Ausnahme, s.u.) am 30. Juni 2005 in Kraft; die aktuelle Version ist (seit September 2006) 1.1. Circa einmal jährlich ist ein Update geplant.

Hintergrund des gemeinsamen Security-Standards der Kreditkarten-Unternehmen war, dass diese nach einer Reihe von Sicherheits-Vorfällen mit Kreditkarten-Daten und daraus resultierenden Kunden-Ängsten befürchten mussten, dass es (v.a. in den USA) zu einer staatlichen Regulierung des Umgangs mit diesen Daten kommen könnte. Einer solchen wollte man (übrigens erfolgreich) qua selbst-verabschiedeter Sicherheits-Spezifikation zuvorkommen, die sich mittlerweile in den davon betroffenen Organisationen überdies zu einem der wichtigsten *Driver* für IT-Security entwickelt hat.

Die Anforderungen des PCI DSS greifen, sobald „a Primary Account Number (PAN) is stored, processed, or transmitted“ (Preface des PCI DSS). Die PAN ist eine bestimmte Dateneinheit des Magnetstreifens einer Karte, die in ISO/IEC 7812-1 definiert ist und zur Vereinfachung im weiteren Artikel mit Kreditkartennummer gleichgesetzt wird. Der Magnetstreifen enthält daneben weitere Daten, u.a. etwa den Karteninhaber, das Gültigkeitsdatum und den *Card Verification Value* (CVV), der bei Telefon- oder Internet-basierten Transaktionen verwendet wird, um den Nachweis zu erbringen, dass der Initiator tatsächlich im physischen Besitz der referenzierten Karte ist.

Der Schutz just dieser Daten ist das zentrale Anliegen des PCI DSS. So dürfen nur bestimmte davon überhaupt gespeichert werden:

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

Die Richtlinien des PCI DSS gehen jedoch über blosse Speicherung weit hinaus und beziehen sich auf Implementierung und Betrieb des „cardholder data environment“, in der diese Daten verarbeitet werden. Dies schliesst alle *System Components* mit ein, wobei diese definiert werden als „any network component, server, or application that is included in or connected to the cardholder data environment“[1].

Kurz gesagt ist die gesamte Umgebung der (Karten-) datenverarbeitenden Systeme inklusive der Infrastrukturkomponenten im Fokus des PCI DSS. Dieser Fokus kann (und sollte) durch geeignete Netzwerk-Segmentierung eingegrenzt werden, was der Standard selbst auch anregt. Die betroffenen Organisationen wiederum (eben alle, bei denen in irgendeiner Form Kartennummern/PANs verarbeitet werden und sei es nur, dass diese auf einer Webseite eingegeben werden, der eigentliche Zahlvorgang aber mithilfe Dritter abgewickelt wird), sind in verschiedene Kategorien unterteilt, die sich an der Anzahl der jährlich durchgeführten Transaktionen orientieren[2]:

[1] Weiter wird spezifiziert:
„**Network components** include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. **Server types** include but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). **Applications** include all purchased and custom applications, including internal and external (Internet) applications.”

[2] Die Unterscheidung etwa von *Merchant* und *Service Provider* soll hier keine Rolle spielen.

Merchant Level	Kriterien	In Kraft	Nachweise		
			Jährliches On-Site Security Audit	Externer Scan, alle drei Monate	Jährlich *Self-Assessment Questionn.*
Level 1	Mehr als 6.000.000 prozessierte Transaktionen jährlich	30. September 2004	Erforderlich	Erforderlich	
Level 2	150.000 bis 6.000.000 Transaktionen jährlich	30. Juni 2005		Erforderlich	Erforderlich
Level 3	20.000 bis 150.000 Transaktionen jährlich	30. Juni 2005		Erforderlich	Erforderlich
Level 4	Alle anderen	-		Empfohlen	Empfohlen

Inhaltlich ist der Standard in folgende zwölf Abschnitte unterteilt:

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

In diesen sind die Richtlinien in (für einen Praktiker) wohltuend durchdachter, detaillierter und konsistenter Form dargestellt (insbesondere im Vergleich zu etwa *Sarbanes-Oxley*, dessen Interpretation doch – zuweilen wenig transparent – teilweise vom Ermessen der Wirtschaftsprüfer abhängt).

Ob und inwieweit eine Organisation *compliant* ist, wird durch verschiedene, von der Einstufung (s.o.) abhängigen Methoden geprüft. *Level 1 Merchants* müssen sich jährlich einem On-Site Security Audit unterziehen[3] und darüber hinaus pro Quartal einen „externen Scan" durchführen lassen. Bei allen anderen besteht die Prüfung aus vierteljährlichen Scans und einem auszufüllenden Self Assessment Questionnaire.

Das On-Site Audit und die externen Scans dürfen nur durch Prüfer vorgenommen werden, die dafür von den Kreditkarten-Unternehmen akkreditiert sind; dies sind die Qualified Security Assessors (QSAs) bzw. Approved Scanning Vendors (ASVs)[4]. Für die externen Scans werden üblicherweise typische Vulnerability Scanner verwendet (nessus et.al.).

Seit PCI 1.1. müssen aber auch „Application-layer penetration tests" (PCI DSS 11.3.2) stattfinden, weshalb verstärkt Applikations-Scanner wie Watchfire Appscan zum Einsatz kommen. Die eigentliche intellektuelle Leistung des ASV ist hinsichtlich der Scans selbst meist gering und besteht eher in der „ansprechenden Aufbereitung" der Ergebnisse.

Aufwendiger ist bei Level 1 Merchants das jährliche On-Site Security Audit. Was dort geprüft wird, ist jedoch in den öffentlich erhältlichen Security Audit Procedures

[3] Dessen „Prüf-Checkliste" auch weitgehend in den xyz spezifiziert ist, was eine Vorbereitung darauf erheblich vereinfacht.
[4] Details zu den Anforderungen an solche finden Sie unter ...

beschrieben; eine entsprechende Vorbereitung der Prüfung also möglich (vorausgesetzt, die inhaltlichen Anforderungen werden erfüllt). Bei Non-Compliance

werden von den Karten-Unternehmen teilweise empfindliche Geldbussen verhängt (dies geschieht in der Praxis tatsächlich). Diese werden zwar nicht veröffentlicht, tauchen aber möglicherweise an irgendeiner Stelle im Geschäftsbericht in erkennbarer Form auf (je nach Höhe).

Es sollte weiterhin stets bedacht werden, dass erfüllte PCI Compliance auch keinesfalls vor der sich aus vielfältiger Quelle eventuell ergebenden Haftung bei Kompromittierung von Kreditkartendaten schützt.

Das Bestreben nach PCI Compliance kann aufgrund der umfassenden, durchdachten Anforderungen sehr hilfreich zur Verbesserung der Gesamt-Sicherheit sein und ist meist ganz „handfest“ motiviert. Aus Sicht des Autors hat PCI schon heute in einer Reihe von Umgebungen mehr bewirkt als diverse andere Standards oder Richtlinien. Umgekehrt erleichtert etwa eine bereits vorhandene ISO 27001 Zertifizierung den Nachweis von PCI Compliance enorm. Zusammenfassend kann festgehalten werden, dass ein ganzheitlicher, strukturierter Sicherheits-Ansatz auch hier der „Compliance“ zuträglich ist.

Quellen:

[1] *PCI DSS Supporting Documents*
https://www.pcisecuritystandards.org/tech/supporting_documents.htm

Mit freundlichen Grüßen,

Enno Rey
CISSP, ISSAP, CISA

Kontakt:
Roland Fiege
Kaufm. Geschäftsführer
ERNW Enno Rey Netzwerke GmbH
Breslauer Str. 28
69124 Heidelberg
Tel. +49 6221 480390
Fax +49 6221 419008
Mobil +49 151 16 22 7557
rfiege@ernw.de, www.ernw.de