T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting 2014
Berlin, 03. - 04.11.2014

Die Schwächen des Sicherheitsstandards PCI DSS (Payment Card Industry Data Security Standard)

Patrick Sauer, M.Sc.
binsec – binary security UG

Patrick Sauer

- Information Security Consultant, binsec - binary security UG
- Chief Information Security Officer, Euro Payment Group GmbH u.a. verantwortlich für die PCI DSS Compliance
- M.Sc. in Security Management, Dipl.-Wirtsch.-Inform.(FH)
- CISSP, CISM, OSCP, TISP, CPSSE, DSB-TÜV
- Profil als PDF unter www.binsec.de/team/

Zielstellung

- Keine detaillierte Einführung in PCI DSS, sondern

  Schwächen des PCI DSS aufzeigen

- Keine Lösungsvorschläge, sondern

  zum Nachdenken anregen

PCI DSS – Key Facts

- 12 übergeordnete Requirement-Kategorien

  organisatorische + technische Anforderungen
- Ziel: Sicherstellung der Vertraulichkeit der Karteninhaberdaten (PAN + Authentifizierungsdaten)
- Compliance-Nachweise abhängig vom Transaktionsvolumen*
  - Für alle: Schwachstellen-Scan (ASV) und Attestation of Compliance
  - Bei Level 1 On-Site Audit QSA/ISA, sonst nur Self-Assessment Questionnaire (SAQ)

*Vereinfachte Darstellung.

Compliance-Kette & Selbstbewertungsbogen

- Annual Self-Assessment Questionnaire (SAQ) für “kleinere” Service Provider (< 300.000 Transaktionen/Jahr) oder Merchants (< 6.000.000 Transaktionen/Jahr) - VISA Europe
- PCI DSS kostet Ressourcen & Geld, eine Unterschrift ist kostenlos (solange nichts passiert)
- Compliance-Kette schwächt sich nach unten ab:
  Acquirer > Service Provider > Merchants (> Service Provider)

Auditoren

- Unterschiedlicher fachlicher Background
- Unterschiedliche fachliche Ansichten
- PCI DSS besitzt Interpretationsspielraum:
  - „Pentest nach signifikanter Änderung?“
  - „Bewertung von Schwachstellen-Reports?“
- Stichprobenhafte Prüfung
- Notwendiges Vertrauen auf wahrheitsgemäße Auskunft

Definition Scope

- Woraus setzt sich das Cardholder Data Environment zusammen?
- Was ist eine effektive Trennung zwischen PCI-Scope & Rest?

Systemadministratoren

- Übermächtige Systemadministratoren
- Nur Gewaltentrennung zwischen Admins vs. Entwicklern
- Kein Review-Prozess analog Software-Entwicklung
- Angriffsvektor No. 1 – Über den Admin-Client

Code & Mobile Apps

- Gut: Change Management, Reviews, uvm.
- Aber:
  - Code-Schutz?
  - Code-Signierung?
  - Buildsysteme?
- Mobile Apps für Endkunden (!= Merchants): Out of Scope

Krypto

- Gut: Key Management, Algorithmen, Konzepte, HSM
- Aber:
  - Krypto sichert nur den „stromlosen Systemzustand“
  - Angriffsvektor „Klartext-PANs im laufenden Betrieb auslesen“

Fazit

- Positiv:
  - Weitgehend guter und sicherer Standard
  - Teilweise sehr konkret und umfassend
- Problematisch:
  - Keine 100%ige Abdeckung aller Angriffsvektoren
  - Weiterhin Interpretationsspielraum
  - Problem Compliance-Nachweis vs. Kosten (SAQ vs. Audit)

Patrick Sauer
ps@binsec.de

binsec – binary security UG

Leistungen:

- Security Consulting
- Penetration Testing
- Secure Application Hosting
- Schulungen

Kontakt: info@binsec.de

Anschrift: binsec – binary security UG (haftungsbeschränkt)
Rotfeder-Ring 11, 60327 Frankfurt am Main