2011 PCI Community Meeting
Újdonságok

Tassi Miklós
Gáspár Csaba

AperSky
Bankkártya és biztonság

2011. december 7.

Napirend

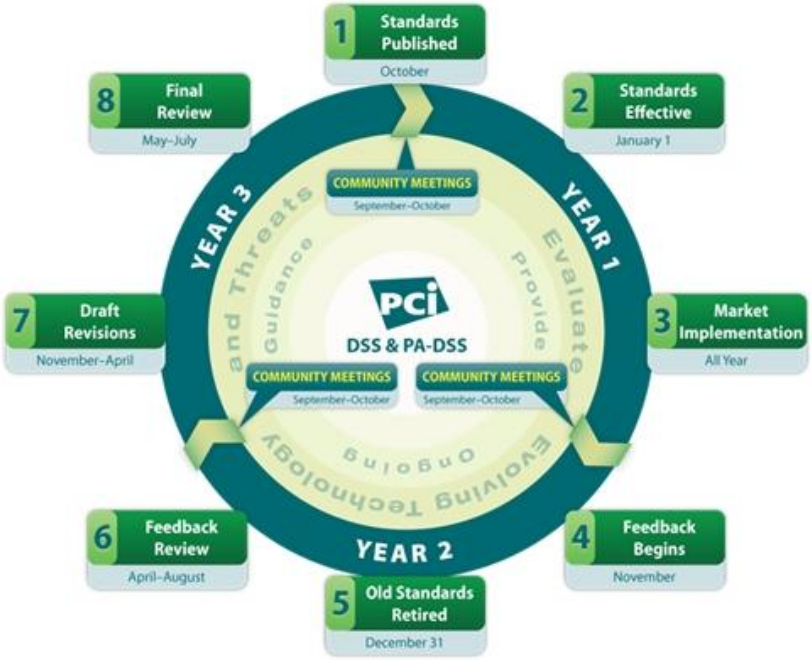
- Mi az a PCI Community Meeting?
- Fontosabb események
- Új ajánlások
  - P2PE
  - EMV
  - Virtualizáció
  - Tokenizálás
  - Vezeték nélküli hálózatok
  - Telefonos kártyaadat tárolás
  - Mobil fizetés

2011 – PCI Community Meeting

- PCI SSC European Community Meeting
- Éves szakmai találkozó és konferencia a PCI érintett szervezetei között
- London, 2011 október 17-19.
- 2 QSA képviselte az AperSky Kft.-t
- Témák:
  - Szakmai előadások ASV-k, QSA-k, ISA-k számára
  - Piaci tendenciák, új területek
  - A PCI szabályozási környezet újdonságai

PCI DSS életciklus

- Aktuális verzió:
  PCI DSS 2.0
- 36 hónapos életciklus a korábbi 24 helyett
- Életbe lépett:
  2011. január 1-én
- Előző verzió (1.2) életciklusának a vége:
  2011. december 31.



Újdonságok: P2PE program 1.

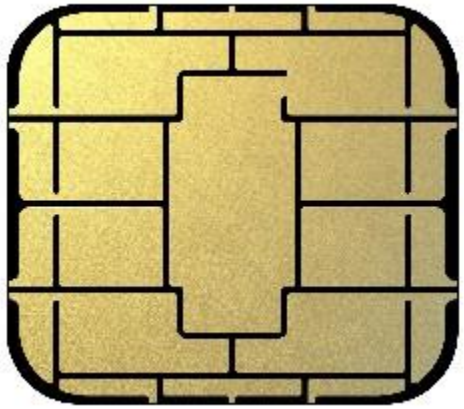
- Point-to-point Encryption Program
- Jelenleg kidolgozás alatt
- Cél: hardver-alapú titkosítási megoldások szabványos értékelése
- Új szabvány és követelménylista
- Nem helyettesíti a meglévő szabványokat, de magába foglal bizonyos elemeket másokból:
  - PTS: Point Of Interaction eszközök validálása
  - PA-DSS: fizetési alkalmazás a POI-n
  - PCI PIN: titkosító kulcsok kezelése
  - PCI DSS: P2PE környezet implementálása

P2PE program 2.

- A P2PE előírások 6 domain-be csoportosítva a hardver, titkosító eszközök és adattovábbítás területén
- Érintettek:
  - Kereskedők, szolgáltatók (csak mint felhasználók)
  - POI eszköz gyártók
  - Alkalmazásfejlesztők
  - P2PE Megoldás szállítók
- Mérföldkövek, határidők:
  - 2011 Szeptember – P2PE követelmények, előzetes változat
  - 2011 Q4 - P2PE követelmények részletes teszteljárásokkal
  - 2012 Q1 – P2PE auditor minősítés és megoldások listája

Újdonságok – EMV & PCI DSS

- Az EMV megoldások kiegészítik a PCI DSS-t (elsősorban fizikai kereskedőknél), de nem helyettesítik azt
- Kártyatársaságok adhatnak könnyítést a chipes környezetekre vonatkozóan
- Védendő adatok megfeleltetése
  - Track Data -> Track Data Equivalent
- Hibrid környezetek -> az EMV biztonsági céljai nem teljesülnek teljes mértékben
- Jövőbeni fejlesztések szükségessége
  - Tiszta EMV kártyák kibocsátása
  - CNP környezetekben kiegészítő biztonsági lépések



Új ajánlás - Virtualizáció

- Az ajánlás tartalma:
  - Virtuális megoldások PCI DSS-érintettsége
  - Virtualizált környezetek kockázati tényezői
  - PCI DSS-megfelelő megoldások, ajánlások
- Kockázatok
  - Bizonyos sebezhetőségek megmaradnak
  - Új támadási felület: a Hypervisor
  - „Leggyengébb láncszem”
- Mi van a scope-ban?
  - Hypervisor
  - Virtuális gép, eszköz, hálózati eszköz, alkalmazás és kliens
- Cloud
  - A CDE elválasztása más entitásoktól
  - PCI DSS-minősített szolgáltatók

Új ajánlás - Vezeték nélküli hálózatok

AperSky
Bankkártya és biztonság

Új ajánlás - Tokenizálás

AperSky
Bankkártya és biztonság

További ajánlások

- Telefonos kártyaadat tárolás
  - Útmutató a hang alapú kártyaadat kezeléshez és tároláshoz
  - Ajánlások az audit scope-jának meghatározásához
  - Felkészülési tanácsok Call Centereknek
- Mobil fizetési alkalmazások
  - Mobil alkalmazások és eszközök PA-DSS kötelezettsége
  - 3 kategória a mobilfizetési eszközök értékelésére és megfelelési kötelezettségeire
  - Okostelefonok, PDA-k, tabletek

Összefoglalás

- A támadások legfőbb célpontjai mi vagyunk
- Nincs bevehetetlen erőd
- Folyamatos technológiai fejlődés
- A fejlesztésekben nem a biztonság az első
- A biztonsági szabványok igyekeznek lépést tartani a fejlődéssel

A PCI szabványainak való megfelelés nem statikus és nem egyszeri tevékenység!

AperSky

Bankkártya és biztonság

Köszönjük a figyelmet!

AperSky Tanácsadó Kft. | **Iroda:** 1053, Budapest, Veres Pálné u. 4-6. | **Telefon:** +36 1 781 2210 | **E-mail:** info@apersky.com | **Web:** www.apersky.hu