QSA assessment tapasztalatok az auditor szemszögéből

Tassi Miklós
Tátrai Péter

AperSky
Bankkártya és biztonság

2011. december 7.

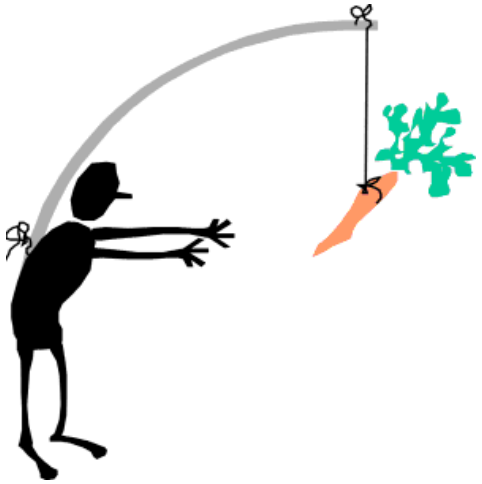
Napirend

AperSky
Bankkártya és biztonság

- A PCI DSS megfelelés motivációi
- Audit kötelezettség háttere
- A QSA assessment szolgáltatás
- Az audit scope meghatározása
- Audit végrehajtása - tapasztalatok
- IT biztonsági vizsgálatok
- Prioritized Approach előnyei
- Önértékelő kérdőívek (SAQ)

A PCI DSS megfelelés motivációi

AperSky
Bankkártya és biztonság



- **Külső felszólítás**
  - Szolgáltatók → Kártyatársaság által
  - Bankok → Kártyatársaság által
  - Kereskedők → Elfogadó bank által
- **Belső kezdeményezés**
  - Új szolgáltató cég indítása → megfelelés kötelező!
  - Üzleti profil bővítés lehetőségei
  - Magas biztonság tudatossági szint

→ A QSA cég csak véleményt nyilvánít, de nem dönt!

PCI DSS audit kötelezettség háttere

AperSky
Bankkártya és biztonság

- **1. szintű Szolgáltatók**
  - Évi 300e tranzakció felett (Visa, MasterCard)
  - Adatvesztésnél
  - Kártyatársasági felszólítás esetén

- **1. szintű Kereskedők**
  - Évi 6 millió tranzakció felett (Visa, MasterCard)
  - Adatvesztésnél
  - Kártyatársasági felszólítás esetén
  - Belső auditor (ISA) is elvégezheti

- **Elfogadó/Kibocsátó Bankok**
  - PCI megfelelés elvárt → nincs általános audit kötelezettség

A QSA assessment szolgáltatás

AperSky
Bankkártya és biztonság

- **Audit keretek meghatározása**
  - Szerepek, felelősségi körök
  - Audit terv és ütemezés
- **Scope meghatározása**
  - Üzleti és technikai profil megalkotása
  - Hálózati diagram elemzése
  - Kártyaszám keresés (PAN scan)
  - Kártyaadat környezet (CDE) mátrix véglegesítése

A QSA assessment szolgáltatás

AperSky
Bankkártya és biztonság

- **Audit végrehajtása**
  - Technikai vizsgálatok
  - Dokumentációk ellenőrzése
  - Folyamatok, procedúrák megfigyelése
  - On-site interjúk
  - Vizsgálati bizonyítékok begyűjtése
  - Kompenzációs elemek dokumentálása
- **Audit dokumentumok kitöltése, átadása**
  - Report on Compliance (ROC)
  - Attestation of Compliance (AOC)
- **Minőségügyi visszajelzések**

Audit felkészülési tanácsok

- Top menedzsment támogatás
- Költségvetés biztosítása
- Külső szakértői támogatás igénybe vétele
- Céges biztonság tudatossági program
- Belső felelős személy kijelölése
- Kommunikáció biztosítása
  - Kártyatársaságok
  - Elfogadó bank
- Felkészülési idő biztosítása (6-12 hónap)
- Előkészítés végrehajtása
  - Előzetes gap analízis
  - Implementáció
- Prioritized Approach használata

Az audit scope meghatározása

- **PCI DSS hatályon kívül kerülés**
  - Kártya adatkezelés kiszervezése másik cégbe
  - Nem kezelni kártyaadatot
- **Audit scope és költségek csökkentése**

Audit végrehajtása - tapasztalatok

AperSky
Bankkártya és biztonság

Audit végrehajtása - tapasztalatok

IT biztonsági vizsgálatok

- **Külső sebezhetőségi vizsgálat (ASV scan)**
  - Negyedévente és minden változtatás után
  - Kizárólag ASV cég!
- **Belső sebezhetőségi vizsgálatok**
  - Negyedévente és minden változtatás után
  - ASV bevonás nem kötelező
- **Web alkalmazás sebezhetőség vizsgálat**
  - Évente egyszer és minden változtatás után
  - ASV bevonása nem kötelező
- **Behatolási teszt**
  - Évente egyszer és minden változtatás után
  - ASV bevonás nem kötelező

Prioritized Approach alkalmazása

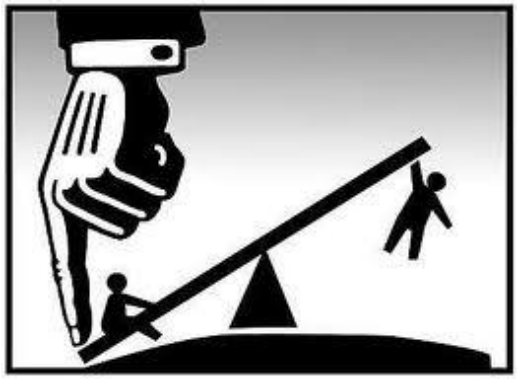
AperSky
Bankkártya és biztonság

Tartalma:

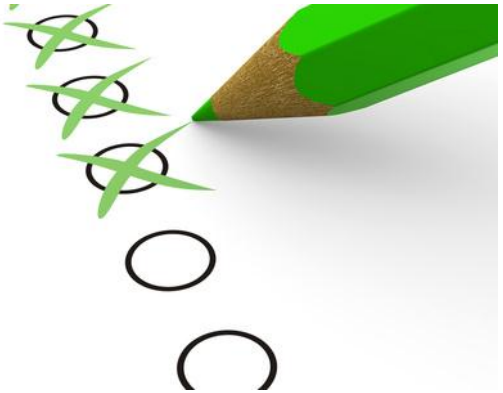
- Letölthető a PCI Council honlapjáról (2.0 verzió)
- Elsősorban kereskedőknek, de másnak is hasznos
- PCI DSS megfelelés 6 priorizált mérföldkő alapján
  - 1. Érzékeny authentikációs adat eltávolítás, tárolás korlátozás
  - 2. Határoló, belső, vezeték-nélküli hálózatok védelme
  - 3. Biztonságos fizetési kártya alkalmazások
  - 4. Rendszer hozzáférések monitorozása, ellenőrzése
  - 5. Tárolt kártyaadatok védelme
  - 6. Fennmaradó megfelelési követelmények, kontrollok biztosítása

Prioritized Approach alkalmazása

AperSky
Bankkártya és biztonság



Önértékelő kérdőívek (SAQ)



- Kire nézve kötelező?
  - 2-3. szintű Kereskedők (>20e évi tranzakció)
  - 2. szintű Szolgáltatók (<300e évi tranzakció)
- Kérdőív átadása kártyatársaság/Elfogadó Bank felé
- QSA cég igénybevétele nem kötelező, de ajánlott
- Csak kereskedőknek:
  - SAQ A: Card-not-present tranzakciók (e-commerce, internet, e-mail, telefonon történő authorizáció), kiszervezett tevékenységként
  - SAQ B: Imprinter („vasaló”) készülék használata, különálló, dial-up POS terminálok, nincs elektronikus bankkártya-adat tárolás
  - SAQ C-VT: Web alapú virtuális terminálok (VPOS), nincs elektronikus bankkártya-adat tárolás
  - SAQ C: Internethez csatlakozó fizetési alkalmazások használata, nincs elektronikus bankkártya-adat tárolás
- Kereskedők és Szolgáltatók:
  - SAQ D: Minden egyéb szervezet, akit a kártyatársaság arra kijelöl

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