PCI DSS

AperSky
Bankkártya és biztonság

Ügyfeleink részére az alábbi teljes körű PCI DSS szolgáltatásainkat kínáljuk.

PCI DSS felkészülés

1. PCI DSS előzetes felmérés (pre-scoping)

A pre-scoping fázis során felmérésre kerül a vállalat lehetséges PCI DSS érintettsége, már implementált működési környezete, illetve megjelölésre kerülnek azok a főbb területek, amelyekre PCI DSS felkészülési alprojektek indítása szükséges lehet.

2. PCI DSS stratégia kialakítása

A pre-scoping fázis során feltárt eredményeket, illetve a PCI DSS megfelelés szükségessége által érintett tevékenységeket áttekintve egyértelmű és reális stratégiai célokat fogalmazunk meg. A tervezés során felmerülő megvalósítási alternatívákra magas szintű költség- és egyéb ráfordításbecslést is végzünk, amely lehetővé teszi egy felsővezetői döntés meghozatalát a további fejlesztési irány kiválasztásához. A stratégiai terv tartalmazza a jelenlegi helyzetnek megfelelő reális felkészülési roadmap-et, melyben külön kiemelésre kerülnek a fontosabb döntési pontok, valamint a felkészülési projekt várható ütemezése.

3. Gap elemzés

Széleskörű vizsgálatot folytatunk az érintett szervezeti egységek bevonásával, majd összefoglaljuk a feltárt hiányosságokat, nem megfelelő elemeket, ezen felül sor kerül az aktuális PCI DSS szabványtól való eltérések meghatározására minden egyes – az audit körébe tartozó – területen.

A Gap elemzés kiterjed az alábbi tevékenységek elvégzésére:

- Kártyakörnyezet meghatározása, feltérképezése
- Gap-ek vizsgálata
  - Meglévő dokumentáció vizsgálata
  - Meglévő procedúrák felderítése
  - Jelenlegi technikai beállítások, paraméterek vizsgálata
- A feltárt gap-ek értékelése és részletes dokumentálása

4. PCI DSS felkészülési megoldás és akcióterv (Remediation plan)

A Gap elemzés eredményeképpen szakértőink részletes dokumentációt készítenek, amely feltárja a gap-ek megoldásához, illetve azok implementációjához szükséges lépéseket. Ezen dokumentáció alapján tanácsadóink az Ügyfél közreműködésével akciótervet készítenek, amely mintegy projekttervként is szolgálva összefogja a szükséges megoldási lépéseket, illetve implementációs folyamatokat. Ezen túlmenően segítjük Ügyfeleinket a lehetséges helyettesítő kontrollok meghatározásában is.

PCI DSS implementáció

Implementációs támogatás

Kollégáink a Remediaton plan alapján megkezdődő implementáció során is támogatást nyújtanak az Ügyfelek részére. Az auditori függetlenség megtartásának érdekében nem magában az implementációban veszünk részt, hanem PCI DSS kérdésekre vonatkozó tanácsadást és dokumentációs támogatást nyújtunk.

PCI DSS oktatás

Ügyfeleink számára egyedi igényekhez igazított PCI DSS oktatást is biztosítunk.

PCI DSS technikai vizsgálatok

ASV scanning (Approved Scanning Vendor) szolgáltatások

Az ASV scanning kötelező eleme minden szintű PCI DSS riportnak, amely vizsgálatot az elfogadói hálózatban részt vevő Kereskedőknek és Szolgáltatóknak is végre kell hajtani. Ügyfeleink részére hivatalos ASV (Approved Scanning Vendor) scanning szolgáltatást biztosítunk partnerünk, a Qualys Inc. bevonásával, amely az alábbiakat foglalja magában:

- Technikai tanácsadás, scanning vizsgálatok elvégzése
- Negyedéves kötelező ASV scan-ek végrehajtása
- Hivatalos ASV dokumentum kibocsátása, amely minden PCI riporthoz szükséges
- Ismételt scan-ek kivitelezése

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

PCI DSS

AperSky
Bankkártya és biztonság

Belső sérülékenységi vizsgálat elvégzése (Internal Vulnerability Scan)

A sérülékenységi vizsgálat minden esetben a belső hálózaton ideiglenesen elhelyezett vizsgálati eszközzel (Scanner Appliance) történik, az adott hálózati szegmenshez tartozó, az Ügyfél által előre meghatározott hálózati eszközökre, illetve IP-címekre.

- Teljes hálózati topológia felderítése
- Vezeték-nélküli hozzáférési pontok felderítése
- Idegen eszközök felderítése
- Az előre meghatározott IP címek scannelése
  - Nyitott portok keresése
  - Az eszköz típusának, operációs rendszerének, verziójának felderítése
  - Sérülékenységek feltárása, az aktuálisan futó hálózati szolgáltatások felmérése
  - A hálózati szolgáltatások mögött futó alkalmazások verziójának felderítése
  - Fenyegetettségek mértékének feltárása, javaslatok a biztonsági hiányosságok megszüntetésére

Web alkalmazások sérülékenységi vizsgálata (Web Application Scan)

A sérülékenységi vizsgálat kiterjed minden olyan webes alkalmazásra, amely nyilvánosan elérhető, és valamilyen módon részt vesz a kártyabirtokosi adatok továbbításában, feldolgozásában vagy tárolásában. Web alkalmazások vizsgálatához cégünk a Qualys Inc. által fejlesztett és üzemeltetett QualysGuard® WAS (Web Application Scan) eszközét veszi igénybe.

A vizsgálat kiterjed:

- Web alkalmazások sérülékenységi vizsgálata
  - SQL Injection sérülékenységek
  - Cross Site Scripting (XSS) hibák
  - Directory traversal
  - Oldal-források védelme
  - Server oldali script hibák felderítése
  - URL átirányítási hibák
- Web alkalmazás autentikációjának vizsgálata
- Riport készítése a vizsgálat eredményéről
  - Összegzés a menedzsment részére
  - Részletes műszaki riport az egyes hiányosságokról

PCI DSS tanúsítás

PCI DSS hivatalos QSA vizsgálat

Az Assessment egy, a QSA cég által vezetett tanúsító audit, melynek scope-ját a QSA cég határozza meg a vizsgált szervezet számára. Az auditot évente kell végrehajtani. Cégünk, valamint PCI DSS szakértőink hivatalos QSA minősítéssel rendelkeznek, ezáltal képesek teljes körű QSA Assessment támogatást és végrehajtást biztosítani az Ügyfelek részére.

A QSA vizsgálat az alábbi főbb elemeket tartalmazza:

- Scope meghatározása
- Gap elemzés
- On-site interjúk és felülvizsgálat
- Vizsgálati bizonyítékok begyűjtése
- Helyettesítő kontrollok dokumentálása
- QSA vizsgálat teljes körű összefoglaló dokumentációja
- „Report on Compliance” dokumentum kiállítása
- “Attestation of Compliance” dokumentum kiállítása
- Minőségügyi visszajelzések összegyűjtése az Ügyfél részéről

PCI DSS Self Assessment Questionnaire (SAQ) felülvizsgálata

Nem minden érintett szereplő számára kötelező az éves PCI DSS audit: bizonyos tranzakciószám, vagy kezelt kártyaadat szám alatt önkéntes értékelés is elfogadott, mely esetén gyakori egy QSA cég bevonása a leírt információk validálásához. Az önértékelés esetén az egyes elfogadói vagy adattárolási tevékenységekre külön-külön, meghatározott típusú kérdőívet szükséges kitölteni. A Kereskedőknek és Szolgáltatóknak az önértékelés lefolytatását tanúsító dokumentumokat az elfogadó bank, illetve a kártyatársaságok rendelkezésére kell bocsátaniuk. Cégünk igénybevétele esetén – mint QSA Assessor – áttekintjük és validáljuk a Kereskedő vagy Szolgáltató által kitöltött dokumentumokat.

Az önértékelési szolgáltatás főbb tartalma:

- Az SAQ kérdőív típusának kiválasztásában való segítségnyújtás
- A SAQ kitöltésének tanácsadói támogatása
- A PCI DSS tanúsítványként szolgáló, a Kereskedő vagy Szolgáltató által kitöltött „Attestation of Compliance form” validálása

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