

The Nixu logo is displayed in white, lowercase letters on a dark blue background. A thin white vertical line is positioned to the right of the logo.

nixu

Kokemuksia Suomalaisista PCI-auditoinneista

6.9.2006

Jonna Särs, QSAP, CISSP
jonna.sars@nixu.com

Sisälllys

- Millainen PCI-auditointi on?
- Auditointiin valmistautumisen minimitaso
- Turhat tavat reputtaa auditointi
- Vaikeaksi osoittautuneet tavat reputtaa auditointi
- Tapoja helpottaa vaatimusten täyttymistä

Millainen PCI On-Site Audit on?

- Auditointiin sisältyy
 - Dokumenttien katselmointi
 - Henkilöstön haastatteluja
 - Käytäntöjen ja toimintatapojen havainnointi käytännössä
 - Verkkolaitteiden, palvelinten, työasemien yms. tietoturvatarkastus
 - Tietoliikenteen suojauksen tarkastus
 - Tilojen fyysisten suojausten katselmointi
- Kesto keskimäärin n. viikon
 - Jos jaksotetaan pitemmälle ajanjaksolle, kalenteriaikaa ensimmäisestä tarkastusosioista raportin luovuttamiseen Visalle/MasterCardille saa kulua korkeintaan 2 kuukautta

Vaatimusten kompensointi ja poikkeukset

- Jos yksittäistä PCI-vaatimusta ei voida suoraan toteuttaa, voidaan hyväksyttävällä kompensoivalla metodilla saavuttaa vaatimustenmukaisuus
- Kompensoivan metodin tulee täyttää vaatimuksen henki ja haettu turvataso
 - Samalla metodilla ei voi kuitata useampaa vaatimusta
- Kompensoivat metodit hyväksyy jokaisen auditoinnin osalta Visa/MasterCard
 - Dokumentoitava erityisen huolellisesti
- Paikalliset lait ja asetukset voivat kumota tai lieventää/tiukentaa PCI-vaatimuksia

Auditointiin valmistautuminen

- Kannattaa ainakin lukea standardi ja täyttää Self-Assessment Questionnaire ennen auditointia
 - Auditoija haluaa nähdä itsearviointin tulokset
 - Lomaketta täyttäessä näkee keiltä kaikilta tietoa täytyy kerätä, eli keiden osallistuminen on tarpeen myös auditoinnissa
 - Lomaketta täyttäessä saa tuntumaa siitä, onko oma tilanne hyvä vai huono
- Listaa sovellukset/järjestelmät joissa on korttidataa
- Jos politiikat ja ohjeistukset, verkkokuvat yms. dokumentit puuttuvat, varsinaista auditointia ei kannata aloittaa
 - Gap-analyysillä voidaan selvittää muut alueet joilla on puutteita

Itsearviointi vs. auditointi

- Itsearviointilomake ei ole yhtä yksityiskohtainen ja kattava kuin auditointivaatimukset
 - Läpi mennyt itsearviointi ei vielä takaa että auditointi menee läpi
- Nyrkkisääntö: itsearviointilomakkeessa edellytetään että suojaavia toimenpiteitä on tehty, auditoinnissa tarkastetaan että ne on tehty tietyllä tavalla
 - Auditoinnissa myös esim. tarkastetaan, että ihmiset todella toimivat määriteltyjen prosessien mukaisesti
- Toisaalta: itsearviointiin ei voi vedota kompensoiviin kontroleihin

“Turhia” syitä reputtaa auditointi

- Tietoturvapolitiikka puuttuu tai siitä ei ole tiedotettu käyttäjille
- Toimintatapoja ei ole dokumentoitu
- Puutteelliset prosessit esim. käyttäjätunnusten ja käyttöoikeuksien luomisessa ja poistamisessa
- Tietoturvakorjausten asentamiseen ja/tai konfiguraation muutoksiin liittyviä prosesseja ei ole, tai dokumentit eivät vastaa todellisia käytäntöjä
- Suunnitelma poikkeustilanteisiin ja väärinkäyttöön reagoimiseksi puuttuu
 - Esim. Tietomurto jossa korttitietoja joutuu väärin käsiin

“Turhia” syitä reputtaa auditointi (jatkuu)

- Verkkokuvat puuttuvat tai eivät ole ajan tasalla
- Palomuurien säännöstöjä ei ole dokumentoitu
- Virustorjunta, sähköpostin salaus ja/tai tunkeutumisen havaitsemisjärjestelmä puuttuvat
- Järjestelmiin liittyvien haavoittuvuuksien havainnointiin ei ole prosessia
- Ylläpitäjät käyttävät salaamattomia yhteyksiä ylläpitoon

Hankalaksi osoittautuneita osa-alueita

- Maksukorttitietojen säilytys salattuna
 - Varmuuskopiot
 - Tietokannat
 - Erityisesti isokoneympäristöt
- Avaintenhallinta
 - Erityisesti säilytettävän tiedon salaamiseen käytettävät avaimet
- Uratietojen säilytyskielto
 - Poistaminen esim. vanhoilta varmuuskopioilta
- Korttitietojen näyttäminen käyttäjille
 - Saattaa vaatia sovellusmuutoksia
- CRM:n ja luottokorttitietojen yhdistelmä
 - Esim. Mihin vedetään “tarve tietää”-raja?

Hankalaksi osoittautuneita osaluueita (jatkuu)

- Vain yksi ensisijainen käyttötarkoitus per palvelin
 - Varsinkin pienissä organisaatioissa
- PCI-vaatimusten sisällyttäminen sopimukseen
 - Sopimuskumppanit eivät välttämättä suoraan niele uusia vaatimuksia, varsinkaan muodossa “Sitoutuu noudattamaan kaikkia PCI-vaatimuksia”
- Tehtävien erottelu
 - Varsinkin pienissä organisaatioissa
- Lokivaatimukset
 - Vaatii usein sovellus- ja järjestelmämuutoksia sekä keskitetyn ja turvallisen toteutuksen lokien ja audit trailin hallintaan
- Järjestelmien koventaminen
 - Vaatimus koskee myös tietoliikennelaitteita

Tapoja helpottaa omaa tilannetta

- Verkon segmentointi palomuuureilla!
- Minimoidaan ja keskitetään paikat, joissa maksukorttitietoja käsitellään ja säilytetään
- Maskataan tai katkaistaan maksukorttitieto aina kun mahdollista, aina ei tarvita salausta
- Hyväksytetään kompensoivia kontroleja, jos suojaukset on toteutettu eri tavalla kuin vaatimuksissa on kuvattu
- Jos kaikkien vaatimusten täyttäminen nopeasti tuntuu haasteelliselta, kannattaa tehdä riskianalyysi ja arvioida mitkä toimenpiteet nopeimmin pienentävät korttitietojen vuotamisriskiä

Yhteenveto

- Tällä hetkellä Euroopassa vain n. 70 vaatimukset täyttävää ja n. 50 “In Progress” -tasolla olevaa palveluntarjoajaa
 - Kauppiaiden statusta ei raportoida julkisesti
- Varsinkin suurilla organisaatioilla jotka toimivat PCI:n näkökulmasta useissa erilaisissa rooleissa ja ovat käsitelleet maksukorttitietoja pitkään, vaatimusten täyttäminen ei välttämättä ole tehtävissä nopeasti
 - Tavoitteena tällä hetkellä saada työ käyntiin ja päästä “In Progress” -statukselle
- PCI-vaatimusten täyttäminen voi aluksi tuntua varsin haasteelliselta, mutta yhteistyössä auditoijan kanssa ongelmakohtiin yleensä löytyy kohtuullinen ratkaisu