LAUREA AMMATTIKORKEAKOULU Uuden edellä

Turvallinen maksaminen kaupoissa

Sorvari, Teemu

2012 Leppävaara

Laurea-ammattikorkeakoulu

Leppävaara

Turvallinen maksaminen kaupoissa

Teemu Sorvari
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Marraskuu, 2012

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Tietojenkäsittelyn koulutusohjelma

Sorvari, Teemu

Turvallinen maksaminen kaupoissa

Vuosi 2012 Sivumäärä 44

Korttirikollisuus on yleistynyt maailmalla. Suomessakin on jo esimerkkejä tietomurroista, jotka liittyvät korttirikollisuuteen. Yritys X:ssä käynnistyi vuonna 2008 Projekti joka keskittyi turvalliseen maksamiseen. Sen päämääränä oli luoda uusi turvallisempi maksuympäristö kauppoihin.

Tarkoituksena oli luoda ympäristö, joka oli PCI-standardin mukainen. Näin ollen monen vuoden esiselvityksen jälkeen päädyttiin tekemään maksupäätejärjestelmä, joka ei tallenna sensitiivistä maksukorttitietoa kauppojen järjestelmiin. Uudessa maksupäätejärjestelmässä asennettiin uudet maksupäätteet, jotka keskustelevat kassan kanssa, mutta eivät jaa maksukorttidataa kaupan järjestelmään.

Maksupäätteiden asentamisen lisäksi projekti on vaatinut paljon työtä PCI-standardin parissa. Kauppoihin oli tehtävä standardin mukaiset muutokset, jotta ne voitaisiin jälkikäteen auditoida. Auditoinnin tavoitteena oli saada kohdeyrityksen kaupoille PCI-sertifiointi. Maksupäätejärjestelmän uusimisen lisäksi projektiin kuului myös yleisen tietoturvallisuuden parantaminen. Tämän opinnäytetyön tavoitteena oli tutkia, millä tavalla kohdeyrityksen projekti ja PCI ovat vaikuttaneet kauppojen jokapäiväiseen toimintaan. Tutkimuksessa perehdyttiin saatavilla olevaan aineistoon kohdeyrityksen raportteja tutkimalla, sekä lopuksi suoritettiin haastattelut viidelle henkilölle. Haastateltavista neljä oli projektissa mukana ollutta yrityksen henkilökuntaa, sekä erään liikenneaseman kauppias.

Haastattelutuloksia tutkimalla saatiin monesta eri näkökulmasta asioita esille, jotka ovat vaikuttaneet kauppojen toimintaan. Tietoturvatietoisuus on ollut keskeisesti esillä ja työssä arvioidaan tietoturvatietoisuuden parantuneen. Projektista on tullut kaupoille myös konkreettista hyötyä. Esimerkiksi vanhojen kuittiarkistojen siivous on tuonut lisää tilaa ahtaisiin tiloihin. Kehitysehdotuksena tutkitaan mitä vaatii että kohdeyrityksen projektista saadaan jatkuva palvelu.

Asiasanat, turvallinen maksaminen, PCI-standardi

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Degree Programme in Business Information Technology

Sorvari, Teemu

Secure payment in stores

Year 2012 Pages 44

Payment card criminality has increased worldwide. In Finland there are already examples of breaking in to systems that hold credit card information. In the year 2008 the project of secure payment was started in Company X. The objective of the project was to create a new more secure environment for credit card payment. The purpose was to create an environment which was PCI (Payment card industry) standard compatible. Therefore, after many years of research the company ended up creating a payment terminal system that does not save sensitive payment card information into the store's IT systems. In the new system they installed new payment terminals that are in touch with the register but do not save any payment card data into the stores IT-systems.

The project has required a great deal of work on the PCI-standard in addition to installing the payment terminals. Necessary changes concerning the PCI-standard had to be made in the stores so that afterwards they could be audited. The goal of the audits was to have all stores of the company PCI-certified. In addition to renewing the payment terminal system the improvement of common information security was also a part of the project.

The objective of this thesis was to conduct research on how the project and PCI have influenced the everyday action in the stores of the company. The information at hand was accessed by reading documents made by the company and finally by performing interviews with five different people. Four of the interviewees were company staff who have been in with the project and the fifth was a service station keeper.

Many different points of view concerning changes in stores emerged from the interview results. Common information security has been in focus and therefore it is estimated in this thesis that information security awareness has improved. There have also been concrete benefits for the stores involved in this project. For example, the cleanup of the old receipt archives has brought more space in the narrow spaces. How to make the project a continuing service is researched as a development proposal.

Keywords secure payment, PCI-standard

Sisällys

1 Johdanto

Tämän tutkimuksen tarkoitus on käydä läpi kohdeyrityksen kauppojen PCI-ympäristö ja kartoittaa kaikki siihen liittyvät tekijät. Keskeisenä osana on kohdeyrityksessä vuonna 2008 käynnistynyt projekti, joka keskittyy turvalliseen maksamiseen. Tavoitteena oli muuttaa kauppojen maksujärjestelmä nykyistä tietoturvallisempaan järjestelmään.

Kauppoihin asennetaan uudet sirumaksupäätteet, jotka keskustelevat kassan kanssa, mutta eivät välitä sensitiivistä korttitietoa kaupan järjestelmiin. Uuden maksupäätejärjestelmän myötä maksaminen muuttuu siten, että pankkikortilla maksettaessa asiakas varmistaa maksutapahtuman ensisijaisesti omaa PIN-koodia käyttäen ja kortin magneettijuovan lukua käytetään vain vaihtoehtoisena maksutapana. Raportissa käydään läpi uudistuneita tietoturvaohjeita ja käytäntöjä joita projektin myötä on tullut. Uudistetut tietoturvaohjeet nojaavat vahvasti PCI-standardiin(PCI-DSS v2.0. 2010), mutta sisältävät myös muita käytännön ohjeita. Kauppiaille on olemassa oma PCI-standardi. Uudistuksen myötä yksittäistä kauppaa koskevien standardin alakohtien määrä kaventuu huomattavasti. Tutkimustapana tullaan käyttämään haastatteluja. Haastattelun kohteet ovat kohdeyrityksen henkilökuntaa sekä yksi kauppias. Haastattelujen tavoitteena oli kerätä mahdollisimman paljon tietoa eri näkökulmista projektiin. Tutkimuksen lopussa käydään läpi haastattelut ja vertaillaan kuinka paljon ja mitä muutoksia projekti on tuonut kaupan toimintaan ja tietoturvaan.

Vuonna 2010 sattuneessa tapauksessa itähelsinkiläiseen kahvilaan tehtiin tietomurto, jossa vietiin suuri määrä korttitietoja. Niki Klaus kirjoitti (Massiivinen luottokorttimurto Suomessa – olisiko se voitu PCI-standardia noudattamalla estää?, Niki Klaus, 2010) siitä, olisiko tietomurto voitu estää noudattamalla PCI-standardia. ”Payment Card Industry Data Security Standard(PIC-DSS) –implementointi on vielä hyvin monella kauppiaalla kesken, ja pienimmät kauppiaat eivät edes tiedä, että heidän tulisi noudattaa kyseistä tietoturvastandardia”, kertoo Klaus. Klausin mukaan standardin noudattaminen olisi todennäköisesti estänyt tämän tietomurron. Syyksi tietomurtoon kerrotaan se, että kassajärjestelmän asentanut yhtiö olisi jättänyt päälle oletusasetukset. PCI:n vaatimuksena oletusasetuksia ei tule käyttää. (Massiivinen luottokorttimurto Suomessa – olisiko se voitu PCI-standardia noudattamalla estää?, Niki Klaus, 2010)

2 Kohdeyrityksen projekti

Kohdeyrityksen projekti käynnistyi yrityksen konsernissa maaliskuussa 2008. Projektin tavoitteena on erityisesti korttimaksamisen turvallisuuden parantaminen. Sen lisäksi että maksamisesta tulee turvallisempaa, se on myös yrityksen liiketoiminnan kannalta kannattavaa. Projekti tukeutuu PCI-DSS v.2.0 korttimaksamisen tietoturvastandardiin. Standardissa selvitetään miten maksukorttitietoa tulee säilyttää ja arkistoida. Projektin myötä maksukorttitietoa ei kerry kauppojen järjestelmiin.

Turvallisen tietoverkon luominen ja ylläpito	Kortinhaltijan tiedon suojaaminen	Haavoittuvuuden hallinta	Käyttöoikeuksien hallinta	Tietoverkon säännöllinen valvonta	Tietoturvapolitiikka
Suojaa tiedot	Suojaa ja salaa kortinhaltijatiedot	Virustorjunta	Rajoita fyysistä ja teknistä pääsyä	Seuraa, valvo, testaa	Tietoturvakäytännöt
Älä käytä oletussalasanoja tai asetuksia		Tietoturva kehityksessä	Yksilöi käyttäjätunnukset		

Taulukko 1 PCI-DSS Tietoturvavaatimusten osakokonaisuudet

Kohdeyrityksen hankkeen keskeiset tavoitteet:

- Parantaa korttimaksamisen turvallisuutta
- Saada merkittäviä säästöjä korttimaksamisen kustannuksissa
- Toteuttaa yhdenmukainen maksamisen ratkaisu kaupan eri järjestelmiin

Asiakkaalle tulevat hyödyt:

- Kaikissa yrityksen kaupoissa on käytössä yhdenmukainen, helppokäyttöinen ja turvallinen korttimaksuratkaisu
- Kansainvälinen toimintatapa, joka kattaa korttimaksamisen turvallisuuteen liittyvät standardit
  (Yrityksen sisäinen dokumentointi, 2011)

2.1 Kohdeyrityksen projektin ratkaisu

Projektin keskeinen ratkaisu sirukorttimaksamisen turvallisuuteen on se, että maksukorttitieto pidetään uudessa järjestelmässä erillään kassajärjestelmistä. Maksupääteohjelmisto keskustelee kassapäätteen kanssa siirtämättä sensitiivistä maksukorttidataa kaupan kassajärjestelmiin. Päästä päähän salauksella, jossa korttitietoa ei siirry muihin järjestelmiin, voidaan saavuttaa tilanne, jossa vain pieni osa PCI:n vaatimuksista koskettaa kohdeyritystä. Maksukorttitapahtuma salataan ja tallennetaan keskitettyyn palveluun. Aikaisempaan järjestelmään verrattuna tämä on yksinkertaisempi. Järjestelmissä oleva korttitieto on vaikeasti erotettavissa muusta tiedosta. Järjestelmäkohtainen sertifiointi oli välttämätöntä, mutta projektin myötä jää vain yhden järjestelmän sertifiointitarve. PCI-ympäristöön kuuluvat maksupäätteet ja vain ne järjestelmät ja mediat, joissa on maksukorttitietoa. (Yrityksen sisäinen dokumentointi 2011)

2.2 Sirumaksupäätteen valinta

Kohdeyrityksessä on kerätty käyttökokemuksia ja verrattu eri sirumaksupäätteiden ominaisuuksia tuotantokäytössä. Tärkein yksittäinen tekijä maksupäätteen valinnassa on sen käyttöergonomia asiakkaalle (Yrityksen sisäinen dokumentointi 2011). Käyttöergonomialla tarkoitetaan käytön helppoutta, jota ovat näytön selkeys ja sen koko. Oleellista on myös toimintojen nopeus, jolla minimoidaan asiakkaan turhat odotusajat. Yksityisyydensuoja nousee myös tärkeäksi ominaisuudeksi. Laitteella tulee olla hyvä suoja tunnusluvun näppäilyä varten. Muita valintakriteerejä ovat päätteen kestävyys ja ominaisuudet, sekä päätelaitteen hinta ja ylläpitokustannukset.

- Päätteessä on selkeä käyttöliittymä
- Kortin syöttöaukko päällä
    - Vaivaton käyttää
- Yksityisyyden suoja
    - Päätten reunat suojaavat tunnusluvun syötössä
- Näppäimistö
    - Näppäintuntuma on hyvä
    - Numerot ovat suuria
    - Funktionäppäinten käyttö on helppoa

- Integroitu NFC-lukija

- Mg-juovan lukija
    - Lukuvarmuus on hyvä

(Yrityksen sisäinen dokumentointi, 2011)

3 Maksupäätejärjestelmän toiminnallinen kuvaus

Tässä luvussa kerrotaan maksupäätejärjestelmän toiminnallinen kuvaus. Seuraavat kappaleet käsittelevät sirukorttimaksamista sen sopimuksista ja ehdoista aina ostotapahtumaan ja siihen liittyviin varmennuksiin.

3.1 Sopimukset ja ehdot

Maksupäätteistä kerättävä data lähetetään konekielisenä Luottokunnan tai pankin hyväksymän tarjoajan kautta Luottokuntaan. Yritys saa tilittäjältä tarvittavat tunnistetiedot tapahtuman välitystä varten. Yrityksen tulee huolehtia siitä, että sen maksupäätejärjestelmät vastaavat luottokunnan sertifikaattien edellytyksiä. Tässä kappaleessa kuvataan sirumaksupäätteen toiminnalliset periaatteet.

Maksunsaaja hankkii maksupäätteen tai maksupäätejärjestelmän ohjelmistotaholta tai laitetoimittajalta. Maksupäätejärjestelmä koostuu tunnuslukunäppäimistöstä, kuittitulostimesta, maksupääteohjelmistosta, näytöstä, näppäimistöstä, siru- ja magneettijuovakortinlukijasta sekä linjayhteydestä. Yksityiskohtaiset käyttöohjeet laitteistolle toimittaa ohjelmistontarjoaja tai maksupäätteen valmistaja. Maksunsaajan on sovittava tilipankkinsa kanssa maksupäätepalvelusopimuksesta. Sopimus pankkikorttien hyväksymisestä maksuvälineenä kattaa kaikkien Suomen pankkien myöntämät pankkikortit. Muiden korttien käyttämisestä maksuvälineenä pitää sopia erikseen asianomaisen korttiyhtiön kanssa. Kullakin korttiyhtiöllä on omat ehtonsa ja muut ohjeet. Varmennuksesta ja reitittimen käyttöönotosta on sovittava pankin, teleoperaattorin tai muun palveluntarjoajan kanssa. (EMV-Maksupäätejärjestelmän toiminnallinen kuvaus V4.2, Finanssialan keskusliitto 2011)

3.2 Sirukortti

Kuva 1 Sirukortti

Sirukortilla tarkoitetaan maksukorttia, joka sisältää magneettijuovan lisäksi pienen mikrosirun, joka toimii pienen tietokoneen tavoin lisäämällä kortin turvallisuutta. Sirun ansiosta kortilla on enemmän toimintoja, mutta pääasiallinen tehtävä on tietoturvan parantaminen. Sen ulkonäkö on perinteisen maksukortin näköinen, siihen on vain upotettu siru. Sen lisäksi siinä näkyy korttinumero sekä voimassaoloaika. Kortin takana on näyte kortinhaltijan allekirjoituksesta. Tietyissä tilanteissa joudutaan turvautumaan vielä vanhaan maksutapaan, jolloin varmistus luetaan kortin magneettijuovalta ja kortinhaltija antaa allekirjoitusnäytteensä todistaakseen olevansa kyseisen kortin haltija. Kyseinen tilanne voi olla esimerkiksi oman pinkoodin unohtaminen. Sirukortin pääasiallinen tunnistus tapahtuukin siis henkilökohtaisella pinkoodilla. Magneettijuova on siis toissijainen vaihtoehto maksamiselle. (EMV-Maksupäätejärjestelmän toiminnallinen kuvaus V4.2, Finanssialan keskusliitto 2011)

3.3 Ostotapahtuma

Ostotapahtuman aikana tiedot ovat ensisijaisesti luettava sirulta kun käytössä on sirukortti. Kortin omistaja asettaa sirukortin ensin maksupäätteen lukijaan, jonka jälkeen tarkistaa maksettavan summan. Seuraavaksi kortinhaltija valitsee maksutavan, mikäli pääte sitä kysyy. Lopuksi kortinhaltija vahvistaa maksutapahtuman näppäilemällä henkilökohtaisen tunnuslukunsa (PIN). Allekirjoitus ja henkilöllisyyden tarkastaminen vastaavat tunnusluvun käyttöä, joten edellä mainitut eivät ole tunnuslukua käyttäessä tarpeellisia. Korttimaksusta tulostetaan asiakkaalle kuitti. (EMV-Maksupäätejärjestelmän toiminnallinen kuvaus V4.2, Finanssialan keskusliitto 2011)

Silloin kun maksetaan siruttomalla magneettijuovakortilla, pitää kortti lukea magneettijuovalukijassa. Allekirjoittamalla kuitin kortinhaltija hyväksyy maksun ja samalla todentaa allekirjoituksella olevansa kortin omistaja. Henkilöllisyyden tarkastus tehdään tilanteen niin vaatiessa. (EMV-Maksupäätejärjestelmän toiminnallinen kuvaus V4.2, Finanssialan keskusliitto 2011)

Maksunsaajan tulee säilyttää pankkikorttitapahtumien maksutietoja ja tositteita 18 kuukauden ajan. Tositteiden säilytys ja tuhoaminen pitää suorittaa standardien mukaisesti, että tietoa ei pääse vuotamaan ulkopuolisille(EMV-Maksupäätejärjestelmän toiminnallinen kuvaus V4.2, Finanssialan keskusliitto 2011)

3.4 Varmennus

EMV-järjestelmässä sirukortti pyytää maksupäätettä tekemään varmennuskyselyn. Se tapahtuu riskinhallintaparametrien avulla, jotka kortinantaja on asettanut. Maksupäätteiden varmennuksessa käytetään salattua TCP/IP-yhteyttä. Maksunsaajan on huolehdittava siitä, että varmennusyhteydet on ohjattu suorinta reittiä pankille. Maksunsaajan käyttäessä ulkopuolista palveluntarjoajaa tulee heidän sopia keskenään vastuunjaosta ja varmennusliikenteen toteutuksesta(EMV-Maksupäätejärjestelmän toiminnallinen kuvaus V4.2, Finanssialan keskusliitto 2011)

3.5 Tapahtumien välitys

Maksupäätteiden ja maksupäätejärjestelmien on oltava Finanssialan Keskusliiton valtuuttaman tahon sertifioimia. Maksunsaajan tulee vastata tapahtumien aineiston oikeellisuudesta, palautteen noutamisesta ja aineiston lähettämisestä. Pankilla on vastuu vastaanotetun aineiston käsittelystä, palautteen muodostamisesta sekä pankkikorttitapahtumien hyvityksestä. Pankit suosittelevat että tapahtumat tulisi lähettää kerran vuorokaudessa. Jos tiedot lähetetään ajastetusti, olisi ne hyvä lähettää muina kuin tasatunteina tiedonsiirtoruuhkien tasoittamiseksi. Pankit vastaanottavat tapahtumia 24 tuntia vuorokaudessa jokaisena viikonpäivänä. Pankkikorttitapahtumat on lähetettävä 20 päivän sisällä tapahtuneesta. Maksupäätejärjestelmä tuottaa raportin lähetetyistä tapahtumista, joka maksunsaajan on tarkastettava(EMV-Maksupäätejärjestelmän toiminnallinen kuvaus V4.2, Finanssialan keskusliitto 2011)

3.6 Turvallisuus

Kaikkien maksunsaajien, jotka hyväksyvät korttitapahtumia, tulee noudattaa kansainvälisiä PCI-standardeja. Finanssialan Keskusliitto, Luottokunta ja Suomen Kaupan Liitto ovat laatineet yhteistyössä suositukset siitä, miten maksupääte tulisi sijoittaa ja millä perusteilla ne tulisi valita. Maksupääte tulee sijoittaa siten, että tunnusluvun voi näppäillä muiden näkemättä tunnuslukua, joka laitteeseen syötetään. Maksupäätteet ovat siirrettävissä, jotta tunnusluvun syöttäminen on mahdollisimman turvallista. Lisäksi on otettava huomioon erityisryhmien tarpeet laitteiden sijoittelussa. Kassahenkilö voi opastaa asiakasta laitteen käytössä,

mutta tunnusluvun asiakkaan täytyy aina näppäillä itse. (EMV-Maksupäätejärjestelmän toiminnallinen kuvaus V4.2, Finanssialan keskusliitto 2011)

Tietoliikenteen on oltava salattu. Tapahtumien välitys tulee suojata Finanssialan Keskusliiton pankkiturvastandardin (PATU) määrittämällä tavalla. Kaikki pankkiaineistoja sisältävä tietoliikenne langattomissa ja julkisissa Internet-verkoissa pitää olla salakirjoitettua. Salauksen tulee olla vahvaa ja sen on ulotuttava siirtoyhteyden päästä päähän(EMV-Maksupäätejärjestelmän toiminnallinen kuvaus V4.2, Finanssialan keskusliitto 2011)

4 PCI-standardi

PCI-standardi on kansainvälisten maksukorttiyhtiöiden luoma standardi turvalliseen korttimaksamiseen. Kaikkien maksukorttitietoja vastaanottavien tahojen on noudatettava PCI:n määrityksiä. Standardin vaatimukset sisältävät yli 200 kohtaa, joita on noudatettava. Kohdeyrityksen projektissa on tähdätty siihen että kauppiaan vastuu pci:n osa-alueissa pienenee. Kun otetaan huomioon että maksupäätteen yhteys on päästä päähän salattu, eli järjestelmään ei tallennu maksukorttitietoja, jää PCI–standardista kauppiaan vastuulle 22 kohtaa. Seuraavaksi luetellaan kohdat PCI-standardista, jotka kohdeyrityksessä valitulla toimintatavalla kuuluvat yrityksen vastuisiin(Yrityksen sisäinen dokumentointi 2011):

Seuraavat PCI-standardin kohdat ovat alkuperäisessä standardissa kohdassa 3:

1. Pidä korttidatan talletus minimissä toteuttamalla datan säilytys- ja hävityspolitiikan menettelyt ja prosessit seuraavalla tavalla.

1.1 Luo datan säilytys- ja hävityskäytäntö seuraavanlaisesti

- Rajaa datan säilytyksen määrä ja säilytysaika maksimissaan siihen mikä tarvitaan oikeus, sääntely ja liiketoiminnan tarpeisiin
- Kuvaa prosessit tiedon turvalliseen poistamiseen kun ne eivät ole enää tarpeellisia
- Luo tarkat korttidatan säilytystä koskevat vaatimukset
- Suorita neljännesvuosittain automaattinen tai manuaalinen prosessi jolla tunnistetaan tiedot ja poistetaan ne turvallisesti, kun säilytyksen maksimi määräaika on tullut täyteen

2. Älä säilytä sensitiivistä todennusdataa vaikka se oli salattua. Sensitiivinen todennusdata sisältää tietoja mitä seuraavissa kohdissa 2.1-2.2 mainitaan. On sallittua säilyttää arkaluonteista tunnistustietoa, jos sille on liiketoiminnalliset perustelut ja se säilötään turvallisesti.

2.1 Ei tule säilyttää täydellisiä tietoja mistään kortin osasta(magneettiraita, korttinumero, siru tai muita). Normaalissa liiketoiminnassa seuraavat tiedot on joissain tapauksissa säilytettävä:

- Kortinhaltijan nimi
- Ensisijainen tilinumero (PAN)
- Viimeinen käyttöpäivä
- Palvelukoodi

Riskien minimoitumiseksi tulee tallentaa vain liiketoiminnan kannalta oleelliset elementit.

2.2 Ei tule säilyttää kortin varmistuskoodia tai arvoa

2.3 Ei tule säilyttää kortin henkilökohtaista tunnistuslukua (PIN) tai salattua PIN-lohkoa

Seuraavat PCI-standardin kohdat ovat alkuperäisessä standardissa kohdassa 12:

3. Laadi, julkaise, ylläpidä ja levitä turvallisuuspolitiikkaa jolla saavutetaan seuraavat:

3.1 Puututaan kaikkiin PCI-DSS vaatimuksiin

3.2 Sisältää vuosittaiset prosessit jotka tunnistavat uhat ja haavoittuvuudet, jotka johtavat viralliseen riskien arviointiin

3.3 Sisältää vuosittaisen katsauksen ja päivitykset ympäristön muuttuessa

4. Varmista että turvallisuuspolitiikka ja toimenpiteet selkeästi määrittelevät tietoturvallisuuden vastuualueet koko henkilöstölle

5. Nimitä seuraavat vastuut joko yksilölle tai ryhmälle:

5.1 Luo, dokumentoi ja jaa turvallisuuskäytännöt ja menettelyt

5.2 Luo, dokumentoi ja jaa turvallisuustapahtuman vastatoimi ja edelleen välittämisen toimenpiteet varmistaaksesi nopean ja tehokkaan käsittelyn kaikissa tilanteissa

6. Toteuta muodollinen tietoturvaohjelma, jossa henkilökunnalle painotetaan korttiturvallisuuden tärkeyttä

6.1 Kouluta henkilökunta työllistämisen yhteydessä ja vähintään kerran vuodessa. Huom. menetelmät voivat vaihdella riippuen henkilökunnan pääsyoikeuksista kortinhaltijoiden tietoihin.

6.2 Vaadi henkilökuntaa todistamaan vähintään kerran vuodessa, että he ovat lukeneet ja ymmärtäneet tietoturvaohjeistuksen turvallisuuspolitiikan ja käytännön

7. Jos kortinhaltijan tietoja jaetaan muun palveluntarjoajan kanssa ylläpidä ja toteuta palvelut, jotka koostuvat seuraavista asioista:

(Kauppiailla tulee olla sopimuslista palveluntarjoajista jotka käsittelevät korttidataa. Sopimusten tulee sisältää selkeästi PCI-vaatimusten noudattaminen)

7.1 Ylläpidä listaa palveluntarjoajista

7.2 Tee kirjallinen sopimus jossa tehdään selväksi, että palveluntarjoaja on vastuussa kortinhaltijan tietojen turvallisuudesta

7.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement

7.4 Ylläpidä ohjelmaa joka seuraa vähintään kerran vuodessa palveluntarjoajan PCI DSS noudattamistasoa

5 Kohdeyrityksen hanke

Maaliskuussa 2008 kohdeyrityksen konsernissa käynnistyi hanke, jonka tavoitteena on korttimaksamisen turvallisuuden parantaminen kohdeyrityksen kaupoissa. Hanketta johdetaan konsernitasoisesta hanketoimistosta, joka koordinoi ja tukee yhtiöiden omia projekteja (Yrityksen sisäinen dokumentointi, 2011).

Kohdeyrityksen hanke jakautuu seuraaviin alaprojekteihin:

- palvelun perustaminen
- käyttöönottoprojekti
- Siivousprojekti
- PCI–auditointiprojekti
- yhtiötasoiset projektit

Ensimmäisessä vaiheessa rakennettiin yhdessä valitun palveluntarjoajan kanssa turvallisen maksamisen palvelu. Toisessa vaiheessa otettiin käyttöön samanlaiset sirukortinlukijat kaikissa kohdeyrityksen kaupoissa. Tämä sisältää valitun palveluntarjoajan tarjoaman palvelun, joka kattaa PCI – standardin vaatimukset. Kolmas vaihe on siivousvaihe. Se pitää sisällään sensitiivisen maksukorttitietojen siivouksen kaikista kaupan järjestelmistä, sekä fyysisten korttidataa sisältävien dokumenttien ja varmenteiden siirtämisen kaupasta turvalliseen säilytyspaikkaan. Viimeisessä vaiheessa kun kaikki yhtiön/ketjun kaupat on siivottu sensitiivisestä datasta, suoritetaan PCI–auditointi.

5.1 Siivous- ja PCI-projekti

Keväällä 2010 kaikissa kohdeyrityksen Suomen ketjuissa tehdyn selvityksen mukaan kaikista kaupan järjestelmistä löytyi sensitiivistä maksukorttitietoa. PCI-sertifikaatin saaminen kohdeyrityksen korttimaksamiselle edellyttää niiden siivouksen. Kansainväliset korttiyhtiöt edellyttävät PCI:n mukaisuutta kaikilta niiltä yhtiöiltä, jotka käsittelevät maksukorttitietoja. Yritys on sitoutunut tähän allekirjoittamalla tilittäjän kanssa sopimuksen korttitietojen välittämisestä. Eräässä vuonna 2007 tehdyssä tutkimuksessa pohdittiin sitä, mitä hyötyä sisäisessä auditoinnissa saavutetaan ja miten tämä hyöty on mitattavissa, koska sisäinen auditointi vie aikaa ja resursseja(Merchants failing to meet PCI-standard, Alvarado, K 2007). PCI–sertifikaatilla tavoitellaan myös maksukorttitietojen välittäjien kilpailutusta korttimaksamisen kustannusten vähentämiseksi. Projektisuunnitelmassa keskeisiä toimenpiteitä olivat siivousprojekti, PCI-auditointi sekä vastuiden jako (Yrityksen sisäinen dokumentointi, 2011). Projektilla on myös huomattavat taloudelliset vaikutukset.

Siivous voidaan käynnistää kun kaikkiin kohdeyrityksen kauppoihin on asennettu uudet sirumaksupäätteet. Siivouksessa poistetaan kaikki sensitiivinen korttitieto järjestelmistä ja tarvittaessa tehdään uudet prosessit, jotta korttitietoa ei enää jatkossakaan kerry. Siivouksen yhteydessä tehdään PCI-esiauditointi, jossa todetaan että sensitiivistä korttidataa ei tarkastettavista kaupoista löydy. Tämän jälkeen voidaan siirtyä varsinaiseen PCI-auditointiin.

Siivous tulee tehdä siten, että ensimmäisestä PCI-auditoinnista saadaan hyväksyttävä tulos. Siivousprojektin yhteydessä hanketoimisto tukee yhtiöitä ja PCI-asiantuntijan käyttäminen apuna on suotavaa laadun takaamiseksi.

Järjestelmän siivouksen tekee kassajärjestelmän toimittaja. Tapa millä siivous tehdään vaikuttaa suoraan siihen miten paljon työtä ja kustannuksia PCI-auditoinnista tulee. Yhtiöiden vastuulla on tehdä kassajärjestelmän toimittajien kanssa sopimus ja huolehtia sopimusvelvoitteista siten, että siivoukset saadaan tehtyä kattavasti, laadukkaasti ja heti ensimmäisellä kerralla hyväksytysti.

Ennen varsinaista auditointia yhtiöt tekevät sovitulla tavalla dokumentin siivouksen hyväksymistestauksesta. Tämä dokumentointi toimii perustana PCI-esiauditoinnille ja lopulliselle PCI-auditoinnille. Testauksen hyväksymisen jälkeen siivous tehdään kaikissa kaupoissa. Jokaisen kaupan siivous dokumentoidaan erikseen siihen tarkoitukseen toimitettuun excel-dokumenttiin. Siivouksessa kaiken korttitiedon tulee ehdottomasti olla poistettu.

5.2 PCI-auditointi

Siivouksen jälkeen valittu PCI-auditoija suorittaa esiauditoinnin, jolla vahvistetaan että ketju on valmis varsinaiseen auditointiin. Jos PCI-auditoija löytää jotain huomautettavaa palataan takaisin edelliseen vaiheeseen. Jos kohdeyrityksen kaupoista vielä PCI-auditoinnin jälkeen löytyy sensitiivistä korttitietoa, ovat sanktiot siitä erittäin kalliit. Tässä tapauksessa kauppias vastaa tilittäjän sopimuksen mukaisesti sanktioiden maksamisesta.

5.3 Vastuut

PCI-projektin vastuut on jaettu kolmeen eri ryhmään, joita ovat konsernitaso, yhtiötaso ja kassajärjestelmän toimittaja. Konsernitason hanketoimiston vastuualueita ovat projektin tavoitteiden määrittäminen ja kommunikointi toimialayhtiöille. Lisäksi siihen sisältyy projektin ohjaus, joka sisältää mm. aikataulutuksen ja projektin seurannan. Näiden ohella konsernin vastuulle kuuluvat seuraavat asiat:

- siivouksen tavoitetilan ohjeistaminen ottaen huomioon PCI-vaatimukset
- sopimusten laadinnan tukeminen järjestelmätoimittajien ja toimialayhtiöiden välillä
- tuki PCI-asiantuntemuksen hankkimiselle yhtiöiden projektien avuksi
- tietoturvaohjeistuksen laatiminen
- tuki PCI-auditoinnissa

- projektin raportointi ohjausryhmälle ja konsernin johdolle

Yhtiötasoisen projektin vastuihin kuuluu yhtiön siivousprojektin läpivienti, sekä yhteistyö kassajärjestelmätoimittajien kanssa siivouksen osalta. Yhtiön tulee ohjeistaa järjestelmätoimittajille siivouksen tavoitetila.
Lisäksi yhtiön vastuihin kuuluvat seuraavat:

- testaus ja pilotointi sekä hyväksymistestauksen dokumentointi
- kassajärjestelmätoimittajien vastuiden määrittely sopimuksella
- siivouksen koordinointi
- PCI:n edellyttämien toimenpiteiden tekeminen ennen auditointia, kuten tietoturvaohjeistus sekä kuittien ja raporttien ohjeiden mukainen arkistointi
- resurssien nimeäminen PCI-auditointiin sekä auditoijan tukeminen
- raportointi projektin hanketoimistolle

Kassajärjestelmätoimittajien vastuulla ovat kassajärjestelmien siivoamisen teknisen ratkaisun määrittely ja kuvaus. Kassajärjestelmätoimittajan vastuulla on myös työmääräarvioiden laadinta. Lisäksi vastuualueina ovat:

- sopimusten laadinta ja hyväksyntä toimialayhtiöiden kanssa
- kassajärjestelmän ja servereiden varsinainen siivous
- sopimuksen mukaisten PCI-vaatimusten täyttyminen

Alla olevassa taulukossa havainnollistetaan kohdeyrityksen projektin tehtävät ja vastuut:

Tehtävä	Projektin PMO	Yhtiön IT	Yhtiön riskienhallinta	Liiketoiminta
Yleinen ohjeistus	V	O	O	O
Yhtiön siivous-ja PCI-projektin johtaminen	I	O	V	O
Yhtiön ohjeistus/IT-järjestelmät	I	V	O	I
Järjestelmien siivoukset	I	V	O	I
Varmistusmedioiden käsittely	I	V	O	I
Järjestelmien käyttäjähallinta	I	V	O	I
Paperisten dokumenttien arkis-toinnit/tuhoamiset	I	I	O	V
Yhtiön ohjeistus/liiketoiminnan prosessit	O	O	O	I
Kauppojen tietoturvaohjeistuksen päivittäminen	O	O	V	O
Kauppojen tietoturvakoulutuksen koordinointi ja valvonta	I	I	O	V
Nimetään henkilöt PCI-auditointiin	I	V	O	V
Sopimuksien päivittäminen PCI-vaatimuksilla	O	V	I	V

V=vastaa, O=osallistuu, I=informoidaan

Taulukko 2 Tehtävät ja vastuut
(Yrityksen sisäinen dokumentointi, 2011)

6 Case-tutkimus

Tässä luvussa esitellään tutkimuksen tavoitteet ja tutkimusmenetelmät. Haastattelujen kuvaus ja niiden toteutus käsitellään myös tässä luvussa. Lisäksi tässä luvussa tulee olemaan pohdintaa siitä, miten haastatteluista saa mahdollisimman monipuolisen, jotta tulosten pohdinnassa lopuksi saa paljon vertailtavaa.

6.1 Tavoitteet

Tämän työn yhteydessä suoritetaan case-tutkimus. Tutkimuksen tavoitteena on kerätä tietoa kauppojen toimintatavoista ennen ja jälkeen kohdeyrityksen projektin vaikutuksen. Tietoturvallisuuden kannalta tiedetään, että uusi maksupäätejärjestelmä tulee olemaan turvallisempi. Sen lisäksi selvitetään kaupan omasta näkökulmasta, kuinka paljon projekti on vaikuttanut kauppojen joka päiväseen työskentelyyn ja sitä, kuinka hyvin uudistettu tietoturvaohje on omaksuttu kaupassa.

6.2 Tutkimusmenetelmät

Case-tutkimuksessa tulee olemaan kvalitatiivinen haastattelu. Haastattelukohteena ovat projektissa mukana olleita kohdeyrityksen työntekijöitä, sekä eräs kauppias. Yrityksen haastateltavat ovat kaikki toimineet eri rooleissa projektin aikana. Haastattelulomake sisältää 12 kysymystä(liite1). Kysymykset pohjautuvat kaupan uudistettuihin tietoturvaohjeisiin. Tutkimusmenetelmänä käytetään case-tutkimusta, joka tehdään konstruktiivisella otteella. Konstruktiivinen tutkimusote tarkoittaa sitä, että pyritään ratkaisemaan aitoja reaalimaaliman ongelmia ja tätä kautta tuottamaan kontribuutioita sille tieteenalalle, jolla sitä sovelletaan(Kari Lukka, Konstruktiivinen tutkimusote, Metodix). Konstruktiivinen ote sopii tähän tutkimukseen hyvin, koska sen tavoitteena on luoda konkreettinen tuotos tai mahdollisesti suunnitelma, mittari tai malli. Kyse on uudenkaltaisen todellisuuden rakentamisesta erityisesti tutkimustiedon pohjalta.(Kehittämistyön menetelmät 2009, Ojasalo, Moilanen, Ritalahti)

6.3 Haastattelut

Kohdeyrityksen kaupan kauppiaalle ja konsernin henkilökunnalle suoritettava haastattelu tuo mukanaan paljon haasteita. Kehittävän tutkimustyön kannalta on tärkeää luoda hyvä pohja haastattelulle, jotta siitä saisi mahdollisimman paljon hyödyllistä informaatiota, jota myöhemmin tulosten analyysissa voidaan hyödyntää. Tässä kyseisessä case-tutkimuksessa ei ole ennalta todettu varsinaista ongelmaa ja sellaisen löytäminen kehittämistyön kannalta on oleellista ja samalla erittäin haasteellista. Konstruktiivisella tutkimusotteella toteutettu haas-

tattelu on tässä tapauksessa hyvä vaihtoehto. Konstruktiivisen tutkimuksen tavoitteena on saada käytännön ongelmaan uudenlainen ja teoreettisesti perusteltu ratkaisu, joka tuo liiketoimintaan ja myös tiedeyhteisöön uutta tietoa (Kehittämistyön menetelmät 2009, Ojasalo, Moilanen, Ritalahti). Tällainen lähestymistapa on melko haasteellinen. Tavoitteena on sitoa käytännön ongelma ja sen ratkaisu teoreettiseen tietoon.

Oikeiden henkilöiden haastattelulla on suuri merkitys. Haastattelemalla eri henkilöitä eri näkökulmista saadaan mahdollisimman kattava näkemys nykyisen toimintamallin toimivuudesta. Tämän tutkimuksen haastateltavina on yksi kauppias sekä yrityksen eri toimialojen projektiin liittyvää henkilökuntaa. Pääasiallinen tavoite on kuitenkin selvittää se, miten kohdeyrityksen projekti on muuttanut kaupan toimintaa ja miten tietoturva-asioita omaksutaan nykyään.

Oman haasteensa tuo se, että erilaiseen liiketoimintaan perustuvilla kaupoilla saattaa olla kuitenkin hyvin erilaisia ongelmia muutosten myötä. Haastattelu tulee olemaan puolistrukturoitu sekä avoin haastattelu. Puolistrukturoidulla tarkoitetaan sitä, että kysymykset on laadittu ennakkoon ennen haastattelua, mutta niiden järjestys saattaa vaihdella haastattelun aikana. Avoimella haastattelulla taas tarkoitetaan sitä, että haastateltavan ja haastattelijan vuorovaikutus on suurta ja heidän välilleen kehittyy yleistä keskustelua ongelmasta tai tutkimuksen aiheesta(Kehittämistyön menetelmät 2009, Ojasalo, Moilanen, Ritalahti). Tämän tyylinen haastattelu on erittäin käyttökelpoinen, koska tutkimuksen tavoitteena on tutkia projektin tuomien muutosten merkitystä osallistujille.

6.3.1 Kauppiaan haastattelu

Ensimmäisenä haastattelukohteena toimi tammikuun 2012 alussa eräs kohdeyrityksen liikenneasemista. Haastattelujen purku ei ole sanasta sanaan kirjoitettuna, vaan hieman muotoiltuna, jotta kriittisimmät salaista tietoa käsittelevät yksityiskohdat eivät tule julki tässä raportissa. Haastattelukysymykset ovat erikseen liitteenä raportin lopussa(liite1).

Uusi maksupäätejärjestelmä tuli käyttöön marraskuun 2011 lopussa eli haastatteluajankohtana se on ollut käytössä noin kaksi kuukautta. Kaupalla on ollut käytössä 20 vuotta vanha finbusin järjestelmä, joka poikkeaa hieman yrityksen maailmasta. Kyseinen järjestelmä oli käytössä polttoaineen rahastuksen takia. Se on käytössä kaikilla liikenneasemilla ympäri Suomen. Viime keväänä kaksi liikenneasemaa toimii uuden maksupäätejärjestelmän pilotteina ja syksyllä tuli kuusi lisää, joihin myös tutkimuksen kohteena oleva liikenneasema kuului. Kyseinen yksikkö on hieman poikkeuksellinen, koska sen toiminta on keskittynyt kahteen eri rakennukseen. Se tuo omat haasteensa projektiin.

Pankkikorttislippejä säilytetään lukitussa toimistossa kaupan puolella. Molemmissa rakennuksissa on isot kassakaapit, joissa säilytetään tavaraa ja muuta raportointiin liittyvää. Haastattelun ajankohtana kun kohdeyrityksen projektissa kauppa oli vielä siirtymävaiheessa, säilytettiin pankkikorttislippejä pääsääntöisesti noin kuukauden ajan lukitussa toimistossa, ennen kuin ne siirrettiin varastoon. Vanhan käytännön mukaan kyseisiä tositteita oli säilytettävä yhdeksän kuukauden ajan. Tästä johtuen ennen marraskuun järjestelmämuutosta tulleet tositteet ovat vielä tallessa. Vielä erikseen ulkona sijaitsevassa varastotilassa on erillinen arkistointikaappi asiakirjojen säilytystä varten. Näihin säilytystiloihin on pääsy vain kahdella henkilökunnan jäsenellä, kertoo kauppias.

Tähän mennessä vanhentuneita tositteita ei ole tuhottu ollenkaan. Haastateltava on ollut kaupassa kolme vuotta kauppiaana ja kaikki vanha data on vielä tallessa. Jatkossa käytäntö menee niin, että kauppaan tulee tietoturvasäiliö muutamaksi viikoksi, jonka jälkeen kaikki materiaali menee tuhottavaksi.

Sähköistä dataa kaupalla ei ole kovin paljoa. Tiedossa olevat datat ovat kopioitu levyille varmuuskopioina. Ketjulla on keskitetysti Fujitsun kassajärjestelmän data. Kaupan omat tiedostot ovat USB-tikulla ja cd-levyllä kassakaapissa. Tärkeimmät tiedot pyritään pitämään varmuuskopioina myös muualla. Hyvänä esimerkkinä siitä miksi säilyttää varmuuskopioita muuallakin kuin liikepaikalla on se, kun eräs yksikkö paloi sähkövian takia, sanoo kauppias. Liikenneasemat ovat usein vanhoja rakennuksia. Tässä tapauksessa toinen rakennuksista on 1970-luvulla rakennettu ja toinen 1980-luvulla.

Maksupäätteiden äärellä on aina joku henkilökunnasta paikalla. Sellaista tilannetta ei tule, jossa asiakas olisi yksin maksupäätteen äärellä. Mittarikentiltä on kuitenkin löydetty ylimääräisiä laitteita. Kauppias luottaa siihen, että murtohälytinjärjestelmä hälyttää aukioloaikojen ulkopuolella, jos kaupan sisällä sattuisi joku liikkumaan. ”Murtohälytyksen tapahtuessa laitteet tietysti tutkittaisiin”, sanoo kauppias. Kaupassa on myös hyvin kattava valvontakamerajärjestelmä, joka varmasti tallentaa kaiken tapahtuneen.

Monen tyyppistä huoltomiestä käy kaupalla ja se tekee ympäristöstä haastavan. Kauppiaan mukaan toimialoja on niin monta, että kaupalla käy noin 15 eri huoltomiestä. Toimintamalli on sellainen, että huolto sopii tulostaan kauppiaan kanssa erikseen. Paikalle saapuessaan huolto useimmiten ilmoittautuu ensin kaupan puolen henkilökunnalle ja sen jälkeen kauppiaalle. ”Toki senkin jälkeen heidän tarvitsee tulla meiltä hakemaan avaimet tai jonkun mukaansa”, kertoo kauppias. Siinä vaiheessa heidän täytyy näyttää henkilökortti. Kauppiaan sanoin jos on ennestään tuttu ja luotettava kaveri, niin voi olla että hänelle annetaan avain mukaan kierroksensa suorittamisen ajaksi. Jos ajatellaan kassapäätteitä turvallisuusriskinä, niin huoltomiehet eivät liiku niissä tiloissa vaan myymälän puolella ja varastotiloissa.

”Omien työntekijöiden perehdytys tietoturvaan varmistetaan netissä tehtävällä tietoturvapassilla. Sillä varmistetaan että kaikki ovat ajan tasalla tietoturvan suhteen ja kaikkien tietotaito muuttuvissa asioissa on päivitetty”, kertoo kauppias. Yrityksellä on hyvin pitkäaikaisia työsuhteita, eikä vaihtuvuus ole kovin suuri. Koulutus/perehdytys tapahtuu siinä vaiheessa kun henkilö tulee töihin.

Henkilökunnan valvontaa ei suoriteta johdonmukaisesti tai säännöllisesti vaan työsuhde perustuu luottamukseen, sanoo kauppias. Muutama luottohenkilö laskee kassoja tai käy tietokoneella. Kauppiaalla ei ole varmuutta siitä voiko kassakoneella surffata netissä. Teoriassa sen pitäisi olla estetty, mutta täysin varma ei kauppias asiasta ole. Netin käyttö työaikana on kielletty.

Seuraavaksi kysyttiin miten toimitaan jos asiakas tulee kertomaan, että häntä on veloitettu maksukortilla tehdystä ostoksesta kahteen kertaan? Tällä hetkellä kauppias ei osaa sanoa, koska vastaavaa tilannetta ei ole vielä tullut vastaan uudella maksupäätejärjestelmällä. Kaikki maksuliikenne liikkui polttoaineveloitusjärjestelmän kautta. Kauppiaan mukaan toiminta oli tuolloin hyvin selkeä. Virhetilanteessa otettiin polttoaineveloitusjärjestelmän toimittajaan yhteyttä ja he tarkistivat maksutapahtuman. Uudessa kassajärjestelmässä on se hyvä puoli, että kauppa pääsee itse käsiksi kuittiarkistoon. Tapahtumat löytyvät siis omalta kassapalvelimelta. Tuplaveloitukset paljastuvat heti, koska se näkyy kontrollinauhalta ja on korjattavissa heti.

Kulkuoikeudet kaupassa perustuvat avaintenhallintaan, koska heillä ei ole sähköistä kulunvalvontajärjestelmää. Ainoastaan luottohenkilöillä on yleisavain, jolla on pääsy kaikkiin tiloihin. Luottohenkilöitä on pari työntekijää per talo. Avaimista pidetään listaa, jotta tiedetään mitkä avaimet ovat kullakin työntekijällä käytössä. ”Tietenkin niin kuin kulkuoikeuksiin ja kassakaappien koodeihin kaikilla on oma henkilökohtainen koodinsa”, sanoo kauppias. Sama pätee myös hälytysjärjestelmään, johon jokainen kirjautuu omalla koodillaan. Kaikista koodeista on olemassa lista, jotta tarvittaessa voidaan selvittää kuka on tapahtuman sattuessa ollut kyseessä ja käyttänyt koodiaan.

Tässä vaiheessa ei vielä kauppiaan mukaan voi sanoa onko nykyisissä tietoturvaohjeissa jotain puutteita. Kohdeyrityksen projektin myötä tulevat muutokset ovat vielä pääosin edessäpäin. Kauppiaan mukaan heidän tiloissaan voisi olla muun kaltaisia säilytysratkaisuja kuin tällä hetkellä. Tilat ovat kuitenkin pienet ja ahtaat. Kassajärjestelmän vaihtuessa vanha palvelin jäi, jossa on vielä kaikki vanha data. Kauppiaan ongelmana onkin se, mitä tehdä vanhalle pc:lle, jossa on vielä kaikki data, jota tullaan tarvitsemaan.

6.3.2 Kohdeyrityksen ketjun projektipäällikön haastattelu

Toinen haastattelu tehtiin kohdeyrityksen henkilölle, joka vastaa erään ketjun kauppojen projektiin siirtymisestä ja valmiudesta pci-auditointiin. Ketjun kaupat ovat valmistautumassa audiointiin ja haastateltava on viime päivinä kierrellyt kauppoja läpi tarkastaen tilannetta. Haastateltavan tehtävänä on neuvoa kauppoja siitä, miten asiat tulee olla.

Korttinumeroita löytyy vielä kassajärjestelmän vanhoista pankkikortin hyväksymiskuiteista. Niitä kauppojen tulee säilyttää 18 kuukautta. Yleensä niitä säilytetään lukitussa toimistossa, jonka jälkeen ne lähetetään tuhottavaksi. Niitä myös saatetaan säilyttää lukitussa toimistossa noin kaksi kuukautta, jonka jälkeen ne siirretään lukittuun arkistoon, jossa säilytetään kaikki muu data, kertoo haastateltava. Yleinen tapa on ollut niin, että kaupoilla on nopea pääsy pieneen määrään arkistodataa ja loput ovat vähän kauempana. Luottokunnan ohje näihin on 18 kuukautta ja sen mukaan kauppoja on ohjeistettu. Arkistoitavista tositteista vanhoja kontrollinauhoja on selkeästi eniten. Ennen sitä kun tuli sähköinen kuittiarkisto vuonna 2009, oli kuittitulostin joka tulosti kaksinkertaisen kuitin. Toisesta jäi kontrollinauha kauppaan. Ohjeistus tämän kirjanpitoaineiston säilyttämiseen on kuusi vuotta. Niitä löytyy arkistolaatikoista ja jätesäkeistä, mutta ne ovat lukitussa arkistohuoneessa, kertoo haastateltava. Haastateltavan mukaan osa kaupoista on jo tuhonnut säilytettyjä kontrollinauhoja projektin myötä. Toisaalla niitä vielä säilytetään lukitussa arkistossa, jonne on pääsy vain kauppiaalla ja talouspäälliköllä.

Projektin ohjeistuksen myötä kaupoilla on arkistohuoneen seinällä selkeä lista tositteita sisältävistä jätesäkeistä ja siitä minä vuonna ne tulee tuhota, kertoi haastateltava. Viime aikoina haastateltavan käydessä kaupoissa tarkastamassa tilannetta, on kaupoista löytynyt selkeä arkistopöytäkirja, kuten on ohjeistettu. Verotarkastuksessa pyydetään näyttämään kirjanpitotositteita, joita lain mukaan tulee säilyttää kuusi vuotta. Nykyään näitä tositteita menee sähköiseen arkistoon eikä niitä kerry kauppaan.

Projekti tuli kohdeyrityksen kyseisen ketjun kauppoihin vuonna 2010 ja sen jälkeen ei ole enää tullut tositteita, joissa olisi ollut maksukorttinumeroita. Pankkikorttitositteita tulee säilyttää 18 kuukautta ja näin ollen syksyllä 2012 tuhotaan viimeiset tositteet kaupoista. Haastateltavalla on mappi, jossa on jokaisen kaupan lähettämä raportti siitä mitä tuhottaville tositteille on tehty tai tullaan tekemään. Raporteissa mainitaan myös se, miten tositteita säilytetään, jotta ne ovat varmasti pci-ohjeiden mukaisia. Aikataulun mukaan kesällä myönnetään ketjulle pci-sertifikaatti, jos auditoinnit kaupoissa menevät läpi. Kaksi kauppaa on jo pääkaupunkiseudulta käyty läpi auditoijan kanssa.

Kaupan järjestelmässä ei ole kassapalvelinta. Uusi järjestelmä joka on vasta tulossa kauppoihin omaa kassapalvelimen. Suomessa on yksi tällainen kauppa, johon palvelin on sijoitettu ja palvelin on lukkojen takana tiloissa jonne ulkopuolisilla ei ole pääsyä. Tiloihin pääsy on vain henkilökunnalla. Palvelimelle ei kuitenkaan päädy maksukorttitietoa uuden maksupäätejärjestelmän myötä.

Maksupäätteiden tarkkailuun liittyen kaupoille on ohjeistus siitä, miten päätteitä tulee tarkkailla. Kassavastaavan pitää päivittäin kiertää kassapäätteet ylimääräisten laitteiden varalta, kertoo haastateltava. Ohjeistuksen mukaan poikkeustilanteessa on otettava välittömästi yhteyttä esimieheen, jonka jälkeen tämä ottaa yhteyttä ketjun riskienhallintaan. Tämän kaltaisia tapauksia ei ole tullut tietoon, mutta haastateltavan mukaan monenlaista yritystä on ollut missä tuntematon henkilö on esittäytynyt maksupäätteiden huoltajana, jotta pääsisi käsiksi laitteisiin. Suomessa on tapahtunut muutama murto kauppoihin, joissa mitään ei ole havaittu vietävän. Tällaisessa tapauksessa tutkitaan voisiko syynä olla maksupäätteiden väärinkäyttö. Todisteita tästä ei Suomessa ole löydetty.

Ketjulla on yksi huoltoliike, joka hoitaa kaupan kaikki laitteet. Vuosien varrella nämä huoltomiehet ovat tulleet henkilökunnalle hyvin tutuiksi, sanoo haastateltava. Ohjeistus siitä mitä tulisi tehdä, jos huoltomies tulee kauppaan, menee niin, että aina tulee tarkastaa huoltomiehen henkilöllisyys. Huoltomiehet saapuvat kauppaan aina työmääräyksen kanssa, josta näkee mitä hän on tulossa tekemään. Huoltomiehillä on henkilökortit aina mukana ja huoltokeikan päätteeksi heidän tulee aina ilmoittautua kaupan henkilökunnalle, että työtehtävä on suoritettu.

Tietoturvapassiin sisältyy sähköinen koulutus, joka jokaisen kaupan henkilökunnasta tulee suorittaa. Tällä hetkellä haastateltavan mukaan tilanne on se, että lähes kaikki ovat suorittaneet sen. Tietoturvapassissa käsitellään hyvin yleistä tietoturvaa ja korttitietojen käsittelyä. ”Siinä on nimenomaan lähdetty liikkeelle pci:n vaatimuksista”, kertoo haastateltava. Kaikki muu kouluttamiseen ja tietoturvaan liittyvä ohjeistus löytyy kauppojen intranetistä.

Henkilökunnan toiminnan valvonta vaihtelee kaupoittain hyvin paljon. Pieni kauppa saattaa sisältää kolme työntekijää, joista kaikki ovat perheenjäseniä ja tällaisessa tapauksessa oman henkilökunnan valvonta on varmasti vähäistä, kertoo haastateltava. Isommissa kaupoissa on kassavastaavat, jotka valvovat kassojen toimintaa. Haastateltava epäili, että suurempi riski oman henkilökunnan suhteen on rahan varastaminen kuin korttitietojen varastaminen. Suurimmassa osassa kaupoissa on varmasti normaalia kaupan sisäistä omavalvontaa. Maksupäätejärjestelmän uusiminen ei ole vaikuttanut henkilökunnan omavalvontaan, vaan samat säännöt pätevät kuin ennenkin, sanoo haastateltava.

Miten toimia jos asiakkaalla tulee maksukortilla tuplaveloitus? Oheistuksen mukaan ensin tulee tutkia sitä, onko saman päivän aikana ollut enemmän heittoa. Jos tilille on jäänyt varauksia roikkumaan, niin siinä tapauksessa pitää ottaa yhteyttä tilittäjään. Puhelimen välityksellä ei kuitenkaan saa kertoa kokonaisia korttinumeroita vaan selvitystä yritetään tehdä korttinumeron loppuosan perusteella. Korttinumeroita ei saa myöskään kirjata ylös mihinkään. Virheenselvitys on ehkä projektin myötä vaikeutunut juuri sen takia, että korttinumeroita ei ole edes missään järjestelmässä kokonaisena. Haastattelijan mukaan maksupäätejärjestelmän muuttuminen ei ole kuitenkaan vaikuttanut suurella tavalla kauppojen toimintaan virheenselvityksessä.

Kulkuoikeuksien määrittely riippuu hyvin paljon kaupan koosta. Kaupoissa henkilökunta pääsee lähes kaikkiin tiloihin. Poikkeuksena ainoastaan arkistohuoneet joihin on tiukempi pääsy. Haastateltavan mukaan arkistohuoneisiin on avaimet noin kahdella tai kolmella kaupan henkilöllä. Kaupalla on avaintenhallintalistat, josta näkee kenellä on pääsy tiettyyn tilaan. Jos kaupassa ei ole varsinaista arkistohuonetta, vaan tositteita säilytetään toimistossa, niin ohjeistuksen mukaan tositteet tulee säilyttää lukitussa kaapissa, jonne on pääsy vain muutamalla henkilöllä. Isojen ja pienten kauppojen tiloissa on hyvin paljon vaihtelua. Ydinasiana on se, että aina tulee olla rajattu pääsy korttinumerotietoihin.

Haastateltavan mukaan ohjeistusta tietoturvasta on kaupoissa riittävästi. Konsernin tehtävänä on ohjeistaa kaupoille tietoturva-asioista, mutta se miten kaupat niitä seuraavat jäävät myös hieman niiden vastuulle. Haastateltavan mukaan niissä kaupoissa, joissa he ovat käyneet, ovat asiat olleet hyvällä mallilla ja tietoturvatietoisuus ollut hyvää.

Haastateltava muistelee sitä kun projektiin lähdettiin ja sirumaksupäätteitä ei ollut vielä asennettu, niin muutos tulisi olemaan hyvin radikaali. Vaikutus oli kuitenkin paljon pienempi mitä aluksi luultiin, kertoo haastateltava. ”Ennakkoon pelättiin että asiakkaat eivät osaa käyttää uutta sirumaksupäätettä tai että myyjät eivät osaa”, sanoo haastateltava. Suurimpana haasteena nähtiin se, että uudessa maksupäätteessä asiakas lukee itse oman bonuskorttinsa. Haastateltavan mukaan joillekin ihmisille se tuntuu olevan vaikeaa. Se nähtiin ongelmana ja siihen reagoitiin jo vuosi sitten ja mietittiin mitä asialle tulisi tehdä. Ratkaisuna on se, että jatkossa voidaan käyttää etäluettavaa bonuskorttia, joten magneettijuovan lukemisessa aiheutuneista ongelmista ei tulisi niin paljon haittaa. Etälukija on kaikissa laitteissa valmiiksi, joten uudelleenasennusta ei tarvita.

6.3.3 Konsernin tietohallinnon palvelupäällikön haastattelu (jatkuva palvelu)

Jatkuvan palvelun yksikön tehtävä on vastata siitä, miten tämä kaikki toimii myös projektin jälkeen. PCI:n näkökulmasta ajatellen itse projekti tekee sen, että ensimmäiset sertifioinnit saadaan aikaan. Tämä prosessi toistuu vuosittain ja heille jää sen ylläpitäminen, kertoo haastateltava. Samat toimenpiteet toistetaan vuosittain. Henkilökunta tulee vuosittain kouluttaa edelleen. Vastuullamme on tehdä uudet koulutukset kauppoihin, sanoo haastateltava. Lyhyesti sanottuna projektin saavuttama tilanne on säilyttävä.

Millä laajuudella jatkossa suoritetaan auditointeja kun kauppoja on kuitenkin niin suuri määrä? Auditoija päättää sen kuinka laajalti auditoinnit suoritetaan. Haastateltavan mukaan auditoijat tarkastavat yksiköiden muutoslokin ja muita dokumentaatioita, joista he katsovat mitä on tehty viime auditoinnin jälkeen. Jos raportoinnit näyttävät järkevältä, ottavat auditoijat luultavasti pienemmän otoksen ja käyvät katsomassa, ovatko asiat oikeasti niin hyvällä mallilla kuin paperilla näyttää, kertoo haastateltava. Jos auditoijan mielestä kirjallinen osuus ei ole kunnossa, on syytä epäillä että tuskin kaupoissakaan on kaikki kunnossa. Tässä tapauksessa auditoijat tekevät isomman otoksen.

Haastateltavan mukaan tarkoituksena on kuitenkin se, että kaupoille tehdään sisäinen auditointi vuosikierron puolessa välissä noin 6-8 kuukauden paikkeilla. Tällä katsotaan että kaikki on kunnossa ja jos huomataan jotain epäkohtia, tehdään niihin korjaustoimenpiteitä. Jos jossain ketjussa huomataan epäkohta auditoinnissa, tullaan tarkastamaan se, että sama virhe ei toistu muissa ketjuissa. Tällä voidaan taata se, että auditointi menee sujuvasti kaikkialla. Tämän jälkeen vasta kun korjaustoimenpiteet on tehty, kutsutaan auditoija paikalle. Auditointikin maksaa, joten hyvä valmistautuminen on tarpeen, jotta se menee läpi sujuvammin ja nopeammin, kertoo haastateltava. Haastateltavan mukaan jatkuvassa palvelussa voidaan myös käyttää tämän opinnäytetyön kysymyslistaa siinä, kun vuoden kuluttua seuraa taas uusi auditointi.

PCI-vaatimuksiin kuuluu se että auditointiin mentäessä tulee henkilökunnalla olla tietoturvakoulutus suoritettuna. Seuraava tietoturvakoulutus ja siihen liittyvä tietoturvapassi tulevat ensi vuoden alussa. Vähän päivitetään tietoturvapassia ja ohjeita, sanoo haastateltava. Maksaminen kehittyy jatkuvasti, joten uudistettuun koulutukseen tullaan lisäämään ajankohtaisia teemoja, jotta koulutus ei vuodesta toiseen ole täysin sama. Koulutuksessa käydään tietoturvaa laajemmin eikä se keskity vain PCI:n näkemykseen. Haastateltavan mukaan se on myös osa heidän vastuuta, että tämä prosessi pyörii. Uusi koulutus tehdään yhteistyössä tarvittavien tahojen kanssa, jonka jälkeen viedään se suoritettavaksi.

Jatkuvuuden ylläpitämisessä keskeinen haaste on se, että kun projekti on noussut korkealle tasolle ja siinä on ollut tarvittavat resurssit ja muut olennaiset asiat, niin tässä saattaa tulla valitettava väärinkäsitys siitä, että kaikki on valmista eikä mitään tarvitse enää tehdä. Asia on kuitenkin päinvastoin. Projektin lopputulosten ylläpitäminen itsessään vaatii jatkuvaa työskentelyä ja kehittämistä. Sitäkin riskiä on pyritty ehkäisemään sillä, että aiheesta puhutaan jatkuvana toimintona.

Toisena haasteena haastateltava näkee sen, että vuosittaisessa prosessissa ei ole yhtä ainutta, vaan kymmenen eri prosessia jotka vaativat tekijänsä. Pelkästään hallinnollinen työ vaatii paljon tekemistä. PCI-standardikin saattaa muuttua ja jos se muuttuu kovin merkittävällä tavalla kauppojen kannalta, niin yllättävien muutosten vienti käytäntöön saattaa olla erittäin työlästä. ”Siihen olemme varautuneet sillä tavalla, että olemme PCI-councilin jäseniä ja kuulemme mahdollisista muutoksista ajoissa ja voimme omalta osaltamme koittaa järkeistää niitä”, kertoo haastateltava. Haastateltavan mukaan riski jatkuvuuden kannalta on se, että tätä aletaan nähdä outona kustannuksena, jota leikataan niin alas kunnes huomataan, että jokin tietty asia on jäänyt tekemättä.

Toimialat ottavat heidän kaupoille aiheutuvan kustannuksen, eli pääasiassa kaikki auditointikulut mitä kaupassa tehdään. Projektin myötä suurimmat kustannukset tulevat toimialalle, eikä suoraan kaupoille. Kaupoille kustannukset pääasiassa tulevat niihin asennetuista maksupäätteistä.

Siivouksen aikana kaupoista hävitettyä arkistomateriaalia on ollut hyvin suuret määrät. Joissain kaupoissa on haastateltavan mukaan tehty niin, että siivousta on keskitetty johonkin tiettyyn paikkaan, jossa on ollut hieman laajempi arkisto sen jälkeen. Ulkoiselta toimittajalta tulee raportit, jossa näkyy tuhottavaksi viedyn tavaran määrä kilogrammoina. Määrät ovat paikoitellen hyvin suuria. Siivouksessa ei niinkään seurata mitä tositteita kaupat lähettävät tuhottavaksi, vaan on myös hyvin mahdollista että tuhottavaksi on viety muutakin kuin vain PCI-standardiin liittyvää tietoturvamateriaalia. Siivouksen myötä joihinkin kauppoihin on vapautunut suuri määrä ylimääräistä tilaa, jota voi jatkossa käyttää hyödyksi.

Jatkossa arkistoitavaksi tulee kirjanpitomateriaalia, joissa ei ole enää korttinumeroita. Niillä on kuitenkin tietty säilytysaika ja ne tulee merkata hyvin. Kaupoilla on käytössä arkistointipöytäkirjat, joissa tulee näkyä koska aineiston voi viedä tuhottavaksi. Erilliset kirjanpitovaatimukset määrittelevät tositteiden säilytysajan. Haastateltavan mukaan ennen kohdeyrityksen projektia vastaavanlaisia hyvin yksityiskohtaisia arkistointipöytäkirjoja ei kovin laajalti ainakaan ole ollut. Kokonaisuutena ajatellen on tapahtunut siis huomattavaa parannusta. ”Esiauditointia ja selvitystä tehtäessä löysimme muutaman varastointimallin, joka ei ollut kovin turvallinen”, kertoo haastateltava.

Siivousprojekti on tällä hetkellä lähes valmis haastateltavan mukaan. Auditointeja tehdään jo kauppoihin. Aikataulun mukaan lokakuun loppuun mennessä tulee auditointien olla valmiina. Osa alueista on jo valmiita ja siirtyneet projektin jatkuvaan palveluun. Tällä hetkellä eteneminen on paljon levollisemmassa vaiheessa kuin kolme kuukautta sitten. Haastateltavan mukaan aikataulussa on pysytty ja viimeinen sertifiointi tulee lokakuun lopulla.

6.3.4 Tietoturvapäällikön haastattelu

Seuraavana haastatteluvuorossa oli konsernin tietoturvapäällikkö. ”Meillä on ollut menossa PCI-projekti, jossa kaupoista poistetaan maksukorttitietoa”, kertoo haastateltava. Tietyistä syistä on kuitenkin säilytettävä joitakin paperisia tositteita esimerkiksi kuitteja, raportteja ja verottajaa varten jotain tietoja. Jos tositteessa ei ole maksukorttitietoja, niin PCI ei ota mitään kantaa sen säilytykseen.

Paperisten tositteiden säilytys on ohjeistettu niin, että ne säilytetään lukitussa tilassa. Tämä tarkoittaa lähinnä kaappia joka lukitaan, kertoo haastateltava. Tämä ei ole kuitenkaan vähimmäisvaatimus, vaan kauppojen on pidettävä arkistointipöytäkirjaa säilytettävistä tositteista. Pöytäkirjaan tulee merkitä kaikki arkistoinnin tapahtumat. Esimerkiksi pelkästään kun kaappi avataan, merkataan se pöytäkirjaan. Se on PCI:n vaatimus, että aina kaikki tapahtumat tilassa, missä on sensitiivistä korttitietoa, pitää aina kirjata ylös. Tietyistä veroteknisistä syistä tulee joitain tositteita säilyttää kuusi vuotta. Haastateltavan mukaan projekti on ollut heillä nyt kaksi vuotta, joten neljä vuotta pitää vielä säilyttää joitain tositteita. PCI:n vaatimus on se, että mitään materiaalia, missä näkyy korttinumeroita, ei saa arkistoida, ellei sen säilytykseen ole erityistä syytä. Säilytysvelvollisuuden loputtua tulee tositteet tuhota heti. Kerran vuodessa tehdään inventointi, jossa tarkastetaan mitä tositteita saa tuhota. Ketjuittain voi olla eri variaatioita. Jotkin ketjut ovat päättäneet poistaa kaiken tai siirtäneet materiaalia keskitettyyn kuittiarkistoon. Riskinä tässä on se, että tulee reklamaatio tai tilintarkastus ja kaikkia tositteita ei löydy enää.

Siinä vaiheessa kun inventointi koittaa ja vanhentuneet tositteet tulee tuhota, kaupoilla on keskitetty palvelu, jota kautta tositteet tuhotaan. Luonnollisesti nämäkin merkitään arkistointipöytäkirjaan. Koko prosessista raportoidaan aina materiaalin tuhoamiseen saakka, jotta ongelmatilanteissa pystytään selvittämään missä välissä ketju katkeaa jos niin pääsee käymään. Inventointi ja tuhoamiset tulee suorittaa kerran vuodessa.

Sähköisissä varmistusmedioissa pätee samat periaatteet kuin paperisissa tositteissa. Sähköisiä medioita pitää säilyttää paremmin, koska riski siitä että niitä hyväksikäytetään, on suuri. Nii-

tä on säilytettävä kassakaapissa. Kassakaappiin pitää olla avaintenhallinta. Siihen oikeus saa olla vain nimetyillä henkilöillä. Kassakaapissakin pidetään pöytäkirjaa.

Kassapalvelimen pitää olla lukitussa tilassa ja tilaan on pääsy vain nimetyillä henkilöillä. Kassapalvelimen käyttöoikeushallinnasta ei ole ohjeissa määritelty, kertoo haastateltava. Kauppa saa itse määritellä sen kenellä on käyttöoikeudet palvelimelle. PCI:n kannalta sillä ei ole merkitystä, koska kassapalvelimet ovat kohdeyrityksen projektin myötä puhdistettu.

Jokaisen kassalla toimivan työntekijän pitää käydä tietoturvapassin koulutus. Siellä on kohta jossa sanotaan, että kassahenkilön tulee tarkastaa kassaympäristö ylimääräisten laitteiden varalta, kertoo haastateltava. Ulkopuolisia kuten huoltomiehiä ei saa päästää maksupäätteiden äärelle ilman työmääräystä. Työmääräyksen lisäksi tulee tarkistaa huoltomiehen henkilöllisyys. Haastateltavan mukaan tästä on tullut palautetta, että kokeilijoita ilman erillistä työmääräystä on käännytetty tiukasti pois. Omat työntekijät perehdytetään tietoturvaan tietoturvapassin koulutuksella. Jokaisen kaupan henkilökunnasta tulee suorittaa tietoturvapassi. Tietoturvapassi tulee suorittaa kerran vuodessa.

Henkilökunnan toiminnan valvomista ei ole erikseen ohjeistettu. Koulutuksessa kerrotaan, että henkilökunnan toimintaa tulee seurata hyvien valvontaperiaatteiden mukaisesti. Kaikkia lakeja ja yksityisyydensuojaa on tärkeätä noudattaa. Haastateltavan mukaan kaupoissa noudatetaan normaalia esimiesvalvontaa, jossa opastetaan miten tulee asioita tehdä. On olemassa muutama asia mitä erikseen voidaan mainita. Kassahenkilöiden tulee käydä tietoturvapassin koulutus. Lisäksi kassahenkilöiden ei tule kirjoittaa korttinumeroita ylös erillisille papereille, eikä myöskään lähettää niitä esimerkiksi sähköpostilla eteenpäin. Koska järjestelmään ei jää enää maksukorttitietoa, voidaan tämä asia hoitaa työnohjausvalvonnallisilla asioilla, kertoo haastateltava.

Jos asiakkaalta on veloitettu maksukortilla tehty ostos kahteen kertaan, korttinumeroa ei saa ottaa ylös. Kuittinumeron mukaan tulee selvittää virheellinen maksu. Käytännössä maksuvirhe tulee selvittää muilla tiedoilla kuin luottokorttinumerolla. Tapahtuma pystytään tunnistamaan ilman kokonaista korttinumeroa. Esimerkiksi korttinumeron alku- tai loppuosa riittää maksutapahtuman tunnistukseen. Osalla ketjuista tapahtuman tarkistaminen menee käsitöiksi ja osalla tiedot ovat sähköisessä arkistossa.

Kaupan kulkuoikeudet on erikseen määritelty. Vaihtelevuutta on hyvin paljon jos verrataan muun muassa kauppojen kokoja. Pienissä kaupoissa on vähemmän tiloja ja henkilökuntaa, joten kulkuoikeuksien määrittämisessä on vähemmän mietittävää. Isoissa kaupoissa sen sijaan pitää selkeämmin määritellä kenellä on pääsy arkistoihin ja palvelintiloihin, sekä muihin lukit-

taviin tiloihin. Ohjeet kulkuoikeuksien valvonnasta on olemassa ja kaupat voivat soveltaa niitä myös itse. Kauppojen kokoerojen takia tätä ei pystytä ohjeistamaan yksiselitteisesti. Tietoturvaohjeista on saatu hyvää palautetta, kertoo haastateltava. Tietoturvapassi ei ole pelkästään PCI:n koulutusta, vaan siinä on myös paljon yleistä tietoturvaa koskevia asioita. Siitä saatu palaute on ollut positiivista, kertoo haastateltava. PCI-standardi päivittyy kolmen vuoden välein. Konsernin tekemät ohjeistukset tarkastetaan ja päivitetään vähintään vuosittain.

Ennen Tumaa ja tietoturvapassia kaupoilla oli hieman erilainen koulutus. Joillakin ei ollut minkäänlaista tietoturvakoulutusta. Esimerkiksi erään ketjun kaupoilla oli kyllä tietoturvaohje, mutta ei läpäisemistä vaativaa passia, sanoo haastateltava. Tietoturvaohjeissa käsiteltiin enimmäkseen yleistä tietoturvaa, esimerkiksi nettisurffailuun liittyvää ohjeistusta ja muuta yleistä. Samat asiat pätevät periaatteessa vieläkin.

Haastateltava on ollut PCI-projektissa mukana alusta asti ja turvalliseen maksamiseen keskittyvään projektiin liittynyt kesken kaiken. Tietoturvapäällikön mielestä projektin ratkaisu ja toteutus on ollut loistava.

Haastateltavalta kysyttiin siitä, minkä hän näkisi haastavimpana asiana näinkin isossa ja laajassa projektissa. Hänen mukaansa projekti vaatii erittäin paljon ohjeistamista, jotta saadaan asiat kerralla oikein. Haasteena hän näkee sen miten saada riittävän hyvät, mutta ei kuitenkaan liian yksityiskohtaiset ohjeistukset. Liian yksityiskohtaiset ohjeistukset eivät välttämättä toimi jokaisessa ympäristössä samalla tavalla. Ohjeistamisen vaikeus on ollut haastavaa meidän ympäristössämme, kertoo haastateltava. Kaupoissa on yhteensä 12 eri kassajärjestelmää, joten yhden ohjeet eivät päde toiseen.

Projekti vaatii valtavan määrän ihmisiä toteuttamaan sitä. Haastateltava pohtii sitä, onko projektissa tarpeeksi ihmisiä toteuttamassa sitä ja ovatko kaikki sitoutuneet omaan osaansa tarpeeksi hyvin. Tämä projekti on vaatinut paljon konsernin, ketjujen ja kauppojen ihmisiltä. Projektissa on siis erittäin suuri määrä ihmisiä joiden täytyy tehdä jotain. Projekti on siis riippuvainen siitä, miten motivoituneita eri osatekijät ovat. Kaupoille kuitenkin kaupanteko on se tärkein asia. Sen takia projektin jalkautuminen on ollut haastavaa, mutta se on pitänyt tehdä selväksi, että tämä projekti on asia joka on pakko tehdä. Haasteltava uskoo, että eri osapuolilla ymmärretään miksi tätä muutosta loppujen lopuksi tehdään ja on luottavainen että kaikkialla ymmärretään tämä asia ja koetaan se hyvänä. Välillä on syntynyt keskustelua tietyistä asioista ja siitä, onko se oikeasti relevanttia, kertoo haastateltava. Jälkikäteen kuitenkin on huomattu, että kun asia on kerralla tehty hyvin, voidaan sitä käyttää muualla hyväksi jälkikäteen. Yleisiä käytännön hyötyjäkin on tullut kaupoille, kun siivouksen ja kuittiarkiston tyhjen-

nyksen jälkeen on huomattu, että kauppaan on tullut niin sanotusti yksi ylimääräinen huone papereiden tuhoamisen jälkeen.

Projekti on vaatinut paljon erilaisia ohjeita. Ketjuittain ohjeet vaihtelevat, koska kaupat tekevät asioita eri tavalla. Konsernissa on tehty valmiiksi pohjia ohjeistuksille ja muulle materiaalille, esimerkiksi valmiita pohjia ympäristökuvauksen tekemiselle, projektisuunnitelmalle tai verkkokuvaukselle.

Projektista on paljon hyötyä. Kustannuksia tulee paljon, mutta projektin mukana tulee paljon toiminnallista hyötyä. Tietoturvallisuus on lisääntynyt merkittävästi. Haastateltava sanoo, että niin kauan kun pysymme poissa otsikoista, olemme onnistuneet. Olemme profiloituneet vastuullisena toimittajana ja tämä tarkoittaa sitä, että jos asiakas antaa korttitietonsa meille, pidämme siitä myös huolta, kertoo haastateltava.

6.3.5 Hankejohtajan haastattelu

Konserni on toimittanut ohjeistuksen siitä miten paperisia tositteita tulee säilyttää. Ohjeistus käydään läpi myös tietoturvapassissa, jonka teko on pakollinen kaikille kaupan työntekijöille, jotka työskentelevät kassalla. Ne paperiset tositteet jotka eivät ole kirjanpitoaineistoa, eikä sisällä maksukorttitietoa tulee kaikki tuhota. Tuhoamisohjeet on määritelty ja kaupat tilaavat samalta toimittajalta tuhottavien aineistojen keräyksen. Konsernin kautta on siis ohjeistettu kaikki, kertoo haastateltava. Konserni on selvittänyt yhdessä tilintarkastajan sekä luottokunnan kanssa sen, mitä kaikkea tulee säilyttää.

Tuhoamisyhtiön kanssa on tehty keskitetty sopimus joka noudattaa PCI:tä. Kaupat raportoivat vanhan datan tuhoamisesta keskitetysti yhtiön hallintaan konserniin. Raportista näkee kuinka paljon hävitettävää tavaraa kaupalta on haettu ja se merkitään kilogrammoissa. Haastattelijan tutkiessa listaa, jossa näkyi hävitetyn tavaran määrä, siinä näkyi mm. eräs kauppa, josta on viety yli 6000kg tuhottavaa materiaalia. Tämä kertoo siitä kuinka paljon ylimääräistä tavaraa kaupoilla on säilössä, joka projektin myötä poistetaan. Hyötynä tässä on se, että tulee lisää tilaa kauppoihin. Konsernin puolelta on tehty sopimus ja ohjeistus, sekä prosessi on määritelty. Tämä palvelu täyttää pci:n vaatimukset. Sopimuksessa täytyy olla pci-lauseke.

Varmistusnauhoista ja muista sähköisistä medioista on ohjeistus. Mitään turhaa ei saa säilyttää. Jos tieto on sähköisesti, on se arkaluontoisempaa kuin paperilla oleva. Sähköisiä medioita ei tarvitse säilyttää, jos ne eivät ole kirjanpitolain mukaista materiaalia. Jokaisen median kohdalla pitää miettiä tapauskohtaisesti mitä se on. Verottajaa varten saattaa olla sähköisiä medioita, joita pitää säilyttää.

Tietoturvapassissa on ohjeet miten maksupäätteitä tulee tarkkailla. Huoltomiesten kohdalla on ohjeistettu niin, että henkilöllisyys on aina selvitettävä kun huoltomies tulee kauppaan. Jokaisen kassalla työskentelevän on käytävä tietoturvapassiin liittyvä koulutus. Sama koulutus on ulkopuolisille kaupan työntekijöille, joilla on myös oltava voimassa oleva tietoturvapassi tullessaan kauppaan työskentelemään. Kulkuoikeuksiin kaupan tiloissa on olemassa tiukat säännöt. Jos jossain varastossa on sensitiivistä korttidataa, niin sen täytyy olla lukitussa tilassa ja avaintenhallinnasta tulee olla selkeä raportointi.

Suurin konkreettinen hyöty kaupoille, joka on tullut projektin myötä, on se, että kauppoihin on tullut suuri määrä ylimääräistä tilaa hävitettyjen tositteiden myötä. Toinen hyöty on se, että henkilökunta on suorittanut tietoturvapassin ja pci-auditointi on tulossa ja tietoturvaan kiinnitetään sen takia tavallista enemmän huomiota. Esimerkiksi huoltomiehet eivät enää pääse kauppaan niin helposti ohjeiden tiukennuttua. Kaupoille on lähetetty selkeä viesti, että korttirikollisuus on yleistynyt ja sitä myötä myös tietoturvan tärkeyttä tuodaan kauppojen tietoisuuteen enemmän. Rikollisuuden mahdollisuus saa kaupan henkilökunnankin suhtautumaan eri tavalla tietoturvaan kuin aikaisemmin.

Projekti on konsernille ollut erittäin suuren työn takana. Projektiin ei pelkästään kuulunut sirumaksupäätteiden asennus vaan myös maksamisen infrastruktuuri on tuotu kauppoihin. Uusi maksupääte on eristetty muista järjestelmistä, jotta sinne ei kertyisi enää sensitiivistä korttidataa, kertoo haastateltava. Ennen projektin ratkaisun löytämistä on projektiryhmällä ollut monen vuoden esiselvitys. Kaupan verkon eristäminen maksupäätejärjestelmästä on vaatinut perusteellista selvitystä, joka on myös vienyt paljon aikaa. Tämän kaiken päälle vielä siivousprojektit ja pci-auditoinnit.

Koulutus on myös ollut suuri osa projektia. Haastateltavan mukaan konserni on kouluttanut noin 20 000 ihmistä projektin aikana. Toimialat vastaavat omien yhtiöidensä siivousprojekteista. Kaupat raportoivat siivouksesta ennen auditointia ja sen lisäksi kaikki auditoitavat kaupat käydään katsomassa toimialayhtiöiden toimesta. Auditoitavat kaupat valitaan pääosin dokumentoinnin perusteella. Tällä tarkoitetaan sitä, kuinka huolellisesti kaupat ovat täyttäneet siivousprojektiin liittyvät lomakkeet. Auditoija voi olettaa siivouksen olevan kunnossa, jos lomake on täytetty huolellisesti.

Suurin haaste projektissa on haastateltavan mukaan ollut se, että asia jota tehdään, on täysin uusi Suomessa, eikä ole mitään mistä ottaa mallia. Kaikki työ ja esiselvitys on jouduttu tekemään itse. Kaupat kuitenkin elävät omaa elämäänsä ja keskittyvät tekemään kauppaa. Konsernin on pitänyt tehdä selvitystä tilintarkastajan kanssa siitä, mitä aineistoa tulee säilyttää ja mitä ei.

7 Tulokset

Tässä luvussa käsitellään ja pohditaan haastattelujen tuloksia ja sisältöä. Haastattelurunkona käytettiin kysymyslomaketta(liite1), mutta sen lisäksi haastattelut olivat erittäin avoimia ja vuorovaikutuksellisia. Tulosten pohdinnan perusteella on tavoitteena tuoda ilmi se, mitä asioita kohdeyrityksen projekti on tuonut mukanaan ja millä tavalla se on vaikuttanut kauppojen toimintaan ja tietoturvaan. Tulosten pohdinnassa oman haasteensa tuo myös se, että haastattelut olivat suurelta osin avoimia, niin toistuvan konkreettisen teeman löytäminen voi olla haastavaa.

Haastattelut sujuivat pääosin hyvin. Tutkimuksen lähestymistapa muuttui hieman työn edetessä, koska haastattelujen saaminen kaupoista osoittautui haastavaksi. Se voidaan kuitenkin todeta hyvänä asiana, koska se kertoo sen, että kauppojen tietoturvatietoisuus on hyvällä mallilla. Haastatteluaiheen ollessa hyvin arkaluonteinen ja tietoturvakysymyksiin liittyvä, eivät kaikki kaupat olleet valmiita jakamaan tietoa haastattelujen muodossa. Tämä osoittaa sen, että projekti viimeistään on tehnyt kaupoille sen selväksi, että tietoturva on tärkeä asia ja siihen tulee panostaa kaupanteon ohessa.

Lopulta päädyin yhden kauppiashaastattelun lisäksi haastattelemaan kohdeyrityksen omaa henkilökuntaa. Jokainen haastateltavista on ollut mukana projektissa. Haastateltavina toimivat hankejohtaja, konsernin tietoturvapäällikkö, jatkuvan palvelun vastaaja, yhden ketjun projektipäällikkö, sekä erään liikenneaseman kauppias. Haastattelukohteet ovat kaikki eri tavalla mukana projektissa, mikä mahdollistaa sen, että haastattelutuloksetkin ovat mahdollisimman monipuolisesta näkökulmasta kuvattu.

7.1 Projektin ratkaisu

Projektin ratkaisun löytäminen on ollut hyvin pitkä prosessi. Projektiryhmä on tehnyt monen vuoden esiselvityksen löytääkseen oikeanlaisen ratkaisun. Tavoitteena oli eristää kaupan verkko maksupäätejärjestelmästä. Suurena haasteena olikin se, että asia jota tehtiin, oli täysin uusi Suomessa. Kaikki esiselvitykset ja tutkimukset oli siis tehtävä itse, koska ei ollut mitään mistä katsoa mallia. Tietoturvapäällikkö on erittäin tyytyväinen projektin ratkaisuun ja toteutukseen. ”Projektin ratkaisu ja toteutus on ollut loistava”, kertoo konsernin tietoturvapäällikkö.

Miksi sitten tehdä näinkin suuri projekti, jossa kustannukset ovat niin korkeat ja työmäärä suuri? Syynä on se, että korttirikollisuus on yleistynyt ja tietoturvallisuus on tärkeässä roolissa nykypäivänä. Kaupoille itse kaupanteko on tärkeintä, mutta se on pitänyt tehdä selväksi, että

tämä projekti on tärkeä ja se tulee tehdä kerralla hyvin. Projektin jalkautuminen on sen takia ollut vaikeaa. Konsernin tietoturvapäällikkö uskoo, että eri osapuolet kuitenkin ymmärtävät miksi tämä muutos tehtiin ja että se koetaan hyvänä. Projekti on vaatinut erittäin suuren määrän työntekijöitä sitä toteuttamaan. Haasteena on ollut se, ovatko kaikki sitoutuneet omaan osaansa tarpeeksi hyvin. ”Projekti on siis riippuvainen siitä, miten motivoituneita eri osatekijät ovat”, kertoo konsernin tietoturvapäällikkö.

7.2 Ohjeistus ja koulutus

Projekti on vaatinut paljon erilaisia ohjeita. ”Ketjuittain ohjeet vaihtelevat, koska kaupat tekevät asioita eri tavalla”, kertoo konsernin tietoturvapäällikkö. Konserni on tehnyt valmiita pohjia ohjeistuksille ja muulle materiaalille. Valmiita pohjia on tehty mm. verkkokuvaukselle, projektisuunnitelmalle ja ympäristökuvaukselle. Ohjeistusta tietoturvasta on kaupoissa riittävästi. Konsernin tehtävä on ohjeistaa kauppoja tietoturvasta, mutta sen miten kaupat niitä seuraavat, jäävät myös hieman kauppojen vastuulle.

Projektin ohjeistuksen myötä on yksi tärkeä asia, joka kuuluu kaikille ketjuille. Jokaisessa kaupassa jossa säilytetään pankkikorttidataa, tulee olla arkistointipöytäkirja. Pöytäkirjaan merkataan kaikki tapahtumat arkistohuoneessa. Se on PCI:n vaatimus, että kaikki tapahtumat tilassa missä on sensitiivistä korttitietoa, tulee aina kirjata ylös. PCI:n vaatimuksena on myös se, että mitään materiaalia, missä näkyy korttinumeroita, ei tule säilyttää ellei siihen ole erityistä syytä. Jos tositteessa ei ole maksukorttitietoja, niin PCI ei ota kantaa sen säilytykseen. Pöytäkirjassa tulee olla merkattuna tositteiden viimeinen säilytyspäivä, jonka jälkeen on suoritettava tositteiden tuhoaminen. Ennen projektia yksityiskohtaisia arkistointipöytäkirjoja ei kovin laajalti ollut. ”Esiauditointia ja selvitystä tehdessä löysimme muutaman varastointimallin, joka ei ollut kovin turvallinen” kertoo PCI:n jatkuvasta palvelusta vastaava taho.

Tietoturvakoulutus on laajentunut ja tullut pakolliseksi kauppoihin. Jokaisella kaupan henkilöllä tulee olla tietoturvakoulutus suoritettuna. Yksi merkittävimpiä henkilökunnan koulutukseen liittyvistä muutoksista on projektin myötä tullut tietoturvapassi. Jokaisen kaupassa työskentelevän henkilön tulee suorittaa tietoturvapassi ja siihen liittyvä koulutus. Tietoturvapassissa käsitellään yleistä tietoturvaa ja korttitietojen käsittelyä. Se pohjautuu pitkälti PCI:n vaatimuksiin. Ennen tietoturvapassia ja projektia kaupoilla oli erilainen koulutus. Joillakin ketjuilla ei ollut minkäänlaista koulutusta, mutta eräällä ketjulla oli kuitenkin tietoturvakoulutus, ilman läpäisemistä vaativaa passia. Aikaisemmin ohjeet pääasiassa painottuivat nettisurffailuun ja muuhun yleiseen tietoturvaan. Samat ohjeet toki pätevät yhä, mutta siihen on liitettynä lisäksi PCI:n vaatimukset. Koulutus on ollut suuri osa projektia. Hankejohtajan mukaan konserni on kouluttanut 20 000 ihmistä projektin aikana.

7.3 Tositteiden tuhoaminen

Vanhojen maksukorttitositteiden tuhoamisesta avautuukin kaupoille aivan uusi konkreettinen hyöty. Ennestään ahtaista tiloista on muodostunut entistä tilavammat tositteiden tuhoamisen jälkeen. Siivousprojektin myötä yksittäisestä kaupasta on viety tositteita tuhottavaksi jopa tuhansia kilogrammoja. Tämä kertoo siitä, kuinka paljon ylimääräistä tavaraa kaupoilla on säilössä. Siivouksen jälkeen monet kaupat ovat yllättyneet siitä, kun tositteiden hävityksen jälkeen heille on ilmestynyt uusi huone, jota voidaan jatkossa käyttää kaupan parhaaksi näkemäänsä tarkoitukseen.

7.4 Kulkuoikeudet

Uusien PCI-ohjeiden myötä huoltomiesten toiminta kaupoissa on tiukentunut. Ohjeet ovat kuitenkin selkeät. Huoltomies saapuu kauppaan aina työmääräyksen kanssa ja hänellä tulee olla henkilökortti, jota näyttää saapuessa. Haastateltavien mukaan kaupoissa on ollut jonkin verran yrityksiä, missä henkilö saapuu kauppaan ilman työmääräystä ja nämä kyseiset henkilöt ovat käännytetty tiukasti pois. Isommissa kaupoissa kulkuoikeuksia maksukorttidataa sisältäviin tiloihin on rajoitettu. Kaupoille on projektin myötä mennyt selkeä viesti perille, että korttirikollisuus on yleistynyt ja tietoturva-asioihin on kiinnitettävä entistä enemmän huomiota.

7.5 Maksupäätteiden tarkkailu

Maksupäätteiden tarkkailuun on tehty selkeät ohjeet. Kassavastaavan tulee päivittäin tarkastaa maksupäätteet ylimääräisten laitteiden varalta. Poikkeustilanteessa on ensiksi otettava yhteyttä esimieheen, jonka jälkeen oman ketjun riskienhallintaan. Tämän kaltaisia tapauksia ei ole Suomessa tullut tietoon, mutta ”monenlaista yritystä on ollut missä tuntematon henkilö on esittäytynyt maksupäätteiden huoltajana, jotta pääsisi käsiksi laitteisiin”, kertoo erään ketjun projektipäällikkö. Suomessa on tapahtunut muutama murto kauppoihin, joissa mitään ei ole havaittu vietävän. Tällaisessa tapauksessa tutkitaan onko syynä maksupäätteiden väärinkäyttö. Todisteita tästä ei ole Suomesta kuitenkaan löytynyt.

7.6 Maksupäätteen haasteellisuus

Haastatteluissa kysyttiin sitä, minkä asian haastateltavat kokivat haastavana projektiin lähdettäessä. Kohdeyrityksen erään ketjun projektipäällikkö pelkäsi, että muutos tulisi olemaan hyvin radikaali. Vaikutus oli kuitenkin luultua pienempi. Ennakkopeloista suurin oli se, miten uutta maksupäätettä osataan käyttää. Osaavatko asiakkaat tai osaavatko myyjät käyttää sitä. Suurimpana haasteena oli se, että uudessa maksupäätteessä asiakas itse lukee oman bonus-

korttinsa. Joillekin ihmisille se tuntuu olevan vaikeaa. Se nähtiin ongelmana ja siihen reagoitiin vuosi sitten. Ratkaisuna on se, että voidaan käyttää etäluettavaa bonuskorttia ongelmia aiheuttaneen magneettijuovan sijasta. Maksupäätteissä tämä kyseinen etäluku on joten uusia asennuksia ei jatkossa tarvita.

7.7 Maksuhäiriöiden virheenselvitys

Maksuhäiriöiden virheselvityksestä on olemassa ohjeet. Yksi yleisimmistä maksuhäiriöistä on se, että asiakkaalta on veloitettu jokin tuote tuplana. Ohjeistuksen mukaan tulee ensin tutkia onko samana päivänä ollut enemmän heittoa maksutapahtumissa. Luottokuntaan tulee ottaa yhteyttä jos tilille on jäänyt varauksia roikkumaan. Puhelimen välityksellä ei kuitenkaan saa kertoa kokonaisia korttinumeroita, vaan selvitystä on tehtävä korttinumeron loppuosan perusteella. On myös ohjeistettu niin, että korttinumeroita ei saa kirjata ylös mihinkään. Virheenselvitys projektin myötä on saattanut hieman hankaloitua juuri sen takia, että korttinumeroita ei ole missään järjestelmässä kokonaisena. Osalla ketjuista selvitys menee käsitöiksi ja osalla tiedot löytyvät sähköisestä arkistosta. Ennen projektia liikenneasemilla maksuliikenne liikkui polttoaineveloitusjärjestelmän kautta. Tuolloin toiminta oli hyvin selkeä. Virhetilanteessa otettiin yhteys polttoaineveloitusjärjestelmän tarjoajaan, josta he tarkistivat maksutapahtuman. Uudessa kassajärjestelmässä on kuitenkin se hyvä puoli, että kauppa pääsee itse käsiksi omaan kuittiarkistoon, koska tapahtumat löytyvät omalta kassapalvelimelta.

7.8 Jatkuva palvelu

Projektia ylläpitää jatkossa jatkuvan palvelun yksikkö. Se vastaa siitä, että kaikki tämä toimii vielä projektin jälkeenkin. PCI:n näkökulmasta projekti tekee sen, että sertifioinnit saadaan aikaan. Tämä prosessi toistuu vuosittain ja jatkuvan palvelun yksikölle jää sen ylläpitäminen. Kauppoihin tehdään joka vuosi uudet koulutukset. Henkilökunta tulee vuosittain kouluttaa uudelleen. Auditoinnit toistuvat vuosittain. Auditoija itse päättää kuinka laajalla otannalla auditoinnit suoritetaan. Auditoijat tarkastavat yksikön muutoslokin ja muita dokumentaatioita ja sen perusteella päättävät mihin auditoinnit tehdään. Jatkuvan palvelun yksikön tavoitteena on suorittaa sisäinen auditointi vuosikierron puolessa välissä. ”Tällä katsotaan että kaikki on kunnossa ja jos huomataan epäkohtia, tehdään niihin korjaustoimenpiteitä”, kertoo jatkuvan palvelun yksikön johtaja. Tällä tapaa voidaan taata, että auditointi menee sujuvasti kaikkialla. Hyvä valmistautuminen on tarpeen, koska auditointi maksaa. ”PCI:n vaatimuksiin kuuluu se, että auditointiin mentäessä tulee henkilökunnalla olla tietoturvakoulutus suoritettuna”, kertoo jatkuvan palvelun yksikön johtaja. Vuoden vaihteen jälkeen tulee seuraava tietoturvakoulutus ja siihen liittyvä tietoturvapassi. Koulutusta tullaan kehittämään ja siihen lisätään ajankohtaisia teemoja, koska maksaminen kehittyy jatkuvasti. Koulutukset eivät keskity pel-

kästään PCI:n vaatimuksiin, vaan käsittelevät tietoturvaa laajemmalta kantilta. Jatkuvan palvelun yksikön johtaja kertoo, että ylläpitämisessä keskeinen haaste on se, miten konserni saadaan myös ymmärtämään jatkuvan palvelun tärkeys, jotta resurssit riittävät jatkossakin. Projektin lopputulosten ylläpitäminen vaatii jatkuvaa työskentelyä ja kehittämistä. Aiheesta onkin juuri sen takia puhuttu jatkuvana toimintona. Toinen haaste on se, että vuosittainen prosessi ei ole vain yksi, vaan monta eri prosessia, jotka vaativat tekijänsä. Hallinnollinen työ yksinään vaatii paljon tekemistä. PCI-standardikin saattaa muuttua. Standardin muuttuessa hyvin merkittävällä tavalla, saattaa yllättävien muutosten vienti kauppaan olla hyvinkin työlästä. Tähän asiaan jatkuvan palvelun yksikkö on varautunut siten, että he ovat PCI-councilin jäseniä ja mahdollisista muutoksista kuullaan ajoissa.

8 Johtopäätökset

Kohdeyrityksen projektin tuomien muutosten jälkeen on nyt entistä turvallisempaa maksaa kaupassa sirukortilla. Sen lisäksi että maksamisen turvallisuus on kehittynyt, on myös tietoturvallisuus yleisesti kehittynyt kaupoissa. Projektin tuoman palvelun käyttöönoton jälkeen maksukorttinumeroita ei enää kerry kauppojen järjestelmiin tai kuittiarkistoihin. Tämä takaa sen, että on entistä vaikeampi hyväksikäyttää korttitietoja rikolliseen tarkoitukseen.

Järjestelmien kehityksen lisäksi on henkilökunnan tietoturvakoulutus noussut uudelle tasolle. Kaikille kaupassa työskenteleville suunniteltu pakollinen tietoturvakoulutus antaa henkilökunnalle paremmat valmiudet ymmärtää tietoturvariskejä ja ongelmatilanteen sattuessa toimia ohjeiden antamalla tavalla. Tietoturvapassin opiskelu ei vie henkilökunnalta suurta määrää aikaa ja sen suorittaminen varmistaa sen, että tekijä on myös ymmärtänyt tietoturvapassissa opetetut asiat. Jokaisen kaupan työntekijän tulee suorittaa tietoturvapassi kerran vuodessa. Tällä tavalla vanhoja asioita kerrataan, sekä uusia ajankohtaisia asioita voidaan oppia. Tämä takaa sen, että henkilökunnalta vaadittava tietoturvaosaaminen on ajan tasalla.

Opinnäytetyön kysymyslistaa voidaan jatkossa käyttää tietoturvakoulutuksen yhteydessä. Jatkuvan palvelun yksikkö voisi esimerkiksi käyttää kysymyslistaa sisäisessä auditoinnissa, joka valmistaa kauppoja varsinaiseen auditointiin. Kysymykset pohjautuvat PCI-standardiin ja tämän takia siitä voi olla hyötyä sisäisessä auditoinnissa.

Etäluettava bonuskortti on hyvä ratkaisu siihen, kun asiakkailla on ollut ongelmia lukea oma bonuskortti uudessa maksupäätteessä. Kehitysehdotuksena vanhaan systeemiin voisi olla se, että asiakkaita varten ovat selkeät ohjeet kassojen läheisyydessä siitä, miten käyttää oma bonuskortti lukijassa oikein, jotta maksamisesta tulisi sujuvampaa.

Kauppojen auditointi on vuosittainen tapahtuma. Samat toimenpiteet ja tarkastukset täytyy käydä läpi vuosittain, jotta varmistetaan se, että PCI-standardin noudattaminen on jatkuvaa. Tämä vaatii myös konsernilta resursseja, joten pohdinnan aiheena on se, miten jalkauttaa projekti niin, että se ymmärretään jatkuvana palveluna. Yhtenä ehdotuksena on se, että projektista voitaisiin mainita mm. yhteiskuntavastuuraportissa. Toinen tapa, jolla henkilökunnalle voisi tuoda projektia esille, on kertoa sen piirteistä ja tavoitteista yrityksen intranetissä. Tätä kautta projektin tärkeydelle voisi saada enemmän näkyvyyttä, jotta kaikki voisivat ymmärtää sitä paremmin. Kohdeyrityksen projekti ei ole vain kertaluontoinen tapahtuma, jonka jälkeen kaikki on valmista eikä siihen ole jälkikäteen puuttumista. Se vaatii jatkuvaa työtä prosessien sujumisen varmistamiseksi. Yrityksen tavoitteena on profiloitua vastuullisena toimittajana. Tämä tarkoittaa sitä, että jos asiakas antaa heille korttitietonsa, pidetään siitä myös huolta. Tietoturvallisuus on nykyajan yhteiskunnassa tärkeä asia. ”Niin kauan kun pysymme poissa otsikoista, olemme onnistuneet” kertoo tietoturvapäällikkö.

Lähteet

Alvarado, K. 2007. Merchants Failing to Meet PCI Standard. The Internal Auditor; Jun 2007

Finanssialan keskusliitto. 2011. EMV-maksupäätejärjestelmän toiminnallinen kuvaus V4.2. http://www.fkl.fi/teemasivut/sepa/tekninen_dokumentaatio/Dokumentit/EMV_maksupaatejarjestelma.pdf

Kari Lukka. Konstruktiivinen tutkimusote, http://www.metodix.com/fi/sisallys/04_virtuaalikirjasto/dokumentit/aineistot/konstruktiivinentutkimusote

Niki Klaus 2010. Tiger Team – Suomalainen tietoturvablogi http://www.nixu.fi/blogi/2010/helmikuu/massiivinen-luottokorttimurto-Suomessa--mutta-olisiko-se-voitu-pci-standardia-noudattamalla-estaa/

Ojasalo, K., Moilanen, T., Ritalahti, J. 2009. Kehittämistyön menetelmät. Sanoma Pro Oy

PCI Security Standards Council. 2010. PCI-DSS v2.0. https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0

Yrityksen sisäinen dokumentointi, 2011

Kuvat

Taulukot

Liitteet

Liite 1 Haastattelulomake

1. Missä säilytätte paperisia tositteita?

2. Miten tuhoatte vanhentuneet tositteet?

3. Missä säilytätte sähköisiä varmistusmedioita (nauhoja, USB-tikkuja tms.)?

4. Miten kassapalvelin on sijoitettu?

5. Kenellä on pääsy kassapalvelimelle?

6. Miten tarkkailette maksupäätteitä / työasemia mahdollisten ylimääräisten laitteiden osalta?

7. Miten toimitte, kun huoltomies tulee kauppaan?

8. Miten omat työntekijät perehdytetään tietoturvallisuuteen?

9. Miten valvotte henkilökunnan toimintaa?

10. Miten toimitte, kun asiakas tulee kertomaan, että häneltä on veloitettu maksukortilla tehty ostos kahteen kertaan?

11. Millaisia kulkuoikeuksia henkilökunnalla on kaupan eri tiloissa? Vaihteleeko se ryhmittäin?

12. Onko teidän mielestä tämän hetkisissä tietoturvaohjeissa jotain puutteellista tai teidän kaupassanne jotain käytännössä parannettavaa?