Yrityksen siirtyminen PCI DSS:n alaiseen järjestelmäylläpitoon

Eatech Oy

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Ammattikorkeakoulun opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

Visamäki, 10.5.2012

Joanna Vroullis

HAMK
HÄMEEN AMMATTIKORKEAKOULU

TIIVISTELMÄ

HÄMEENLINNA, VISAMÄKI
Tietojenkäsittelyn koulutusohjelma

Tekijä Joanna Vroullis **Vuosi** 2012

Työnnimi Yrityksen siirtyminen PCI DSS:n alaiseen järjestelmäylläpitoon

TIIVISTELMÄ

Opinnäytetyön toimeksiantaja oli Eatech Oy. Työn tarkoituksena oli tehdä selvitys PCI DSS -standardista ja sen vaatimuksista. Kyseessä oleva standardi tarjoaa tietoturvavaatimukset maksukorttiostamiseen liittyen. Standardista on tällä hetkellä voimassa versio 2.0 ja siirtyminen tulee olemaan pakollista kaikille niille, jotka ovat osallisena kortinhaltijoiden tietojen käsittelyyn. Aihe on ajankohtainen yritykselle, joka toimii kortilla maksamisessa palveluntarjoajan roolissa. Standardi tulee vaikuttamaan jokaisen henkilöstön jäsenen työskentelyyn. Työn tärkein tarkoitus on olla pohjana standardin mukaisuuteen siirtymisessä ja sen siirtymävaiheen tarkemmassa suunnittelussa. Työ tuottaa myös perustietoa standardista kaikille henkilöstön jäsenille.

Työssä käsiteltiin aluksi standardia yleisesti. Seuraavassa luvussa käytiin tarkemmin läpi PCI DSS:n 12 vaatimusta ja näihin liittyviä osa-alueita. Tässä käsiteltiin vaatimukset turvallisesta verkosta, korttimaksuun liittyvien tietojen suojaamisesta, haavoittuvuuksilta suojautumisesta, käyttäjien hallinnasta, verkon valvonnasta sekä yrityksen tietoturvakäytänteistä. Seuraavaksi pohdittiin standardin pohjalta siirtymävaihetta yleisesti sekä toimeksiantajan kannalta. Työssä käytettiin pääasiallisena lähteenä PCI DSS:n omaa dokumentaatiota standardista sekä muutamia muita Internet lähteitä. Toimeksiantajaan liittyvien tietojen keräämiseen käytettiin vapaamuotoisia haastatteluita.

Työn tuloksena syntyi kattava selvitys aiheesta ja ehdotus Eatech Oy:lle jatkotoimenpiteistä standardin suhteen. Standardi ei ollut työtä kirjoittaessa vielä pakollinen, mutta siirtymävaihe on lähteiden mukaan tulossa pian. Kyseessä on laaja standardi, joten työssä suositeltiin siirtymävaiheeseen varattavan vähintään puoli vuotta aikaa. Lisäksi yrityksen tulee huomata, että vaatimusten noudattaminen vaatii myös jatkuvaa työtä.

Avainsanat Maksukorttiliikenne, tietoturva, PCI DSS

Sivut 25 s.

HAMK
UNIVERSITY OF APPLIED SCIENCES

ABSTRACT

HÄMEENLINNA, VISAMÄKI
Degree Programme in Business Information Technology

Author Joanna Vroullis **Year** 2012

Subject of Bachelor's thesis Company's transition to PCI DSS compliant system administration

ABSTRACT

This thesis was assigned by Eatech Oy. The purpose of this study was to do research of the PCI DSS standard and its requirements. The standard is a data security standard for payment card transactions. The current standard version is 2.0 and will be mandatory for every participant in the payment card transactions. The subject is topical for the company which acts as a card transaction service provider. The standard will affect the work of every member of the personnel. The main goal of this thesis is to be a base for a transition into the compliance of the standard and for planning it thoroughly. This thesis will also provide basic knowledge of the standard for the personnel.

At first basic info about the standard is introduced. In the next chapter the 12 requirements of the PCI DSS standard are described with more detail. This includes requirements for secure network, protecting the cardholder data, protecting the system and data from vulnerabilities, controlling access, monitoring the network and maintaining a security policy for the personnel. Next the transition is considered based on the standard generally and for the subscribing entity. The main reference used in this study is the documentation of the standard and a few other Internet-based sources. For collecting information about the entity, informal interviews were used.

As a result of the study the company was presented with a proposal for further preparation for the transitional period. A research of the standard is also provided. When writing this document the standard is not yet mandatory but according to a few sources used in this thesis the transition period will be commenced soon. The standard is a wide concept and for that it is recommended in the study that at least half a year should be reserved for the transition period. The company should also be prepared to maintain compliance with the requirements of the standard after the transition.

Keywords Payment card processing, data security, PCI DSS

Pages 25 p.

SISÄLLYSLUETTELO

1 JOHDANTO 1

2 PCI DSS -STANDARDI 3

2.1 Auditointi 3
2.2 PA DSS 3

3 PCI DSS -VAATIMUSLUOKAT 5

3.1 Turvallinen verkko 5
3.1.1 Palomuuri ja reititys 6
3.1.2 Ohjelmistotoimittajien oletussalasanat ja asetukset 8
3.2 Korttimaksuun liittyvien tietojen suojaaminen 10
3.2.1 Tallennetut kortinhaltijatiedot 10
3.2.2 Kortinhaltijoiden tietojen siirto 12
3.3 Haavoittuvuuksilta suojautuminen 12
3.3.1 Virustorjunta 13
3.3.2 Turvalliset järjestelmät ja ohjelmistot 13
3.4 Käyttäjienhallinta 14
3.4.1 Tietoihin pääsyn rajoitus 14
3.4.2 Yksilöllinen käyttäjätunnus 15
3.4.3 Fyysisen pääsyn rajoittaminen 15
3.5 Verkon valvonta 17
3.5.1 Verkkoliikenteen valvonta 17
3.5.2 Suojausmenetelmien säännöllinen testaus 18
3.6 Tietoturvakäytänteet 19

4 SIIRTYMINEN PCI DSS:N MUKAISUUTEEN 21

4.1 Siirtymävaihe ja sen suunnittelu 21
4.2 Siirtymävaihe Eatech Oy:n kannalta 22

5 YHTEENVETO 24

LÄHTEET 25

Sanasto ja lyhenteet

CVSS	Common Vulnerability Scoring System, haavoittuvuuksien pisteytysjärjestelmä
DMZ	Demilitarized Zone eli suljettu sisäverkko, johon ei voida ottaa yhteyttä suoraan ulkoverkosta
Etäyhteys	Etäyhteydellä tarkoitetaan tässä työssä eri PC:eille otettavaa yhteyttä toimistoltamme, jolla koneita ylläpidetään ja tarjotaan tarvittaessa tukea asiakkaille.
Haittaohjelma	Erilaiset haittaa aiheuttavat ohjelmistot, kuten virukset, troijalaiset, tietokonemadot, vakoilu- ja mainosohjelmat sekä rootkit-tiedostot
Maksukorttiliikenne	Kaikki korttimaksuihin liittyvät tapahtumat
NTP	Network Time Protocol, verkon yli toimiva aikaprotokolla, jolla voidaan synkronisoida esimerkiksi samassa verkossa olevien tietokoneiden kellot samaan aikaan
PA-DSS	Maksukorttiliikenteen ohjelmistotuotantoon liittyvä standardi
Palomuuri	Ohjelma tai laite, joka suodattaa ei haluttuja verkkoliikenne paketteja tai hyökkäyksiä verkosta
PCI DSS	Payment Card Industry, Data Security Standard eli standardi, joka ohjaa maksukorttiliikenteeseen liittyviä toimia
PCI SSC	Payment Card Industry Security Standards Council, maksukorttialan tietoturvastandardijärjestö
Reititys	Ohjaaminen ohjelmitse verkko-osoitteeseen ilman, että suoraa IP-osoitetta tarvitsee paljastaa
SNMP	Simple Network Management Protocol, standardi verkossa olevien laitteiden hallintaan
Virustorjunta	Ohjelmisto, joka on tarkoitettu haitallisten ohjelmien tunnistamiseen ja käsittelemiseen

1 JOHDANTO

PCI DSS on standardi, joka ohjaa maksukorttiliikenteeseen liittyviä toimia. Standardi on tällä hetkellä kehityksen alaisena, joten vaatimukset saattavat vielä muuttua ja tarkentua. Standardi tulee olemaan pakollinen kaikille tahoille, jotka käsittelevät, säilyttävät tai välittävät maksukorttitapahtumien tietoja.

Työn toimeksiantaja Eatech Oy kehittää ja ylläpitää erinäisiä järjestelmiä, joista osassa käsitellään maksukorttitapahtumia. Tästä syystä yrityksen tulee valmistautua PCI DSS -standardin voimaantuloon ja varmistaa, että kaikki osa-alueet ovat standardin vaatimalla tasolla. Yritykselle on myös erityisen tärkeää tarjota tietoturvaltaan luotettavaa palvelua ja ohjelmistoratkaisuja myös tulevaisuudessa. Työn tavoitteena on luoda yleiskuvaus PCI-DSS -standardista koko yritykselle sekä lähtökohdat tarkkojen toimintamallien luontiin ylläpito-osastolle.

Työn aihealueeseen perehdytään kahteen keskeiseen tutkintakysymyksen nojaten: Mitä PCI DSS -standardi sisältää? Miten standardin alaisuus voitaisiin saavuttaa? Aluksi työssä perehdytään PCI DSS -standardiin yleisesti perustiedon kartuttamiseksi ja samalla tuoden koko yritykselle kattavan selvityksen aiheesta. Selvitystä aiheesta tehdään pääasiassa standardin kehittäneen neuvoston dokumentoinnin pohjalta, muiden Internet-pohjaisten lähteiden sekä yrityksen jäsenten haastatteluiden avulla. Tässä perehdytään myös Luottokunnan tekemään ohjeistukseen. Tämän jälkeen käsitellään standardin mukaisuuteen siirtymistä yrityksen kannalta ja suositellaan tehtäviä toimenpiteitä. Tässä pyritään saamaan parempaa kuvaa yrityksen sisäisistä käytänteistä sekä niiden suunnittelusta haastattelemalla yrityksen jäseniä.

Työ tulee tuottamaan laajaa tietoa PCI DSS -standardista käytännön näkökulmasta sekä kuinka Eatech Oy:n tulee valmistautua standardin voimaantuloon. Opinnäytetyö tarjoaa myös maksuliikenteeseen liittyvien palvelujen tarjoajana toimivalle yritykselle toimintatavat ylläpitotoimintaan PCI DSS:n suhteen.

Työstä rajataan tilaajayrityksen salassapitovelvollisuuden vuoksi tarkempi selvitys toimintaympäristöstä ja vaadittavista korjaustoimenpiteistä. Lisäksi siirtymävaiheen tarkat toimintamallit on rajattu työn ulkopuolelle sillä tarkkojen mallien luontiin tulisi varata jopa vuosi, joten työ toimii yritykselle lähtökohtana mallien luontiin. Aiheeseen liittyvän PA DSS ohjelmistokehitysstandardin tarkempi selvitys on rajattu työn ulkopuolelle. Yleistä tietoa standardista löytyy kuitenkin luvusta 2, sillä PCI DSS -standardin mukaisessa ylläpitoympäristössä tulee ottaa huomioon käytettyjen sovelluksien PA DSS:n mukaisuus.

Aihe on hyvin ajankohtainen, sillä siirtyminen PCI DSS:n mukaiseen työskentelyyn tapahtuu lähitulevaisuudessa. Työyhteisö tulee hyötymään työstä, koska aikaisempia toimintamalleja tai ohjeistusta aiheeseen liittyen ei ole yrityksen ylläpitotehtävissä toimiville.

Tämä on aiheena ideaalinen tekijän oman tietoperustan laajentamiseen jo opintojen kautta kerrytetyn lisäksi sekä yritykselle hyvin oleellinen selvitystyö tulevia toimintamalleja toteuttaessa ja muutoksiin valmistautumisessa. Standardi tulee lisäksi olemaan osana koko organisaation päivittäistä työskentelyä.

2 PCI DSS -STANDARDI

PCI DSS, joka tulee englanninkielisistä sanoista Payment Card Industry Data Security Standard, on *PCI Security Standards Council* -neuvoston tuottama tietoturvaa koskeva standardi. Se ohjaa maksukorttiliikenteeseen liittyviä toimia.

Standardin noudattaminen koskee kaikkia maksukorttitapahtumia käsitteleviä tahoja, kuten kauppiaat, palveluntarjoajat, pankit ja maksunvälittäjät. Tätä edellyttävät luottokorttiyhtiöt ja Luottokunta. Standardia tulee noudattaa aina, kun kortinhaltijoiden tietoja tallennetaan, käsitellään tai välitetään tavalla tai toisella. Tarkoituksena on tehdä kortilla maksamisesta turvallisempaa ja luotettavampaa. Noudattamalla standardia suojataan korttitietoja leviämästä ja päätymästä vääriin käsiin.

Tarkoituksena on myös muodostaa maailmanlaajuisesti yhtenäiset tietoturvakäytänteet. Standardia tulee käyttää lähtökohtana kortinhaltijoiden tietojen turvaamiseen tarkoitetuille teknisille ja operatiivisille vaatimuksille. Standardi tarjoaa minimivaatimukset tietoturvalle ja yrityksen tai organisaation on suositeltavaa kehittää ja parantaa tietoturvaa näiden pohjalta.

Standardia sovelletaan kaikkiin maksukorttien käsittelyssä mukana oleviin toimijoihin. Näitä ovat mm. kauppiaat, tietojen käsittelijät, tapahtumien vastaanottajat, tietojen välittäjät, palveluntarjoajat sekä kaikki, jotka tallentavat näitä tietoja. Tässä työssä keskitytään palveluntarjoajan rooliin PCI DSS -standardin noudattamisessa. (PCI DSS 2.0:2010).

2.1 Auditointi

Standardin mukaisuuden toteutumisen voi tarkastuttaa riippumattomalla taholla auditoinneilla. Auditointi suoritetaan käyttämällä PCI SSC:n sivuilta löytyvää arviointilomaketta (PCI DSS 2.0:2010). Samaa lomaketta voidaan käyttää myös standardiin valmistautuessa. Auditointi tulee suorittaa vuosittain tai kun organisaatiossa tehdään uusia muutoksia. Arviointi suoritetaan uudestaan niin kauan, kunnes vakavia puutteita ei löydy.

Ennen varsinaista auditointia yritys voi suorittaa sisäisiä auditointeja, mutta lopullinen auditointi tulee aina suorittaa virallisesti hyväksytyn auditoijan toimesta. Auditoijaa tai muita asiantuntijoita voidaan kuitenkin konsultoida muutoksiin valmistautuessa tai niitä suunniteltaessa sekä muissa standardiin liittyvissä kysymyksissä. (PCI DSS 2.0:2010).

2.2 PA DSS

PCI DSS -standardiin liittyy maksusovellusten tekoa ohjaava PA DSS -tietoturvastandardi. PA DSS tulee sanoista Payment Application Data Security Standard ja toimii tietoturvastandardina ohjelmistokehittäjille. PA DSS ei korvaa PCI DSS -standardia vaan toimii sitä laajentavana standardina. Koska tämä työ käsittelee ainoastaan ylläpitoon liittyvää PCI DSS -standardia, rajataan PA DSS työn ulkopuolelle.

PCI DSS:n mukaisessa järjestelmien ylläpidossa tulee ottaa huomioon, että ympäristöön implementoidut sovellukset tulee olla luotuna PA DSS standardin mukaisesti. Vastaavasti myös sovelluksen toteutusympäristön tulee noudattaa PCI DSS -standardia. (PA DSS 2.0:2010.)

3 PCI DSS -VAATIMUSLUOKAT

PCI DSS -standardia voidaan hahmottaa kuuden vaatimusluokan pääpiirteiden avulla: turvallinen verkko, korttimaksuun liittyvien tietojen suojaaminen, haavoittuvuuksilta suojautuminen, käyttäjienhallinta, verkon valvonta ja tietoturva. Luokat ja näihin sisältyvät vaatimukset ovat listattuna taulukossa 1. Seuraavissa kappaleissa käydään edellä mainitut luokat pääpiirteittäin läpi.

Taulukko 1. PCI DSS -standardin vaatimukset luokittain (PCI DSS 2.0:2010).

	Luokka		**Vaatimus**
I.	Turvallisen verkon rakentaminen ja ylläpito	1.	Asenna ja ylläpidä palomuuriratkaisua.
		2.	Älä käytä ohjelmistojen tai laitteiden oletussalasanoja tai -asetuksia.
II.	Kortinhaltijoiden tietojen suojaaminen	3.	Suojaa tallennetut kortinhaltijatiedot.
		4.	Salaa kortinhaltijoiden tiedot, joita lähetetään julkisissa verkoissa.
III.	Haavoittuvuuksilta suojaavien ohjelmistojen ylläpito	5.	Käytä virustorjuntaohjelmistoa ja päivitä sitä säännöllisesti.
		6.	Kehitä ja ylläpidä tietoturvallisia järjestelmiä ja ohjelmistoja.
IV.	Tiukan pääsynhallinnan käyttöönotto	7.	Rajoita pääsyä kortinhaltijoiden tietoihin työn vaatimusten perusteella.
		8.	Määritä jokaiselle tietokoneen käyttäjälle yksilöllinen tunnus.
		9.	Rajoita fyysistä pääsyä kortinhaltijoiden tietoihin.
V.	Verkkojen säännöllinen seuranta ja testaaminen	10.	Seuraa ja valvo kaikkea verkkoresurssien ja kortinhaltijoiden tietojen käyttöä.
		11.	Testaa turvajärjestelmät ja prosessit säännöllisesti.
VI.	Tietoturvakäytänteiden ylläpito	12.	Luo koko henkilöstöä koskevat tietoturvakäytänteet ja ylläpidä niitä.

Tarkat vaatimukset ja arviointikriteerit löytyvät PCI DSS:n dokumentaatiosta kappaleesta *"Detailed PCI DSS Requirements and Security Assessment Procedures"*. Näitä tulee käyttää standardin mukaisuutta tutkittaessa (PCI DSS 2.0:2010). Nämä ovat myös hyvä apu tietoturva-asioita kehittäessä ja suunniteltaessa.

3.1 Turvallinen verkko

Ensimmäinen vaatimus on turvallisen verkon luonti ja ylläpito. Standardi on rajannut tähän kuuluvaksi palomuuri- ja reititysratkaisuiden käytön sekä näiden ylläpidon. Toisena osa-alueena on laitteistojen sekä ohjelmistojen oletusasetusten ja -salasanojen muuttaminen ennen käyttöönottoa. Nämä pitävätkin sisällään tärkeimmät työkalut verkkoliikenteen suojaamiseen ja rajaamiseen sekä poistavat mahdolliset väärinkäytöt oletussalasanoja tai -asetuksia käyttäen. Ilman turvallista verkkoa koko järjestelmä on turvaton.

3.1.1 Palomuuri ja reititys

Verkon tulee olla palomuurilla suojattu, jotta ei-haluttu liikenne voidaan estää. Palomuuriratkaisua tulee lisäksi ylläpitää ja päivittää säännöllisesti. Palomuurin ja reitittimen toiminta on suunniteltava järjestelmällisesti ennen varsinaista käyttöönottoa. Organisaatiolla on oltava testaus- ja hyväksymismenettelyt palomuurin ja reitittimen asetuksille ja näiden muutoksille. Näin varmistetaan, että uusia sääntöjä luodessa ne on asianmukaisesti testattu. Tätä voidaan hyödyntää suuremmalla mittakaavalla koko arkkitehtuuria muodostettaessa, jolloin tarkistus tehdään kaikille luotaville säännöille.

Verkkokaaviot ovat oleellinen osa suojausta rakennettaessa. Näitä tulee ylläpitää ja pitää jatkuvasti ajan tasalla. Verkkokaaviossa tulee olla esillä kaikki yhteydet kortinhaltijoiden tietoihin. Verkkokaavion avulla voidaan hahmottaa mitkä ovat osana kriittisten tietojen käsittelystä ja näin vaativat parempien suojamenetelmien käyttöönottoa.

Palomuuria on käytettävä kaikissa verkkoliikenteissä, mukaan luettuna Internet, DMZ-verkko sekä sisäisen verkkoalueen välisissä yhteyksissä. Lisäksi kaikki liiketoiminnalle tarpeelliset sallitut palvelut, protokollat ja portit tulee olla dokumentoituna. Jos liiketoiminta erityisestä syystä vaatii niin sanotusti turvattomiksi katsottujen protokollien käyttöä, näiden käytön perustelu sekä näiden turvallisuusmenetelmät tulee olla lisäksi dokumentoituna.

Palomuurin ja reitittimien säännöt tulee katselmoida vähintään puolen vuoden välein. Tämä siksi, että varmistetaan kaikkien tarpeellisien sääntöjen olemassaolo muutoksien tai lisäyksien varalta. Myös tarpeettomaksi käyneet säännöt on hyvä poistaa.

Jotta ympäristö, jossa maksukorttitietoja säilytetään ja käsitellään, olisi turvallinen, tulee sen yhteyksiä ulkoverkkoon rajoittaa. Tässä ulkoverkolla tarkoitetaan verkkoa, joka ei ole palveluntarjoajan hallittavissa tai valvottavissa. Palomuureille ja reitittimille tuleekin luoda määritykset, jotka rajoittavat yhteyksiä ulkoverkosta kaikkiin maksukorttiympäristössä oleviin komponentteihin.

Saapuvaa ja lähtevää verkkoliikennettä tulee rajata. Hyvä lähtökohta on estää kaikki saapuva ja lähtevä liikenne maksukorttien käsittelyympäristöstä ja erikseen sallia vain liiketoiminnan kannalta välttämättömät yhteydet. Näin vältytään mahdollisilta aukoilta palomuurissa ja rajataan liikennettä korttitietoihin ja myös vähennetään mahdollisuutta tietojenvuotoon.

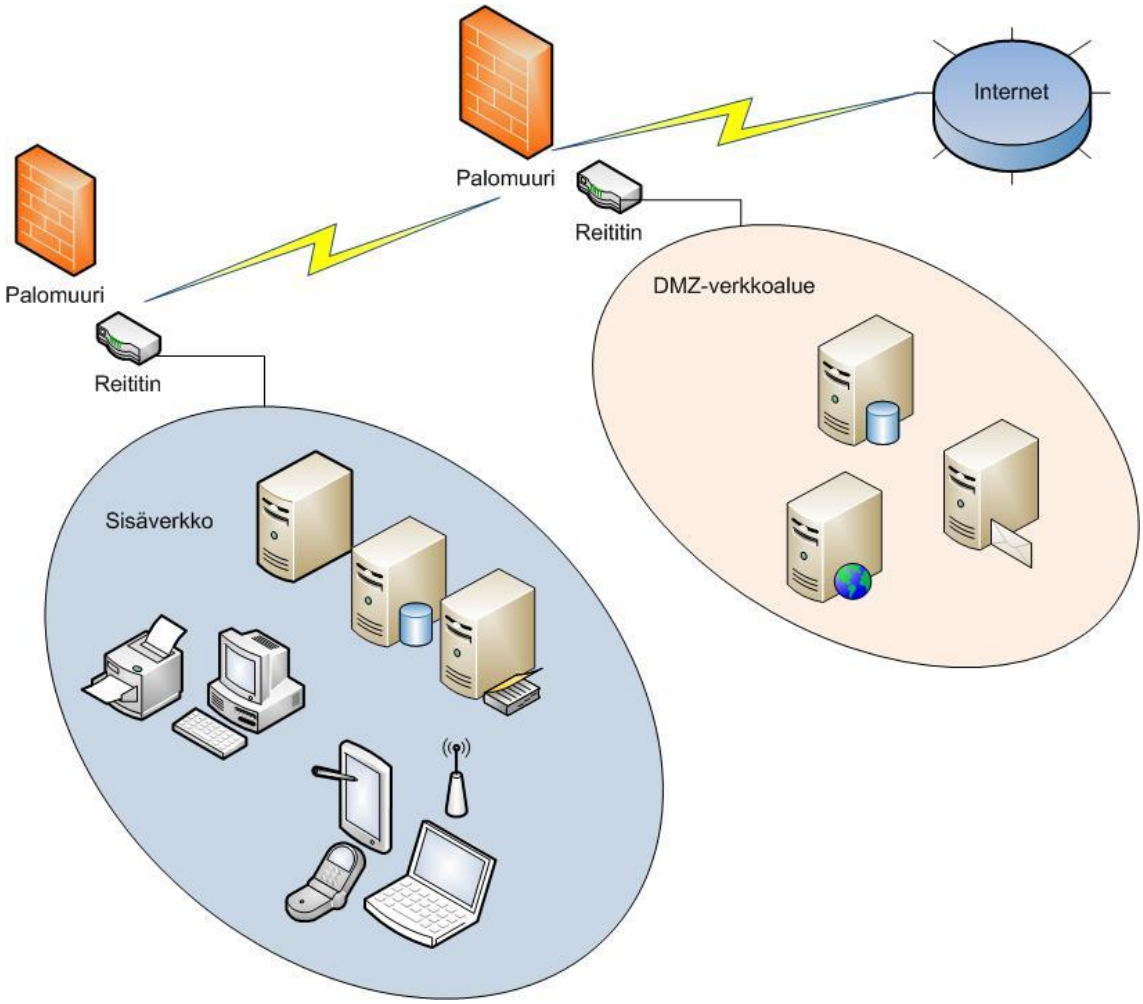
Jotta edellä mainitut säännöt ja määritykset ovat aina toiminnassa, vaatii standardi myös niiden turvaamisen ja synkronisoinnin. Näillä toimilla vältetään asetusten hukkuminen laitteiden tai ohjelmistojen uudelleen käynnistyessä tai virhetilanteissa esimerkiksi, kun virta katkeaa yllättäen. Erillisillä asetustiedostoilla saadaan myös tarvittaessa siirrettyä tiedot uuteen laitteeseen mahdollisen laiterikon jälkeen.

Koska langattomat verkot ovat helpommin saavutettavissa kuin langalliset, tulee kaikki liikenne näistä estää ympäristöön, jossa kortinhaltijoiden tietoja käsitellään. Estäminen tulee standardin mukaan tehdä rajapalomuurein. Tästä on poikkeuksena liiketoiminnan kannalta välttämätön liikenne, esimerkiksi langaton kortinlukija tai jokin muu maksuympäristön osa, jolloin langattoman verkon liikenteen tarkkaa valvontaa edellytetään.

Kaikki suora julkinen pääsy Internetistä järjestelmäkomponentteihin tulee estää. Tämän rajoitukseen tulee käyttää DMZ-verkkoratkaisua. DMZ eli *demilitarized zone* (demilitarisoitu alue) on verkkoalue, joka on palomuurilla erotettu sisä- ja ulkoverkosta. Tällä voidaan jakaa osa organisaation sisäverkossa sijaitsevia tiedoista tai palveluista ilman suoranaista pääsyä sisäverkkoon.

Standardi määrittää, että DMZ-verkosta tulee rajata pääsy ainoastaan niihin järjestelmäkomponentteihin, joita tarvitaan liiketoiminnallisista syistä ja joihin on valtuutettu julkinen pääsy. Kaikki komponentit, jotka säilyttävät kortinhaltijoiden tietoja tulee olla erotettuna DMZ-verkosta ja sijaita vain kortinhaltijaympäristön sisäverkossa, johon ainoastaan sisäverkossa olevat laitteet voivat kommunikoida.

Kaikki liikenne tulee lisäksi rajata DMZ-verkon IP-osoitteisiin eikä mitään suoraa liikennettä saa olla ulkopuolisen verkon ja kortinhaltijatietojen ympäristön välillä. Esimerkki DMZ-verkosta on esitetty kuvassa 1.



Kuva 1. DMZ-verkon rakenne (TechRepublic, 2005)

Verkon rajauksessa tulee käyttää myös palomuurissa asetettavaa pakettisuodatusta, eli vain ennalta määrätyt yhteydet ovat sallittuja, muut estettyjä. Lisäksi mitään verkkoihin liittyviä IP-osoite- tai reititystietoja ei tule levittää ulkopuolisille tahoille. (TechRepublic:2005; PCI DSS 2.0:2010, 20-23.)

Lisäksi kaikille tietokoneille, joita käytetään organisaation verkossa ja joista on suora pääsy Internetiin, tulee olla asennettuna palomuuriohjelmisto. Ohjelmiston tulee olla aktiivisena ja asetukset määritetty organisaation määritysten mukaisesti sekä käyttäjien tekemät muutokset näihin tulee estää. (PCI DSS 2.0:2010, 20-23.)

3.1.2 Ohjelmistotoimittajien oletussalasanat ja asetukset

Standardi vaatii, että ympäristössä, jossa käsitellään kortinhaltijoiden tietoja, ohjelmistojen tai laitteistojen oletusasetuksia ja oletussalasanoja ei käytetä. Nämä asetukset tulee vaihtaa ja tarkistaa ennen laitteen asentamista verkkoon.

Syynä salasanojen ja asetuksien vaihtoon on se, että nämä ovat yleisesti saatavilla olevaa tietoja ja tekevät näin suuren tietoturva-aukon järjestelmään. Näitä voidaan esimerkiksi käyttää hyväksi järjestelmään kohdistuvissa hyökkäyksissä, jolloin tietomurron riski on suurempi ilman vaihtoa.

Poistettavia oletusasetuksia on esimerkiksi verkkojen hallinnassa käytettävä tietoliikenneprotokollan SNMP:n yhteisönimet (simple network manager protocol) sekä kaikki oletuksena tulevat käyttäjätilit, jotka eivät ole järjestelmän ylläpidon tai liiketoiminnan kannalta tarpeellisia. Jos oletuskäyttäjätilejä kuitenkin jätetään käyttöön, tulee näiden salasanat vaihtaa.

Langattomissa verkoissa tulee lisäksi huomioida yhteyden salausavaimet. Nämä tulee vaihtaa oletusasetuksista sekä kun ne tietävä henkilö poistuu yrityksestä tai vaihtaa työtehtäviä. Vahva tunnistuksen ja tietojenlähetyksen salaus tulee myös taata lataamalla uusimmat ohjelmistoversiot laitteistoihin.

Kun uusia järjestelmiä määritetään, tulee käyttää näiden käyttötarkoitukseen soveltuvia määritysstandardeja. PCI DSS vaatiikin, että kaikkien järjestelmäkomponenttien asetusten määritykseen tulee luoda määritysstandardit, joilla taataan, että oletusasetukset vaihdetaan johdonmukaisesti sekä haavoittuvuuksiin varautuen.

Luotujen standardien tulee olla alalla hyväksyttäviä sekä näitä tulee päivittää aina, kun uusia haavoittuvuuksia havaitaan. Määritysstandardeissa tulee olla käsiteltynä seuraavat neljä osa-aluetta.

1. Kullakin palvelimella on vain yksi toiminto. Tämä siksi, että vältetään samalla palvelimella eri turvallisuustasoja vaativien toimintojen suorittamista, joka ei ole tietoturvan kannalta suositeltavaa.

2. Ainoastaan tarpeelliset ja turvallisiksi todetut palvelut, protokollat, taustaprotokollat ja muut vastaavat tulee ottaa käyttöön. Näin pystytään paremmin hallitsemaan ympäristöä ja vältytään odottamattomilta tietoturva-aukoilta järjestelmässä. Jos on liiketoiminnan kannalta välttämätöntä käyttää turvattomiksi luokiteltuja palveluita tai taustaprosesseja tulee ne suojata.

3. Yleiset tietoturva-asetukset tulee olla määritettynä väärinkäytön estämiseksi.

4. Järjestelmästä tulee poistaa kaikki tarpeeton toiminnallisuus, kuten komentosarjat, ajurit, lisäominaisuudet, alijärjestelmät, tiedostojärjestelmät ja www-palvelimet. Tämä vähentää myös tietoturva-aukkojen mahdollisuutta. Kaikki jätettävä toiminnallisuus tulee olla dokumentoitua.

Lisäksi kaikki etähallinnan kautta tehtävät järjestelmänhallintatoimet tulee salata vahvalla salauksella. Tässä voi käyttää esimerkiksi SSH- tai VPN-teknologioita Web-pohjaista ja muuta etähallintaa varten. Näitä testatessa tulee varmistaa, että yhteys on salattu ennen salasanan syöttöä, etäkirjautumiskomennot eivät ole käytettävissä sisäisesti, www-pohjaisen etähallinnan salaus on vahvaa tasoa. (PCI DSS 2.0:2010, 24-27.)

3.2 Korttimaksuun liittyvien tietojen suojaaminen

Korttimaksuun liittyvien tietojen suojaaminen pitää sisällään tietojen tallentamisen suojatussa muodossa sekä siirtämisen salattuna julkisissa verkoissa. Näillä suojausmenetelmillä vältetään tiedon väärinkäyttö pitämällä se muodossa, jossa se ei ole luettavissa ilman tarvittavia salausavaimia tai tunnuksia, joko tilanteessa jossa järjestelmään murtaudutaan tai välittäessä tietoja julkisessa verkossa, jossa myös ulkopuolisilla on niihin pääsy.

3.2.1 Tallennetut kortinhaltijatiedot

Kaikki kortinhaltijat tulee säilyttää salattuina. Näin varmistetaan, että mahdollisen tietomurron sattuessa tiedot eivät ole luettavissa ilman oikeita salausavaimia eikä murtautuja voi käyttää tietoja hyväkseen.

Kriittisimpiä tietojensalausmenetelmiä ovat tietojen salaus salausavainta käyttäen, tietojen katkaisu ja maskaus. Salausavaimella tehtävä suojaus varmistaa sen, että tiedot eivät ole luettavissa ilman salaukseen käytettyä avainta. Tietojen katkaisulla säilytetään vain se osa tiedoista, jotka ovat välttämättömiä liiketoiminnan kannalta, esimerkiksi säilytetään korttinumerosta vain kuusi ensimmäistä ja neljä viimeistä numeroa, jolla kortti voidaan tunnistaa, mutta ei väärinkäyttää. Lisäksi tulee huomata, että PAN- eli korttinumeroa ei tule koskaan lähettää suojaamattomana loppukäyttäjille tarkoitetuissa viestimissä, kuten pikaviestinohjelmissa tai sähköpostissa.

Kortinhaltijoiden tietojen suojaamiseen liittyy myös se, että tietoja säilytetään vain maksimissaan se aika mikä on tarpeellista lainsäädännön, muun säännöstelyn sekä liiketoiminnan kannalta. Muita säännöstelysyitä tietojen säilyttämiseen voi esimerkiksi olla ostojen peruutukset, erilaiset hyvitykset sekä tietojen hukkuminen järjestelmästä. Kun tämä aika on ylittynyt, tulee tiedot tuhota. Edellä mainittujen vaatimusten varmistamiseksi, yrityksen tulee luoda käytännöt tietojen säilytyksestä ja tuhoamisesta.

Arkaluontoista tietoa ei tule varmennuksen jälkeen säilyttää salattunakaan. Tästä poikkeuksena ovat ainoastaan korttien liikkeellelaskijat ja liikkeelle laskemiseen liittyviä palveluita tarjoavat yritykset, jotka tarvitsevat tietoja liiketoiminnallisesti perustellusta syystä. Tällöin tarvittavat tiedot tulee säilyttää suojattuna.

Kaikkia kortin magneettiraidan osien tietoja ei tule tallentaa, eikä myöskään vastaavia tietoja sirulta tai muualta. Esimerkiksi seuraavat tiedot ovat yleensä vain tarpeellista tallentaa normaaleista liiketoiminnallisista syistä: kortinhaltijannimi, korttinumero, kortin voimassaoloaika sekä käyttöalakoodi, joka kertoo mitä kortilla saa ostaa. Edellä mainituista tiedoista tulee tallentaa vain ne, jotka ovat välttämättömiä liiketoiminnan kannalta. Kaikki tallennetut tiedot tulee säilyttää ja tallentaa salattuna. Lisäksi on huomattava, että kortin tarkistetunnusta, jota käytetään kortinvarmennukseen ostotapahtumissa joissa kortti ei ole läsnä, esimerkiksi verkko-ostoksissa, tai PIN- eli tunnuslukua tai salattua PIN-lohkoa ei saa tallentaa missään tilanteessa.

Maksukortin korttinumero tulee olla maskattuna, kun se on esillä esimerkiksi maksupäätteillä tai kuitilla. Numerosta saa olla näkyvillä enintään kuusi ensimmäistä ja neljä viimeistä numeroa. Tämä rajoitus ei koske henkilöitä, joiden tarvitsee liiketoiminnallisista syistä nähdä koko PAN, eikä myöskään syrjäytä tiukempia vaatimuksia kassapäätteiden kuiteissa.

Maksukortin numeroa (PAN) tallennettaessa se tulee salata. Salauskeinoja on mm. yksisuuntainen vahva salausalgoritmi, merkkijononkatkaisu sekä kertakäyttöiset salausavaimet. Jos katkaistua ja peitettyä korttitietoa säilytetään samassa ympäristössä, tulee varmistaa etteivät ulkopuoliset henkilöt pysty yhdistämään näitä tietoja ja näin mahdollisesti palauttamaan alkuperäisiä korttitietoja. Lisäksi on huomattava, ettei PAN saa olla luettavissa korttivarmennuksen lokeista. Tarkempaa tietoa korttitiedoista, joita saa tallentaa, on taulukossa 2.

Taulukko 2. Korttitietojen tallentaminen (Luottokunta:2010)

Tallennettava tieto		**Saa tallentaa**	**Suojattava**
Kortinhaltijan tiedot*	Korttinumero (PAN)	Kyllä	Kyllä
	Kortinhaltijan nimi	Kyllä	Kyllä
	Käyttöalakoodi	Kyllä	Kyllä
	Voimassaoloaika	Kyllä	Kyllä
Arkaluonteiset tunnistustiedot**	Magneettijuovan kaikki tiedot	Ei	-
	CAV2/CVC2/CVV2/CID	Ei	-
	PIN / PIN lohko	Ei	-

Selvitykset:

PCI DSS vaatimukset ovat voimassa, jos kortinnumeroita tallennetaan, käsitellään tai välitetään

* Nämä tiedot saa tallentaa, mutta niiden on oltava suojattuna jos tallennetaan korttinumeron yhteydessä

**Arkaluonteisia tietoja ei saa tallennetaan missään olosuhteissa

Myös salaukseen käytettävien salausavainten tulee olla suojattu. Salausavaimiin pääsy tulee rajata mahdollisimman pieneen ryhmään avaintenhaltijoita. Ne tulee lisäksi tallentaa suojattuina, mahdollisimman harvoihin paikkoihin ja muotoihin.

Salausavainten hallintaan tulee laatia dokumentoidut käytännöt. Käytännöissä tulee määrittää vahvat salausavainten luonti-, salausavainten suojattu jakelu-, suojattu tallennus- sekä avainten vaihto- ja poistotoimenpiteet.

Avaimet tulee vaihtaa, kun niille määritetty toiminta-ajanjakso tai tietty määrä salattua aineistoa täyttyy. Avaimet tulee poistaa käytöstä tai korvata, kun niiden koskemattomuus on vaarantunut esimerkiksi, kun työntekijä lähtee yrityksestä tai kun on epäilys niiden paljastumisesta ulkopuolisille. Käytöstä poistaminen tehdään joko tuhoamalla, arkistoimalla, tai peruuttamalla. Jos avaimia on syytä arkistoida, tulee se tehdä suojatusti. Arkis-

toituja avaimia tulee käyttää vain salausten purkamiseen tai tarkastukseen eikä salaukseen. Salausavainten luvaton korvaaminen tulee olla estetty.

Avaintenhallintaan uskottujen tulee lisäksi antaa kirjallinen sitoumus. Tässä sitoumuksen antaja toteaa ymmärtävänsä ja hyväksyvänsä asetetut vastuut. (PCI DSS 2.0:2010, 28-34.)

3.2.2 Kortinhaltijoiden tietojen siirto

Arkaluonteiset kortinhaltijantiedot tiedot tulee salata, jos niitä siirretään julkisissa verkoissa tai muissa verkoissa, joihin ulkopuolisilla on helppo pääsy. Hyökkäyksiä kohdistetaan jatkuvasti huonosti määritettyihin WLAN-verkkoihin sekä salaus- ja todennusprotokollien haavoittuvuuksiin.

Standardi edellyttää vahvaa salausta ja vahvojen turvaprotokollien käyttöä, kuten SSL, TLS ja IPSEC, kun kortinhaltijoiden arkaluonteisia tietoja siirretään avoimissa ja julkisissa verkoissa. Julkisia verkkoja, jotka tulee ottaa huomioon, ovat esimerkiksi Internet, langattomat verkot, GSM sekä GPRS.

Edellisistä PCI DSS määrittää lisäksi langattomia eli WLAN-verkkoja käytettäessä tarkemmat tietoturvavaatimukset verkon helpomman pääsyn vuoksi. Tällä hetkellä standardi vaatii uusimman langattomien verkkojen tietoturvastandardin IEEE 802.11i:n käyttöä kaikissa langattomissa verkoissa, jotka siirtävät tai ovat yhteydessä kortinhaltijoiden tietoja sisältäviin ympäristöihin. Tällä varmistetaan parhain mahdollinen suoja käyttäjien tunnistamiseen sekä tietojen siirtoon. Lisähuomiona, ensimmäisen langattomien verkkojen suojausprotokollan WEP:n käyttö on kielletty suojausmenetelmänä 30.6.2010 lähtien.

Suojaamattomia korttinumeroita ei saa koskaan lähettää sähköpostitse, pikaviestimissä tai erilaisissa chat-ohjelmissa. Jos tietoja on välttämätön lähettää loppukäyttäjien viestimissä, tulee ne muuttaa lukukelvottomaan muotoon lähetyksen ajaksi tai salata vahvalla salauksella.
(PCI DSS 2.0:2010, 35-36.)

3.3 Haavoittuvuuksilta suojautuminen

Virustorjuntaohjelmat etsivät koneelta haitallisia ohjelmia ja tiedostoja ja näin suojaavat tietokonetta. Tästä syystä on tärkeää hankkia viruksentorjuntaohjelmisto. Ohjelmisto tulee myös pitää ajan tasalla, koska virusuhat muuttuvat nopeaa tahtia. Toinen tärkeä osa on turvallisten järjestelmien ja ohjelmistojen kehitys ja näiden ylläpito. Tietoturvaltaan heikko ohjelma saattaa toimia epäjohdonmukaisesti tai pahimmassa tapauksessa levittää tietoja.

3.3.1 Virustorjunta

Tietokoneet voivat altistua haitallisille ohjelmistoille, kuten viruksille, tietokonemadoille ja troijalaisille, normaaleissa liiketoiminnallisesti hyväksytyissä toimissa. Hyökkäyksille alttiita ovat esimerkiksi sähköposti, Internetin kautta tapahtuva työskentely, kannettavat tietokoneet sekä erilaiset tallennuslaitteet. Haittaohjelmistot käyttävät hyväksi järjestelmän haavoittuvuuksia. PCI DSS vaatii, että virustorjuntaa käytetään kaikissa hyökkäyksille alttiissa järjestelmissä, kuten palvelimissa ja henkilökohtaisissa tietokoneissa, nykyisiä ja mahdollisia tulevia uhkia vastaan.

Virustorjuntaohjelmistojen toimivuus ja ajantasaisuus tulee varmistaa säännöllisesti. Tähän sisältyy ohjelmisto- ja virustorjuntamääritysten säännöllisen päivityksen, jatkuvan käytössä olon varmistamisen, lokien luonnin sekä määräaikaiset tarkastukset. Lokitiedostot tulee lisäksi säilyttää PCI DSS:n vaatimuksen 10.7 mukaan, jotta ne voidaan tarkastaa auditoinnin yhteydessä ja varmistaa virustorjuntaohjelmiston toimivuus sekä tarkistaa mahdolliset tietoturvamurrot järjestelmään.

Virustorjuntaohjelmiston tulee havaita ja poistaa kaikki tunnetut haittaohjelmistotyypit. Näitä ovat esimerkiksi virukset, troijalaiset, tietokonemadot, vakoilu- ja mainosohjelmat sekä rootkit-ohjelmistot. (Virustorjuntaa.fi:2009; PCI DSS 2.0:2010, 37.)

3.3.2 Turvalliset järjestelmät ja ohjelmistot

Kaikissa kortinhaltijoiden tietoja käsitteleviin ympäristöihin liitoksissa olevissa järjestelmissä ja ohjelmistoissa tulee ottaa huomioon niiden turvallisuus. Näissä olevia tietoturva-aukkoja voidaan käyttää hyväksi järjestelmään murtautumisessa joten on erityisen tärkeää pitää yllä korkeaa tietoturvatasoa. Ohjelmistotoimittajilta saadut tietoturvapäivitykset paikkaavat monia tietoturva-aukkoja ja järjestelmän ylläpitävän tahon tuleekin viipymättä asentaa nämä päivitykset. Käytössä tulee olla viimeisimmät ja tarkoituksenmukaiset päivitykset, jotta järjestelmä pystytään suojaamaan kortinhaltijoidentietojen hyväksikäytöltä ja paljastumiselta.

Kaikki järjestelmäkomponentit ja ohjelmistot tulee suojata tiedossa olevia haavoittuvuuksia vastaan. Kriittiset tietoturvapäivitykset on asennettava kuukauden sisällä niiden julkaisemisesta.

Tietoturvapäivitykset tulee testata ja arvioida mahdollisten päällekkäisyyksien varalta nykyisten määritysten kanssa. Lukuisilta haavoittuvuuksilta voidaan välttyä käyttämällä alan standardien mukaisia kehitysprosesseja sekä turvallisia ohjelmointitekniikoita. Tietoturvapäivitysten käyttöönottoon ja ohjelmistomuutoksiin tulee olla hallintamenettelyt. Hallintamenettelyissä dokumentoidaan näiden tuomat muutokset, vaadittavat hyväksynnät käyttöönottoon, muutoksien toiminnallisuuden testaaminen järjestelmän tietoturvan kannalta sekä käyttöönoton peruutusmenetelmät.

Organisaatio voi halutessaan käyttää riskien luokituksiin perustuvaa aikataulutusta, jossa kriittisimmät tietoturvapäivitykset asennettaan kuukauden

sisällä julkaisusta, näitä ovat esimerkiksi julkiset laitteet, järjestelmät sekä tietokannat ja vähemmän kriittiset, kuten organisaation sisäiset palvelut ja laitteistot, kolmen kuukauden sisällä.

Organisaatiolla tulee olla käytäntö riskien tunnistamiseen ja uusien havaittujen riskien luokitukseen. Riskienhallinta tulee tehdä 30.6.2012 jälkeen PCI DSS:n vaatimuksen 6.2a:n mukaan, joka määrää, että organisaatiolla tulee olla prosessit riskien tunnistamiseen ja niiden luokitukseen.

Kaikki kortinhaltijatietoja käsittelevässä ympäristössä käytetyt ohjelmistot tulee lisäksi kehittää PCI DSS ja PA DSS -vaatimusten sekä alan parhaiden käytänteiden mukaisesti. Lisäksi tietoturva tulee ottaa huomioon kaikissa ohjelmistokehityksen vaiheissa.

Ohjelmistojen tietoturvan kannalta tulee ottaa huomioon seuraavat osa-alueet. Kehityksessä käytetyt käyttäjätilit, tunnukset ja salasanat tulee poistaa ennen julkaisua ja käyttöönottoa, ettei ohjelmistoihin jää ylimääräisiä tilejä, joille ei ole erikseen annettu pääsyä järjestelmään. Kaikki mukautettu ohjelmakoodi tulee katselmoida haavoittuvuuksien varalta. Kyseisen osan ohjelmoijat eivät saa suorittaa katselmointia. Ohjelmakoodiin tehtyjä mukautuksia voivat olla esimerkiksi tietyn asiakkaan tarpeiden mukaan ohjelmistoon räätälöidyt ominaisuudet.

Järjestelmäkomponenttien muutoksista tulee luoda käytänteet ja toimintamallit, jotka sisältävät seuraavat vaatimukset. Ohjelmistokehityksellä ja -testauksella sekä tuotannolla tulee olla erilliset ympäristöt sekä selkeästi eriytetyt tehtävät. Eriytys on tehtävä siksi, etteivät ympäristöt vaikuta toisiinsa eikä testauksessa olevaa tietoa pääse leviämään tuotantoon tai toiseen suuntaan.

Tuotantotietoja, kuten käytössä olevia korttinumeroita, ei tule käyttää testauksessa tai ohjelmistokehityksessä. Tämä aiheuttaa tietoturvariskin sekä pienen riskin siihen, että testiostoja saattaa mennä veloitukseen asti testeissä käytettävältä kortilta. Myös testaustiedot ja testauksessa käytetyt tilit tulee poistaa ennen käyttöönottoa. Näin vältetään tilanne, että esimerkiksi kassajärjestelmässä on testauksien aikaisia ostoja, jotka näkyvät lokeissa tai jopa ostotapahtumina kassassa. On myös tärkeää, että ainoastaan tarkoituksenmukaisesti lisätyt ja hyväksytyt käyttäjätilit ovat järjestelmässä. (PCI DSS 2.0:2010, 38-43.)

3.4 Käyttäjienhallinta

Standardi vaatii tehokkaan käyttäjienhallinnan käyttöä. Tällä rajoitetaan pääsy tietoihin ja tiloihin vain niitä välttämättä tarvitseville henkilöille. Samalla valvotaan käyttäjien tekemiä toimia sekä hallitaan organisaation tiedonkulkua.

3.4.1 Tietoihin pääsyn rajoitus

PCI DSS vaatii lisäksi arkaluonteiseen tietoon pääsyn rajaamista. Pääsy tulee sallia vain niille henkilöille, jotka tarvitsevat tietoa välttämättä työ-

tehtäviensä suorittamiseksi ja vain niiltä osin kuin se on tarpeellista. Eli pääsy tulee estää muilta ja tietoihin pääsy rajataan mahdollisimman pieneksi. Pääsynhallinta tulee toteuttaa myös kaikissa järjestelmäkomponenteissa.

Käyttöoikeudet, joilla tietoihin päästään, myönnetään yksittäiselle henkilölle työn luokituksen ja työtehtävien mukaan ja kaikkiin oikeuksiin tulee olla päättävän tahon kirjallinen valtuutus, jossa kaikki tarvittavat oikeudet ovat lueteltuna. Pääsyn jatkuvan seurannan ja hallinnan takaamiseksi pääsynhallinta tulee toteuttaa automatisoidulla järjestelmällä. (PCI DSS 2.0:2010, 44-45.)

3.4.2 Yksilöllinen käyttäjätunnus

Jokaisella käyttäjällä tulee olla yksilöllinen tunnus ennen pääsyä järjestelmäkomponentteihin tai kortinhaltijatietoihin. Näin kaikki järjestelmässä tehdyt toimet voidaan yhdistää tiettyyn henkilöön sekä voidaan varmistaa, että vain tunnetut ja valtuutetut pääsevät käsittelemään kriittistä dataa.

Käyttäjää tunnistaessa tulee käyttäjätunnuksen lisäksi käyttää vähintään yhtä seuraavista tunnistusmenetelmistä: salasana, tunnistuslaite, älykortti tai biometrinen tunnistus. Etäyhteyttä käytettäessä tunnistamiseen tulee käyttää "kahden tekijän" tunnistamista eli vähintään kahta yllämainituista.

Kaikki järjestelmässä käytettävät salasanat tulee suojata lähetyksen ja säilömisen aikana, jotta salasanojen leviäminen ja väärinkäyttö estetään. Salasanat tulee olla lukemattomissa ja vahvasti salattuja. Lisäksi palveluntarjoaja vastaa asiakkaiden salasanojen suojauksesta.

Yksilöllisestä kirjautumisesta saadaan kiistattomat hyödyt ainoastaan jos käyttäjäoikeuksien tunnistamisen ja todennuksien hallinta on toteutettu riittävällä tasolla. PCI DSS -standardi esittää näille hallintatoimille hyvin yksityiskohtaiset määritteet vaatimuksessa 8.5. Nämä pitävät sisällään tarkat vaatimukset salasanoista sekä käyttäjätunnusten ja todennustietojen poistoon, lisäämiseen ja muutoksiin, ei-aktiivisten käyttäjätilien poistoon, tunnuksen lukitukseen ja yhteyden aikakatkaisuun liittyen. (PCI DSS 2.0:2010, 46-50.)

3.4.3 Fyysisen pääsyn rajoittaminen

Standardi määrittää myös, että fyysistä pääsyä korttimaksutietoihin ja niitä käsitteleviin järjestelmiin tulee rajoittaa ja valvoa. Tietoturvan kannalta myös fyysinen pääsy kortinhaltijoiden tietoihin tulee ottaa huomioon. Standardi vaatiikin fyysisen pääsyn rajoittamista ja valvomista.

It-alalla tietoturvaa pohdittaessa useimmiten ajatellaan ohjelmistojen tai verkkojen kautta tehtyjä hyökkäyksiä, vaikka fyysinen tietoturva on yhtä tärkeää, ellei jopa tärkeämpää. Mietitään tilannetta, jossa kaikki tiedot ovat tallennettuina esimerkiksi palvelin-PC:lle, ja konetta säilytetään turvaamattomassa paikassa, josta sen voi helposti viedä. Koneesta voi saada hyvin paljon tietoja käsiinsä, eikä suojausmenetelmiä voida välttämättä enää

jälkikäteen tehdä, jos konetta ei liitetä verkkoon. Fyysisessä tietoturvassa tietokoneiden lisäksi esimerkiksi paperitulosteiden ja muiden tallennusmedioiden säilytys ja näiden sisältämien tietojen tuhoaminen tulee ottaa huomioon.

Standardissa määritetään, että kaikki pääsy suoraan kortinhaltijoiden tietoihin tai niitä sisältävään järjestelmään tulee olla tarkasti rajattu. Näin pyritään välttämään luvattomat pääsyt tietoihin ja järjestelmiin sekä näiden luvattomat poistot.

Yrityksessä tulee käyttää kulunhallintaa tietokone- ja tietokeskuksiin sekä muihin tiloihin, joissa käsitellään kortinhaltijoiden tietoja. Kulkua tulee valvoa kulkukortinlukijoilla ja pitämällä tilat lukittuina.

Korkeaan tietoturvaan luettavilla alueilla, kuten tietokeskukset, palvelinhuoneet tai muut tilat joissa on järjestelmiä, jotka prosessoivat tai lähettävät kortinhaltijoiden tietoa, kulkua tulee lisäksi valvoa kameroilla tai muilla pääsynhallintamekanismeilla. Kulunhallintatietoja tulee tallentaa ja säilyttää vähintään kolme kuukautta tai lain sallimissa määrin. Näistä kulunvalvontamekanismeista tulee lisäksi varmistaa, ettei niitä voida luvattomasti kytkeä pois tai niiden toimintaa muuttaa.

Fyysiseen tietoturvaan lasketaan myös verkkolaitteisiin pääsyn rajoittaminen. Pääsyä avoimiin verkkoliittimiin tulee rajoittaa ja ainoastaan tarvittavat liitännät on aktivoituna käyttöön työntekijöille. Jos tiloissa on avoimia liittimiä, vieraat eivät saa liikkua tiloissa yksin. Myös pääsyä WLAN-verkkojen fyysisiin laitteisiin tulee rajoittaa, esimerkiksi reitittimiin ja muihin verkkoliikennettä jakaviin laitteisiin sekä liitäntöihin.

Vierailijat ja organisaation henkilöstö tulee olla selkeästi erotettavissa toisistaan henkilökorteilla, jossa näkyy henkilön nimi ja edustettava yritys. Kaikille vierailijoille tarjotuille tunnistusmenetelmille, kuten henkilökorteille, tulee määrittää voimassaoloaika jonka pituus on vain tarvittavan määrän. Kortit tulee ottaa haltuun vierailta yrityksen tiloista poistuttaessa tai niiden vanhentuessa.

Organisaation tiloissa käyneistä vierailijoista tulee ylläpitää listaa, josta ilmenee vierailijan nimi, edustettu yritys sekä vierailijan valtuuttaman henkilöstön jäsenen nimi. Näitä tietoja tulee säilyttää vähintään kolme kuukautta, ellei laki muutoin rajoita. Listaan tulee tallettaa tiedot myös mahdollisista käynneistä tietokonetiloissa sekä tietokeskuksissa, joissa kortinhaltijoiden tietoja käsitellään. Lisäksi tulee huomata, ettei vierailijantunnisteella tule olla ilman saattajaa pääsyä tiloihin, joissa kortinhaltijoiden tietoja ylläpidetään tai käsitellään.

Standardi määrittää erinäisiä turvallisuustoimia käytettäessä fyysisiä tallennusmedioita. Näitä voi tässä yhteydessä olla esimerkiksi paperitulosteet, ulkoiset kovalevyt ja muistitikut. Mahdolliset varmuuskopiot ja muut arkaluonteista tietoa sisältävät mediat on säilytettävä suojatussa tilassa mieluiten eriytettynä yrityksen päätoimitiloista ja ne tulee inventoida vähintään vuosittain. Lisäksi tallennusmedioiden sisäistä ja ulkoista jakelua tulee rajoittaa. Lisäksi sisällön arkaluonteisuus tulee luokitella, jotta pysty-

tään helposti määrittämään tarvittavat suojaustoimenpiteet esimerkiksi tallennusmedioiden kuljetuksen aikana. Arkaluonteista tietoa sisältävien medioiden kuljetukset tuleekin suorittaa turvatusti sekä kaikkiin kuljetuksiin vaaditaan perusteltu syy sekä johdon hyväksyntä.

Kun tallennusmediaa ei enää tarvita liiketoiminnallisista tai lain vaatimista syistä, tulee se asianmukaisesti tuhota. Paperitulosteet tulee tuhota niin, ettei kortinhaltijoiden tietoja pystytä niistä enää palauttamaan. Paperit voidaan tuhota joko silppuamalla, on huomattava kuitenkin, että silppurin pitää silputa paperit myös poikittain eikä vain pituussuunnassa, tai polttamalla. Lisäksi tuhottavaksi menevät materiaalit tulee säilyttää suojattuna, esimerkiksi lukittuna kaapissa. Sähköisellä medialla olevat tiedot tulee käsitellä lukemattomaksi, niin ettei tietoja pystytä palauttamaan. Tähän on olemassa erilaisia ohjelmia, jotka ylikirjoittavat kaikki tiedot kovalevyllä niin ettei niitä pystytä palauttamaan ohjelmallisesti. Media voidaan myös fyysisesti tuhota, esimerkiksi kiintolevyjen magneettisella tuhoamisella. (PCI DSS 2.0:2010, 51-54.)

3.5 Verkon valvonta

Fyysisen tietoturvan lisäksi myös verkon kautta tapahtuvaa pääsyä kortinhaltijoiden tietoihin ja niitä käsitteleviin ympäristöihin tulee seurata ja monitoroida. Seuranta ja monitorointi perustuvat pääosin tapahtumien kirjaamisesta lokiin ja muihin mekanismeihin, jotka tallentavat käyttäjien verkossa tekemiä toimia.

Lokien ja seurannan avulla pystytään mahdollisiin tietomurtoihin valmistautumaan. Näiden avulla mahdollisia tietomurtoja pystytään havaitsemaan, ehkäisemään sekä varautumaan niiden aiheuttamiin vahinkoihin. Tarpeellisella tasolla olevat lokitiedostot mahdollistavat esimerkiksi tapahtumien tarkan seurannan, hälytysmekanismit sekä analyysin, kun tietomurto tai muu vahinko on sattunut.

3.5.1 Verkkoliikenteen valvonta

Kaikkiin järjestelmäkomponentteihin liittyvät toimet tulee olla yhdistettävissä tiettyyn käyttäjään, jotta mahdolliset väärinkäytökset pystytään välttämään. Jotta edellä mainittu olisi mahdollista, vaatii standardi automatisoitujen prosessien käyttöä pääsytietojen tallentamisessa. Näistä tiedoista tulee ilmetä kaikki pääsyt kortinhaltijoiden tietoihin, järjestelmänylläpitäjän tunnuksilla tehdyt toimet, pääsytietojen käsittely, epäonnistuneet kirjautumisyritykset sekä yhteydessä käytetyt käyttäjän tunnistamis- ja todentamismenetelmät.

Jotta verkon kautta tehtyjä tapahtumia pystytään tarkasti seuraamaan ja monitoroimaan tulee varmistaa, että lokien aikaleimat ovat oikeelliset ja yhdenmukaiset. Standardi vaatii ajan synkronointia eri järjestelmän osien välillä. Tähän voidaan käyttää esimerkiksi NTP:tä ”Network Time Protocol”. Kaikilla kriittisillä järjestelmillä tulee olla oikea ja johdonmukainen aika ja aikadatan tulee olla suojattu, niin ettei sitä pystytä vahingonteon

tarkoituksessa muuttamaan. Kaikki saatu aikadata tulee olla saatuna luotettavasta lähteestä.

Pääsynhallintatietojen tulee olla suojattuna, ettei niitä pystytä muokkaamaan esimerkiksi tapahtumia peittääkseen. Niihin pääsy tulee olla rajattu, niiden muokkaaminen tulee olla estetty ilman valtuuksia sekä niistä tulee olla varmuuskopiot.

Järjestelmäkomponenttien lokeja tulee seurata päivittäin, sisältäen vähintään kriittisimmät toiminnot. Katselmoinnin tulee sisältää tietoturvatoimia suorittavien palvelimien lokitiedostojen tarkastus. Katselmoinnissa voidaan käyttää avuksi myös ohjelmallisia ratkaisuja. Järjestelmäkomponentteihin liittyviä lokeja tulee säilyttää vähintään vuoden ja vähintään kolmen kuukauden lokit tulee olla saatavissa välittömästi mahdollisia analyysejä varten. (PCI DSS 2.0:2010, 55-58.)

3.5.2 Suojausmenetelmien säännöllinen testaus

Verkkoon liittyviä suojamenetelmiä on tärkeää testata säännöllisesti mahdollisten haavoittuvuuksien ja puutteiden havaitsemiseksi. Tutkijat ja haittaa tahtovat henkilöt löytävät jatkuvasti haavoittuvuuksia ohjelmistoista. Näitä löytyy myös uusista ohjelmistoista, joissa kaikkia tietoturvaan liittyviä kohteita ei ole vielä pystytty ottamaan huomioon tai ohjelmiston käytöstä ei vielä ole riittävää määrää tietoa. Tästä syystä onkin ensiarvoisen tärkeää jatkuvasti seurata ja tutkia järjestelmäkomponentteja, prosesseja sekä räätälöityjä ohjelmistoja, jotta kaikki mahdolliset haavoittuvuudet havaitaan ja pystytään kehittymään muuttuvassa ympäristössä tietoturvan kannalta.

Yleisesti WLAN- eli langattomia verkkoja pidetään haavoittuvampina, kuin langallisia, koska ne kattavat laajemman alueen ja ovat helpommin saavutettavissa, kun fyysistä liitäntää ei tarvita. Tästä syystä langattomien verkkojen liityntäpisteet tulee testata ja kartoittaa neljännesvuosittain mahdollisten luvattomien pisteiden havaitsemiseksi.

Sisä- ja ulkoverkkojen haavoittavuustarkastukset on tehtävä vähintään neljännesvuosittain ja merkittävien muutosten jälkeen. Näitä muutoksia ovat esimerkiksi järjestelmäkomponenttien vaihdot, verkon loogisen rakenteen muutokset, palomuurisäädösten muutokset ja laitteistojen päivitykset. Organisaation henkilöstö voi suorittaa muutosten jälkeiset tarkastukset.

Pätevän tahon tulee suorittaa sisäisten verkkojen tarkastukset. Tämä voi olla joko yrityksen sisäinen taho tai kolmas osapuoli. Sisäisissä tarkastuksissa havaitut vakavat uhat tulee olla ratkaistuna ennen PCI DSS:n auditoinnin hyväksymistä.

Ulkoisten verkkojen haavoittuvuustarkastuksissa tulee käyttää PCI SSC:n hyväksymää tarkastajaa. Tarkastuksessa ei saa ilmetä yli CVSS:n 4-tason vakavuuden haavoittuvuuksia.

Verkon murtautumistestit tulee suorittaa ulko- ja sisäverkoilla vähintään vuosittain ja suurien muutosten jälkeen. Näissä tulee testata verkkokerrosten, eli verkkoon liittyvien komponenttien ja käyttöjärjestelmien, sekä ohjelmistokerrosten, eli ympäristössä olevien ohjelmistojen kautta mahdollisia, murtautumisia. Näillä varmistetaan mahdolliset aukot verkon suojauksissa, jotka mahdollistavat murtautumisen organisaation verkkoihin. Nämä tietoturva-aukot tulee olla paikattuna ja korjaukset testattu hyväksytysti ennen auditoinnin hyväksyntää.

Kaikkea kortinhaltijoiden tietoihin liittyvää verkkoliikennettä tulee lisäksi valvoa tunkeutumista estävillä ja havaitsevilla järjestelmillä. Järjestelmän tulee lisäksi ilmoittaa henkilöstölle mahdollisista tietomurtoepäilyistä, jotta toimenpiteet voidaan aloittaa viipymättä.

Tiedostojen eheyttä tulee edellisten lisäksi seurata niille suunnatuilla ohjelmistoilla. Näiden tulee lähettää varoitus havaituista luvattomista muokkauksista järjestelmäasetus- ja sisältötiedostoissa. Ohjelmiston tulee suorittaa myös viikoittainen laajempi tiedostojen vertailu muutosten havaitsemiseksi. Yleensä kriittisiksi luetut tiedostot eivät muutu usein, eli niiden muokkaaminen voi olla merkki tietomurrosta. Ohjelmistoihin on yleensä määritetty jo oletuksena käyttöjärjestelmän kriittiset tiedostot. Kauppiaan tai palveluntarjoajan tulee arvioida ja määrittää muut kriittiset tiedostot tapauskohtaisesti. (PCI DSS 2.0:2010, 59-63.)

3.6 Tietoturvakäytänteet

Vahvat tietoturvakäytännöt vaikuttavat suurelta osin koko yrityksen asenteeseen tietoturvaa kohtaan ja samalla selventävät henkilöstölle mitä heiltä odotetaan. Koko henkilöstön tulisi olla tietoinen käsittelemiensä tietojen arkaluonteisuudesta sekä tiedostaa heidän vastuunsa näiden suojaamisessa.

Standardi vaatii tietoturvakäytänteiden kehittämistä ja niiden noudattamista. Näissä tulee ottaa huomioon se, että kaikkia PCI DSS:n vaatimuksia noudatetaan sekä niihin kuuluu vuosittaiset riskien ja uhkien tunnistamiset ja näiden pohjalta tehtävä riskienhallinta-analyysi. Tietoturvakäytänteet tulee katsoa vähintään vuosittain tai kun ympäristöön tulee muutoksia. Näissä tulee määrittää kaikki tietoturvaan liittyvät toimet ja rutiinit, myös päivittäisellä tasolla. Päivittäisiin rutiineihin kuuluu esimerkiksi järjestelmän ylläpitotoimet, käyttäjien hallinta, lokien seuranta ja tarkkailu.

Kaikkien kriittisiksi luettujen teknologioiden, kuten etäyhteystyökalujen, langattomien verkkojen, kannettavien tietokoneiden ja sähköpostin käyttöön tulee määritellä omat käytänteet, joissa varmistetaan näiden oikeanlainen ja turvallinen käyttö. Näihin kuuluu esimerkiksi käytön valtuutus, käyttäjien tunnistaminen, sallitut käyttötarkoitukset, käyttöoikeudet vain liiketoiminnan kannalta tarvituksi ajaksi sekä selvitys kaikista laitteista ja niiden käyttäjistä.

Tietoturvakäytänteiden eri osa-alueisiin ja näiden suorittamiseen tulee määrittää vastuussa oleva henkilö tai ryhmä. Näin pystytään paremmin takaamaan, että jokainen osa-alue on otettu huomioon ja pystytään pitämään

ajan tasalla. Osa-alueita, joilla täytyy standardin mukaan olla virallisesti nimetty vastaava, ovat tietoturvakäytänteiden dokumentointi ja jakelu henkilöstölle, tietoturvahälytysten analysointi sekä asiaankuuluvien henkilöiden tiedottaminen, toimintasuunnitelman muodostaminen ja päivittäminen tietomurtojen ja -hyökkäyksien varalta, käyttäjienhallinta sekä kaiken tiedon käsittelyn hallinta ja seuranta.

Kaikki mahdolliset palkattavat henkilöt tulee tarkastaa ennen palkkausta, jotta mahdollisia riskejä sisäisiin hyökkäyksiin voidaan pienentää. Tähän voi kuulua esimerkiksi edellisten työnantajien, rikosrekisterin, luottotietojen sekä suosittelijoiden tarkastaminen.

Jos kortinhaltijoiden tietoja jaetaan palveluntarjoajien kanssa, tulee organisaation varmistaa, että palveluntarjoaja vastaa osaltaan käsittelemiensä tietojen turvallisuudesta. Palveluntarjoajien vastuusta tietojen turvaamisen suhteen tulee olla kirjallinen sopimus, jotta kaikki vaadittavat toimet ovat selkeästi määritetty ja niitä noudatetaan. Ennen yhteistyönaloittamista tulee organisaation varmistaa palveluntarjoajan luottamuksellisuus ja yhteistyön aikana tulee lisäksi seurata näiden PCI DSS mukaisuutta vuosittain. Organisaation tulee myös ylläpitää listaa kaikista käyttämistään palveluntarjoajista.

Tietoturvakäytänteisiin kuuluu lisäksi suunnitelma tietomurtojen varalta. Tässä tulee ilmetä roolit, vastuut, yhteydenpitostrategiat sekä maksukorttiyhtiöiden tiedottaminen tietomurron sattuessa.

Kokonaisuudessaan suunnitelmaan kuuluu siis tarkat toimet tietomurron sattuessa sekä liiketoiminnan palauttamis- ja jatkuvuustoiminnot. Suunnitelmaan tulee myös sisältyä tietojen varmuuskopiointikäytänteet sekä lain vaatima analysointi sattuneista välikohtauksista. Suunnitelmassa tulee huomioida maksukorttiyhtiöiden toimintamallit ja näitä käytetäänkin joko pohjana tai sisällytetään muuten yrityksen omiin toimintamalleihin. Suunnitelma tulee lisäksi testata ja käydä läpi vähintään vuosittain, mahdollisten puutteiden ja muuttuneiden tarpeiden havaitsemiseksi ja päivittää tarvittaessa siihen kehitettyä päivittämisprosessia käyttäen.

Henkilöstö tulee kouluttaa uhkia vastaan säännöllisesti sekä tehtävään määritettyjen henkilöiden tulee olla ympärivuorokautisesti valmiita reagoimaan tuleviin tietoturvahälytyksiin. Hälytyksiä tule muodostua tunkeutumisen tunnistamisesta ja estämisestä sekä tiedostojen eheyden valvontajärjestelmiltä. (PCI DSS 2.0:2010, 64-69.)

4 SIIRTYMINEN PCI DSS:N MUKAISUUTEEN

PCI DSS -standardilla ei ole varsinaista edeltäjää. Kyseessä on pitkään odotettu standardi, joka tarjoaa tarkat pelisäännöt kortilla maksamiseen liittyvien tietojen suojaamiseen ja siihen liittyviin tietoturvatoimiin. Aikaisemmin käytössä ovat olleet lähinnä yhteiset periaatteet ja väärinkäytöistä määritetyt sakot sekä korvausvaateet jos kortinhaltijoiden tietoja on laiminlyöty. Standardilla pyritään siihen, että tiedot on mahdollisimman hyvin suojattu, että maksaminen kortilla on täysin turvallista ja tietovuodoilta vältytään täysin. Tämä tukee myös kauppiaita ja palveluntarjoajia, jos tietomurto sattuu, kun PCI DSS:ää noudatetaan täysin, he eivät ole korvausvelvollisia.

Standardi asettaa paljon vaatimuksia toimijoille, mutta samalla tuo turvaa sitä noudattaville yrityksille ja kaikille korttimaksuja käyttäville. Standardin laajuuden vuoksi yrityksen kannattaa varata siirtymäaikaan vähintään puoli vuotta. Lisäksi tulee huomata, että vaatimusten ylläpitoon tullaan vaatimaan aktiivista työtä myös siirtymäajan jälkeen. Standardiin panostaminen ja sen noudattaminen on kaikkien toimijoiden etu.

4.1 Siirtymävaihe ja sen suunnittelu

PCI DSS -standardi on ensimmäinen laatuaan, joten muutoksia ja tarkennuksia tulee jatkuvasti. Tällä hetkellä voimassa oleva versio on 2.0, kun edeltävä 1.0 on vuodelta 2008. Standardi tulee luultavasti kehittymään ja tarkentumaan eikä siirtyminen välttämättä tapahdu vielä standardin versiossa 2.0, joten yritysten kannattaa odottaa vakaampaa versiota ennen standardin käyttöönottoa kokonaisuudessaan. Kaikki osa-alueet voidaan tällöin tehdä standardin mukaisiksi siirtymävaiheen aikana ilman riskiä laitehankintojen, ohjelmistojen tai muiden organisaatiossa tehtävienmuutoksien uusimisesta. (Mäkelä, haastattelu 2.4.2012; Kopponen, haastattelu 27.3.2012.)

Yrityksen kannattaa kuitenkin ottaa standardiin siirtyminen mahdollisuuksien sallimissa määrin huomioon uusissa projekteissa, laitehankinnoissa sekä tilojen suunnittelussa. Esimerkiksi uusien laitteiden tulisi olla kykeneväisiä toimimaan PCI DSS:n alaisuudessa tai tukemaan näitä vaativia asetuksia ja ohjelmia. Organisaatioiden tilojen tulee olla turvattu, ettei tiloissa pääse liikkumaan ilman tarvittavia avaimia tai kulkukortteja, eikä kehitys- ja ylläpitopuolilla tule olla pääsyä toistensa tiloihin. Nämä voidaan ottaa huomioon yritysten tiloja valitessa, esimerkiksi ottamalla yrityksen käyttöön toimisto, jossa tiloja on mahdollista sulkea toisistaan lukollisilla ovilla ja valmius lisätä kulunvalvontajärjestelmiä.

Itse siirtymävaiheessa yrityksen olisi kannattavaa nimittää vastaava PCI DSS:n vaatimuksien mukaisuuden tarkastamiseen ja vaatimuksien kartoittamiseen. Standardiin siirtyminen on laaja prosessi, joka vie helposti puolikin vuotta. Standardiin ja sen vaatimuksiin perehtymiseen olisi hyvä nimetä yksittäinen työntekijä tai työryhmä, jotta kokonaisuus saadaan kattavasti käsiteltyä. Toimintasuunnitelman laatiminen ja eri osa-alueille vas-

tuuhenkilön määrittäminen toisi lisäksi varmuutta siitä, että kaikki osa-alueet otetaan siirtymävaiheessa huomioon.

Organisaation kannattaa suorittaa aluksi itsearviointi standardin mukaisuudestaan, jonka jälkeen tehdään suunnitelmallisesti tarvittavia muutoksia ja korjauksia. Näiden aikana voidaan konsultoida auditoijaa, joka pystyy opastamaan standardin vaatimuksissa. Auditointi tulisi suorittaa vasta, kun edellä mainituin toimin ympäristö on saatu standardin vaatimalle tasolle. Tähän voi sisältyä organisaation sisäisesti tekemä tarkastus. Näin pystytään pienentämään tarvittavien tarkastusten määrää, sillä auditointi tulee suorittaa uudelleen jos vakavia puutteita tai ongelmia löytyy.

Koska henkilöstö on hyvin suuressa osassa standardin noudattamisessa, tulee henkilöstö pitää ajan tasalla siirtymän eri vaiheissa. Tämä voidaan toteuttaa palaverein ja koulutuksin. Näin varmistetaan, että kaikki ovat tietoisia tulevista muutoksista ja heille asetetuista odotuksista ja vastuista. Samalla pystytään myös varmistumaan, että työskentelytavat päivittyvät tietoturvatarpeita vastaaviksi.

4.2 Siirtymävaihe Eatech Oy:n kannalta

Eatech Oy toimii kortinhaltijatietojen käsittelyssä palveluntarjoajan roolissa. Yritys kehittää kortilla maksamiseen liittyviä ohjelmistoja sekä tarjoaa näihin liittyviä ylläpitopalveluita. Tässä perehdytään PCI DSS:n vaatimuksiin järjestelmien ylläpidollisten toimien kannalta. Koska Eatech Oy:n asiakassuhteet ovat pääosin salassapitovelvollisuuden alaisia, käsitellään tässä standardin "vaatimia" toimintamalleja yleisesti, asiakkaasta riippumattomina.

Eatech:n olisi hyvä tehdä kartoitus asiakaskohtaisista vaatimuksista ja tarpeista tietoturvan suhteen, johon liittyy selvitys asiakasympäristöissä liikkuvien tietojen arkaluonteisuudesta. Tämän kartoituksen perusteella suunnitellaan tarkat toimintamallit asiakkaan ympäristössä toimimiselle. Tähän liittyvät turvatut etähallintatyökalut ja muut etäyhteysvälineet, käyttäjätunnukset, tietojen käyttö, turvallinen säilyttäminen sekä lähettäminen.

Yrityksen sisäiset verkko- ja laiteratkaisut tulee myös tarkistaa ja arvioida sekä uusia tarvittaessa. Verkon tulee olla rajattu, luotettava sekä laitteiden mahdollistettava kaikki vaadittavat turva-ratkaisut.

Palomuurien- ja virustorjunnan tulee olla kunnossa. Eatech:lla onkin käytössään jo yhtenäinen, palvelimella hallittava virus- ja palomuuriohjelmisto. Näiden asetukset ja määritykset tulee vielä tarkistaa, tarkentaa ja dokumentoida. Lisäksi tulee huomioida, että peruskäyttäjän, eli tässä yhteydessä organisaation henkilöstön, ei tule pystyä ottamaan ohjelmistoja pois käytöstä.

Käyttäjienhallinta on jo käytössä, mutta tätä ja tähän liittyviä toimia pitää lisäksi tarkentaa. Lisäksi olisi hyvä virallisesti nimittää henkilö, joka hallinnoi kaikkia käyttäjien lisäämiseen, muokkaamiseen ja poistamiseen sekä käyttöoikeuksien hallintaan liittyviä toimia. Tähän liittyy myös tilojen

fyysinen rajoittaminen. Tällä hetkellä yrityksellä on jo kehitys- ja ylläpitotilat erillään, mutta tilat on lukittava. Myös vierailijoiden liikkumisessa tiloissa tulee luoda tarkat käytänteet. Vierailijoista tulee tallentaa tiedot vierailijalokiin sekä määrittää henkilöstön jäsen, joka vastaa vierailijan toimista sekä tarvittaessa saattaa tiloissa.

Kaikkea verkkoliikennettä ja käyttäjien toimia tulee valvoa ja suositeltavaa olisi automaattisen ohjelmiston implementointi, joka luo tarvittavat varoitukset ja ilmoitukset verkosta ja käyttäjistä vastaaville henkilöille, joten toimiin pystytään tarvittaessa ryhtymään.

Viimeisenä osa-alueena ovat tarkat tietoturvakäytänteet koko yritykselle. Nämä tulee myös dokumentoida ja määrittää yksiselitteisesti. Organisaation henkilöstölle tulee muodostaa ohjelma, jossa käytänteet ja sille asetetut vaatimukset selvitetään henkilöstölle ja tietämystä pidetään yllä. Myös vaadittavat salassapitosopimukset ja muut kirjalliset vaatimukset tulee pitää ajan tasalla ja allekirjoittaa tietyin väliajoin.

5 YHTEENVETO

PCI DSS on ensimmäinen laajasti käytössä oleva standardi korttimaksujen tietoturvaan liittyen. Tällä hetkellä käytössä oleva versio on 2.0 ja muutoksia ja parannuksia saattaa vielä olla tulossa. Kun standardista on saatu vakaa versio, tulee se tarjoamaan tarkat pelisäännöt kaikille korttimaksuihin liittyville toimijoille parantaen huomattavasti korttimaksujen turvallisuutta.

Luvussa kaksi on käyty standardi läpi yleisellä tasolla, jotta lukija pystyy paremmin hahmottamaan mistä työssä käsiteltävässä PCI DSS -standardissa on kyse. Luvussa 3 käytiin tarkemmin läpi kaikki standardin vaatimusluokat sekä niihin kuuluvat vaatimukset. Näihin sisältyy vaatimukset turvallisesta verkosta, korttimaksuihin liittyvien tietojen turvaamisesta, haavoittuvuuksilta suojautumisesta, käyttäjien hallinnasta, verkon valvonnasta sekä henkilöstölle määritettävistä tietoturvakäytänteistä.

Työn tavoitteena oli löytää vastaukset tutkintakysymyksiin: Mitä PCI DSS -standardi sisältää? Miten standardin alaisuus voitaisiin saavuttaa? Työssä pystyttiin vastamaan ensimmäiseen tutkintakysymykseen hyvin. Standardi pystyttiin käymään hyvin läpi PCI DSS:n dokumentaation pohjalta sekä saaden helposti hahmotettava kokonaisuus asiaan perehtymättömälle, jonka kaikki henkilöstön jäsenet voivat lukea. Standardin laajuuden vuoksi työn aikana rajaus muuttui toisen tutkintakysymyksen osalta. Työn toimeksiantajan ja työn tekijän toimesta päädyttiin työstä tekemään pohjustus standardin mukaisuuteen siirtymisestä palveluntarjoajan kannalta tarkkojen toimintamallien sijaan. Itse siirtymävaihe ja standardin tarkkojen toimintamallien luonti vaatisi jopa vuoden työpanoksen ja salassapidon alaisien asioiden läpikäymisen, joten tämän rajaus työn ulkopuolelle oli mielekäs. Tämän rajauksen puitteissa saatiin työssä vastattua myös toiseen tutkintakysymykseen.

Työn tuloksena tilaaja saa tiiviin paketin standardista, jota tullaan käyttämään henkilöstön perehdyttämisessä standardiin ja joka tulee olemaan vapaasti organisaation jäsenten luettavissa. Työn tekijänä sain työstä myös välittömän hyödyn, sillä standardi ei ollut itselleni ennestään tuttu ja standardi tulee olemaan jatkossa vahvasti mukana työtehtävissäni. Työtä voidaan myös käyttää apuna standardiin siirtymistä suunniteltaessa.

LÄHTEET

Kopponen, A. 2012. Projektijohtaja. Eatech Oy. Haastattelu 27.03.2012.

Luottokunta Oy. 2010. PCI DSS Lyhyesti. Viitattu 9.4.2012.
Saatavilla:
http://www.luottokunta.fi/fi/toimialatietoa/pci_standardit/pci_dss_lyhyesti

Mäkelä, E. 2012. Toimitusjohtaja. Eatech Oy. Haastattelu 2.4.2012.

PCI Security Standards Council, PCI DSS -standardi 2.0. 2010.Viitattu 01.02.2012. Saatavilla:
https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

PCI Security Standards Council, PA DSS-standardi 2.0. 2010. Viitattu 01.04.2012. Saatavilla:
https://www.pcisecuritystandards.org/documents/pa-dss_v2.pdf

TechRepublic. 2005. SolutionBase: Strengthen network defenses by using a DMZ, viitattu 9.4.2012
Saatavilla:
http://www.techrepublic.com/article/solutionbase-strengthen-network-defenses-by-using-a-dmz/5756029

Virustorjuntaa.fi. 2009. Virustorjuntaohjelmat, viitattu 20.3.2012
Saatavilla:
http://www.virustorjuntaa.fi/