Aleksi Alppi

PCI-standardin kohdentaminen Indoor Groupin tarpeisiin

Opinnäytetyö

Syksy 2009

Liiketalouden, yrittäjyyden ja ravitsemisalan yksikkö

Pienen ja keskisuuren yritystoiminnan liikkeenjohdon koulutusohjelma

Tuotantotalous

Seinäjoen ammattikorkeakoulu
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Liiketalouden, yrittäjyyden ja ravitsemisalan yksikkö
Koulutusohjelma: Pienen ja keskisuuren yritystoiminnan liikkeenjohdon
Suuntautumisvaihtoehto: Tuotantotalous

Tekijä: Aleksi Alppi

Työn nimi: PCI-standardin kohdentaminen Indoor Groupin tarpeisiin

Ohjaaja: Jorma Imppola

Vuosi: 2009 Sivumäärä: 55 Liitteiden lukumäärä: 26

Tämän opinnäytetyön tutkimuskohteena on PCI-standardi. Se on suurimpien luottokorttiyhtiöiden tekemä ohjeistus yritysten tietoturvallisuuden vähimmäistasosta. Sen tarkoituksena on suojata kortinhaltijoiden tiedot parhaalla mahdollisella tavalla sekä nostaa yritysten tietoturvallisuustasoa. Kaikkien yritysten, jotka vastaanottavat, välittävät ja tallentavat luottokorttikorttitapahtumia, tulee noudattaa PCI-standardia.

Työn tarkoituksena oli luoda kohdennettu tietoturvastandardi Indoor Groupin tarpeisiin. Työ toteutettiin toiminnallisena opinnäytetyönä, jonka lopputuloksena saatiin uudelleen järjestetty ja tulkittu standardi. Se toimii standardin hakemisen työkaluna ja helpottaa kokonaisprosessia. Kohdennetulle standardille todettiin olevan käyttöä, koska vanhassa standardissa oli paljon tulkinnanvaraisia vaatimuksia sekä sen järjestyksen koettiin heikentävän hakuprosessin etenemistä ja aikatauluttamista.

Työssä tutustutaan aikaisempiin standardeihin sekä perehdytään PCI-standardiin. Käytännönläheistä tietoa asiasta saatiin haastattelujen ja yritysvierailujen yhteydessä Indoor Groupin yhteyshenkilöiltä. He kertoivat standardin hakuprosessistaan, sen tuottamista ongelmista ja antoivat niihin käytännön ratkaisumalleja. Näin vanhojen standardien ongelmakohdat löydettiin ja ne voitiin korjata uudessa mallissa.

Kohdennetun standardin etuina tutkija piti sen uutta toimivampaa järjestystä, jonka avulla siitä saatiin selkeämpi kokonaisuus. Uuden järjestyksen ansiosta standardin hakuprosessin etenemistä on helpompi seurata ja aikatauluttaa. Standardin uudessa tulkinnassa sen vaatimukset käännettiin suomeksi ja tulkinnanvaraisuuksia karsittiin, joka helpottaa sen sisällön ymmärtämistä.

Avainsanat: Tietoturva

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: Finnish School of SME Business Administration
Degree programme: SME Business Management
Specialisation: Production Economics

Author/s: Aleksi Alppi

Title of thesis: Targeting PCI-standard for Indoor Group needs

Supervisor(s): Jorma Imppola

Year: 2009 Number of pages:55 Number of appendices:26

The research subject of the present thesis is PCI-standard. PCI-standard defines minimum level of companies' information security and it gives the best possible protection for clients who use credit cards. Every company which receives, forwards and saves credit card transactions information must obey PCI-data security standard.

The aim of the present thesis was to create a modified PCI-standard for Indoor Group Company. The idea of the new standard was to support the application process of the standard and help to understand the main point of it. A company may find it easier to schedule the whole process with the modified standard. A new version of the standard was needed because there were many problems such as confusing content and poor interpretation in the existing version.

Information was collected from Indoor Group information security employees. They reported on practical methods of PCI-standard as well as problems encountered in the application process. That way the difficulties and the problems of PCI-standard were identified and dealt with in the new modified standard.

The advantages of the modified standard are practicality and a better context. With the help of a modified standard Indoor Group Company can save time and money when they are applying PCI-standard.

Keywords: Information security

SISÄLTÖ

Termit

DMZ:

(Demilitarized zone) Yrityksen tietoverkossa oleva kerros Internetin sekä yrityksen verkon välissä, jossa on arkaluontoista tietoa. Sen tarkoituksena on suojata yrityksen tietoa ja estää ulkopuolisia tunkeutumasta siihen.

Haavoittuvuus-skannaus:

Sillä pyritään löytämään verkon heikot kohdat, jotka aiheuttavat tietomurtoja. Sen avulla tarkistetaan myös verkkokomponenttien mahdolliset haavoittuvuudet.

Korttitietojen maskaus:

Maskaus on kortin numeroiden peittämistä siten, että kortteja ei pystytä käyttämään vääriin tarkoituksiin.

Kulun valvonta:

Ohjelma, joka rajaa tiedon saantia tai käsittelyä vain niille henkilöille, jotka ovat oikeutettuja käyttämään sitä.

Kortinhaltijoidentieto:

Kuvaa tietoa, jota luottokorteista on saatavilla. Kortin tunnistetiedot ovat kortinhaltijan nimi, voimassaoloaika sekä varmennusnumero.

Kortinhaltijoiden tiedon ympäristö:

Alue yritysten verkossa, jossa on arkaluontoista tietoa kuten kortinhaltijoiden tiedot.

PCI auditointi:

Tavoitteena on varmistaa, että asiakkaan järjestelmä vastaa PCI tietoturvastandardin vaatimuksia. Kuten rakentaa ja ylläpitää suojattua verkkoa, suojelee korttitietoja, ylläpitää haavoittuvuudenhallinnan ohjelmaa, toteuttaa vahvat pääsynhallintatoimenpiteet, monitoroi ja testaa verkot säännöllisesti ja ylläpitää tietoturvapolitiikkaa.

PCI PED:

(Payment Card Industry Pin Entry Device) hyväksyntä on tietoturvastandardi, joka koskee maksupäätettä. PCI-PED sertifiointi tehdään laitetoimittajan toimesta. (Korttimaksamisen turvastandardit [viitattu 21.10.2009].)

PA-DSS:

(Payment Application Data Security Standard) on tietoturvastandardi, joka koskee maksupääteohjelmistoa. Standardi on PCI Security Standards Councilin julkaisema. (Korttimaksamisen turvastandardit [viitattu 21.10.2009].)

PCI DSS:

(Payment Card Industry Data Security Standard) on kansainvälinen maksukorttialan tietoturvastandardi, jossa ovat mukana kaikki suuret luottokorttiyhtiöt kuten Visa, Master Card, American Express, JCB ja Discover Financial Services. (Korttimaksamisen turvastandardit [viitattu 21.10.2009].)

1 JOHDANTO

PCI-standardin kohdentaminen on toiminnallinen opinnäytetyö, jonka tarkoituksena on perehdyttää lukija nykyaikaiseen korttitietojen suojaamiseen. Työn lopputuloksena saadaan kohdennettu PCI-standardi kohdeyritys Indoor Groupin tarpeisiin. Kohdennettu standardi toimii yrityksen työkaluna PCI-standardi hakuprosessin eri vaiheissa ja sen tarkoituksena on helpottaa ja nopeuttaa sen edistymistä.

PCI-standardin tarkoitus on kiteyttää yrityksen tarvitsema tietoturvataso. Se sanelee tietoturvan vähimmäistason, joka yrityksen tulee saavuttaa. Tason mittaukseen yritykset voivat käyttää valtuutetun PCI-standardi toimijan tekemiä itsearviointilomakkeita. Tämän prosessin avulla yritys oppii ymmärtämään omaa tietoturvaansa laajemmin ja sen noudattaminen muodostuu osaksi arkipäivän rutiineja. Tämä on ainoa tapa ylläpitää vahvaa tietoturvaa, jota nykypäivän liiketoiminta vaatii. PCI-standardilla yritys saavuttaa myös imagollisia hyötyjä, koska vain harva yritys on saanut sen lunastettua Suomessa kuten HP, TeliaSonera sekä Screenway. (Lahti, [viitattu 16.11.2009]).

PCI-standardi on hyvin ajankohtainen aihe, koska tietomurtojen määrä on kasvanut räjähdysmäisesti viime vuosien aikana. Tästä esimerkkinä voidaan pitää Luottokunnan väärinkäyttötappioita, joista yli 70% on syntynyt väärennettyjen luottokorttien avulla. (Kallio, [viitattu 20.7.2009].) PCI-standardin hakeminen lähti Suomessa ja Euroopassa huonosti liikkeelle, mutta nyt asiaan on herätty ja monet yritykset ovat aloittaneet toiminnan sen eteenpäin viemiseksi. PCI-standardin hakuprosessin käynnistämiseen Suomessa on vaikuttanut Luottokunta. Se on asettanut vaatimuksia ja aikarajoja sen asiakkaina oleville yrityksille, jotta PCI-standardin hakeminen saadaan aluilleen. Mikäli yritykset eivät käynnistä sen hakemista, joutuvat he itse korvaamaan tietomurtojen aiheuttamat vahingot sekä pahimmassa tapauksessa purkamaan sopimuksensa Luottokunnan kanssa. Tämän ansiosta yritykset ovat vihdoin ottaneet PCI-standardin hakemisen vakavasti. (Siltala, viitattu 30.9.2009.)

1.1 Tutkimusongelma ja työn rajaus

Kyseessä on toiminnallinen opinnäytetyö, jonka tarkoituksena on tulkita ja kääntää suomeksi priorisoitu PCI-standardi 1.2. Ongelmana vanhassa PCI-standardissa tutkija koki sen vaikeaselkoisuuden ja tulkinnanvaraisuuden. Näihin asioihin kohdennetussa PCI-standardissa tehtin muutos, jonka ansiosta Indoor Groupin on helpompi jatkaa standardin hakemista tulevaisuudessa.

PCI-standardi sertifikaatin hakuprosessi olisi ollut aivan liian iso kokonaisuus opinnäytetyöaiheeksi, joten uuden priorisoidun standardin tulkitseminen suomeksi koettiin hyväksi ja riittäväksi rajaukseksi. Työ antaa sertifikaatin hakemiselle apuvälineet sekä yleiskäsityksen, kuinka se tulee suorittaa ja mitä asioita siihen kuuluu. Rajauksen suorittaminen on tehty opinnäytetyöohjaajan sekä Indoor Groupin yhteyshenkilöiden yhteisymmärryksellä.

1.2 Tutkimusmenetelmät

Tutkimusmenetelminä käytettiin keskusteluja Indoor Groupin yhteyshenkilöiden kanssa sähköpostin, puhelimen sekä yritysvierailujen yhteydessä. Tutkimuskohteena oli priorisoitu PCI-standardi 1.2, joka toimi myös toiminnallisen osuuden runkona. Myös aikaisempi standardi 1.1 oli käsittelyn kohteena, koska uusi standardi pohjautuu siihen suurelta osin.

Teoriaa PCI-standardista löytyi parhaiten Internetistä, koska aihe on hyvin uusi. Valtuutettujen PCI-standardi toimijoiden kotisivuilla oli runsaasti tietoa kyseisestä asiasta ja siksi kirjallisuuden puuttuminen ei haitannut teoriaosuuden tekemistä. Tietoturvallisuudesta löytyi hyvin aineistoa kirjallisuudesta. Teoksia löytyi niin suomeksi kuin englanniksikin.

2 PCI-STANDARDI

Luotto- ja maksukortteja koskevat tietoturvasuositukset ovat dokumentoitu PCI-standardissa. PCI on lyhenne englanninkielisestä sanasta Payment Card Industry. Niitä julkaisee PCI Security Standards Council, joka on suurimpien luottokorttiyhtiöiden perustama kuten American Express, Visa sekä MasterCard. (Hämäläinen 2009, 57.) Sen tarkoituksena on ohjata maksukorttien tili- ja tapahtumatietojen vastaanottamista, käsittelyä, tallentamista ja välittämistä. Standardia tulee noudattaa kaikkien, jotka vastaanottavat, välittävät tai tallentavat korttitapahtumia. (Luottokunta PCI-tietoturvastandardi, [viitattu 20.8.2009].)

PCI Council hallinnoi kolmea eri PCI-standardia. Ensimmäinen niistä on PCI PED, joka tulee sanoista Payment Card Industry Pin Entry Device. Sillä tarkoittaa laitetta, johon maksaessa syötetään neljä-numeroinen koodi. Tämän standardin avulla maksupäätteen turvallisuus voidaan taata. Toinen standardi on PA-DSS, joka on lyhenne sanoista Payment Application Data Security Standard. Tällä standardilla pyritään varmistamaan maksuohjelmiston turvallisuus ja turvatason riittävyys PCI-tietoturvastandardin täyttämiseksi. Kolmas Councilin myöntämä standardi on PCI DSS eli PCI Data Security Standard. Sillä taataan kokonaisten järjestelmien ja prosessien turvallisuus. (Nixu Web Journal, [viitattu 8.9.2009].)

PCI-standardin noudattaminen on jatkuvaa työtä, johon kuuluu kolme perusvaihetta. Ensimmäinen vaihe on tilanteen arviointi, jossa tietoturvataso määritellään. Toinen vaihe on tilanteen korjaaminen, jotta tietoturva kohoaisi ja kolmas vaihe on raportointi, joka suoritetaan valtuutetulle PCI-standardin valvojalle. (PCI Quick Reference Guide, [viitattu 20.8.2009].)

Suomen ensimmäinen PCI-standardin parissa toiminut yritys on Nixu, joka on perustettu 1988. Sen ydinosaamiseen voidaan lukea tietoturva ja tietoliikenneohjelmointi. Nixulla on Visan sekä MasterCardin hyväksyntä tehdä PCI-auditointeja sekä haavoittuvuusskannauksia. Sillä on meneillään useita auditointi ja kehittämisprojekteja PCI-standardin parissa. (Vehviläinen, [viitattu 20.8.2009].)

2.1 PCI-standardin tarkoitus

PCI-standardin tarkoitus on sanella vähimmäisvaatimukset korttidataan liittyville käytännöille, ohjelmistoille ja järjestelmille. Siinä on 12 pääkohtaa, jotka jakautuvat teknisiin sekä fyysisiin käytäntöihin. (Hämäläinen 2009, 57.)

1. Suojaa tiedot asentamalla palomuuriratkaisu ja ylläpitämällä sitä. Tämä on erityisen tärkeää, koska palomuurit valvovat yrityksen verkkoliikennettä. Niiden tarkoituksena on estää liikenne, joka ei täytä määriteltyjä turvakriteerejä. Kaikki järjestelmät tulee olla suojattu palomuureilla riippumatta siitä, mihin tarkoitukseen verkkoa käytetään. Tällä tavoin voidaan varmistaa, että yrityksen verkkoon ei ole mahdollisuuksia päästä.

2. Älä käytä ohjelmistotoimittajan määrittämiä oletussalasanoja tai muita tietoturva-asetuksia, koska ne ovat yleisessä tiedossa sekä helppo hankkia julkisista lähteistä. Salasanoja muuttamalla suojaustaso kasvaa ja sitä kautta verkkoon murtautuminen tehdään entistä vaikeammaksi.

3. Suojaa tallennetut kortinhaltijatiedot. Paras mahdollinen tapa suojata tiedot on olla dokumentoimatta niitä yrityksen tietokantaan. Jos tietojen dokumentointi on välttämätöntä liiketoiminnassa, ne tulee säilyttää salattuina. Salauksen ansiosta menetettyä tietoa ei päästä välttämättä käyttämään vääriin tarkoituksiin. Yksi hyvä tapa salata tietoa on maskata korttitapahtumien yhteydessä syntyvät kuitit, jolloin kortin kaikki numerot eivät näy ja täten väärinkäyttö voidaan estää varmasti.

4. Siirrä kortinhaltijatiedot ja muut luottamukselliset tiedot julkisissa tietoverkoissa salattuina. Se on erityisen tärkeää, koska tietoihin on helppo päästä käsiksi siirrettäessä niitä Internetissä. Jos salaus on vahva, tietojen pääsy ulkopuolisten käsiin minimoi mahdolliset vahingot.

5. Käytä virustorjuntaohjelmistoa ja päivitä se säännöllisesti. Virukset pääsevät usein yrityksen verkkoon sähköpostien kautta. Tämän takia kaikissa sähköpostijärjestelmissä sekä käyttäjien tietokoneissa tulee olla virustorjuntaohjelma.

6. Kehitä turvallisia järjestelmiä ja sovelluksia sekä ylläpidä niitä. Tietoturvapäivitysten lisäksi on kehitettävä standardoituja ohjelmistokehityskäytäntöjä sekä turvallisia ohjelmistokehitysmekanismeja, jotta verkossa ei olisi haavoittuvia osia. Kun oikeat käytännöt tunnetaan ja viimeiset tietoturvapäivitykset ovat ajan tasalla, on verkko turvattu standardin vaatimalla tasolla.

7. Pääsy yrityksen tietokantaan on tarkoitettu vain niille, jotka tarvitsevat tietoa liiketoiminnallisiin tarkoituksiin. Kun pienempi osa yrityksen henkilökunnasta pääsee käsiksi tärkeisiin tietoihin, niin osuus tietoturvamurtoihin laskee, koska ihminen on usein vastuussa tietoriskien syntymisestä yrityksessä.

8. Luo jokaiselle tietojärjestelmän käyttäjälle yksilöllinen käyttäjätunnus, jotta voidaan tarkkailla, kuka tietoja on käyttänyt ja mihinkä tarkoitukseen.

9. Rajoita fyysinen pääsy kortinhaltijoiden tietoihin huolellisesti, koska se antaa mahdollisuuden tarkastella, muokata tai poistaa tietoja. Tämä tulee ottaa huomioon erityisesti kiinteistön suunnittelussa. Tarkoituksena on eristää vierailevat ihmiset yrityksen tiloissa työskentelevistä ihmisistä, jotta heillä ei olisi pääsyä arkaluontoisten tietojen lähelle.

10. Seuraa ja valvo kaikkea verkossa olevaa kortinhaltijoiden tietojen käyttöä. Paras tapa valvoa tietojen käyttöä on pitää lokikirjaa, johon merkitään kaikki tapahtumat. Lokien luominen kaikissa ympäristöissä mahdollistaa tarkan seurannan sekä analyysin virhetilanteissa. Jos joku pääsee murtautumaan verkkoon, niin tilanteen selvittäminen on helpompaa, kun nähdään kuka ja milloin tietoja on käyttänyt.

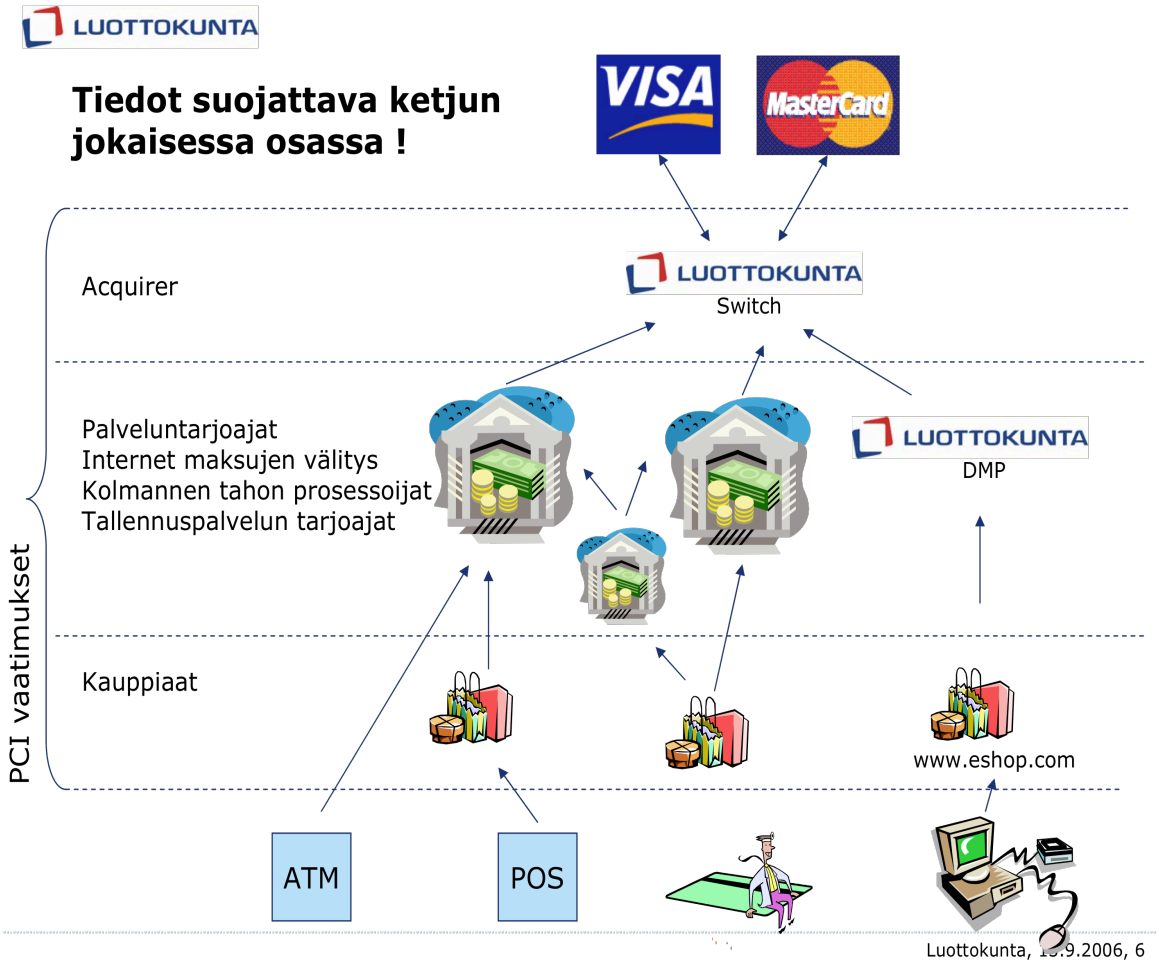
11. Testaa tietoturvajärjestelmät ja –prosessit säännöllisesti. Tietoturva-aukkoja saattaa syntyä, kun uusia ohjelmistoja otetaan käyttöön ja niitä ei ole testat-

tu vielä käytännössä täysin. Tämän takia ohjelmistoja sekä prosesseja tulee testata jatkuvasti, jotta voidaan varmistua riittävästä tietoturvasta.

12. Luo työntekijöitä ja alihankkijoita koskeva tietoturvakäytäntö. Se edesauttaa koko yritystä suhtautumaan oikealla tavalla tietoturvaan ja sen säilyttämiseen. Kaikkien yrityksessä työskentelevien tulisi olla tietoisia yrityksen tietojen luottamuksellisuudesta ja heidän vastuistaan sen suojaamisessa. (Luottokunta PCI-tietoturvastandardi, [viitattu 20.8.2009].)

2.2 Maksutapahtumien suojaaminen

Maksutapahtuman aikana kaikkien osapuolten tietoturva tulee olla PCI-standardin vaatimassa kunnossa. Kuviossa yksi on esitelty erilaisia maksu -ja korttitapahtumaketjuja, joissa tiedot on suojattu kaikissa eri korttitapahtumien vaiheissa. Nostoautomaateilla sekä kaupassa suojaus tapahtuu neljä-numeroisella koodilla. Jos sirukorttipäätettä ei ole, niin magneettinauhaa käytettäessä tulee henkilöllisyys todistaa yli 50 euron ostoksissa. Asioitaessa Internetissä on henkilöllisyys todennettava sähköisesti, joten sielläkin suojaus on voimassa ostotapahtumien aikana. Se ei kuitenkaan riitä, että vain ostotapahtumahetkellä tiedot suojataan, vaan suojaus pitää olla voimassa koko ajan ketjun alusta loppuun. Se tarkoittaa, että kauppiaiden ja palvelun tarjoajien tulee noudattaa PCI-vaatimuksia, jotta ostotapahtuma olisi turvallinen alusta loppuun.



KUVIO 1. Tiedon suojaaminen (Kallio, [viitattu 20.7.2009].)

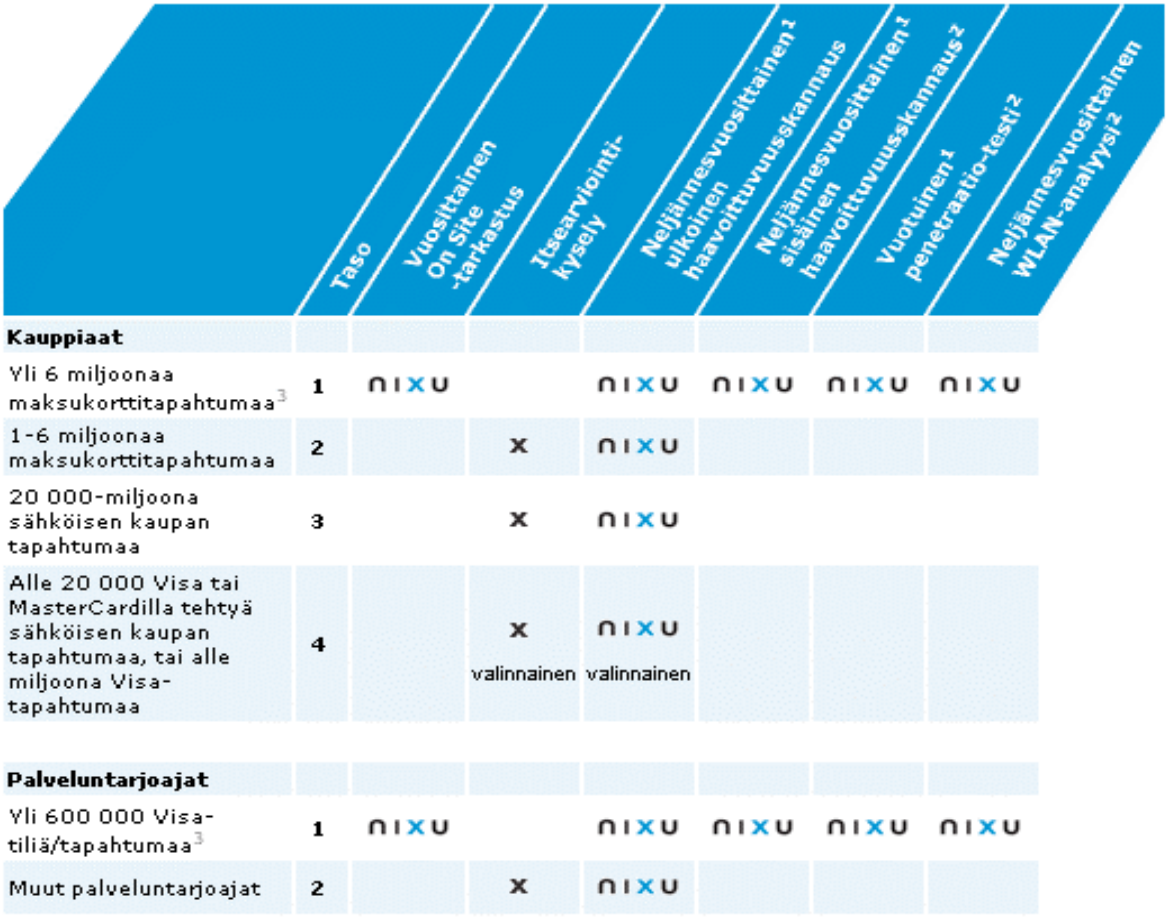
Kuviossa kaksi on esitelty kortin tärkeimmät tiedot, joita tulee suojata parhaalla mahdollisella tavalla. Yhdellä kortin tiedolla väärinkäyttö ei ole mahdollinen, vaan siihen tarvitaan useampia tietoja kuten kortinnumero ja voimassaoloaika. Usein kuitenkaan nämäkään tiedot eivät riitä nettiostoksen tekemiseen, koska cvv2-numerosarja vaaditaan, jos kortti ei ole paikalla. Ccv2-lyhenteellä tarkoitetaan kortin kääntöpuolella olevia kolmea viimeistä varmennusnumeroa. Internetissä tehtävien ostojen suojaustasoa nostaa huomattavasti se, että kortista tarvitaan paljon erilaisia tietoja, jotta sen käyttö mahdollistuu. (Luottokunta, PCI-tietoturvastandardi, [viitattu 20.8.2009].)

KUVIO 2. Mitä tietoja tulee suojata (Kallio, [viitattu 20.7.2009].)

2.3 PCI-standardi käytännössä

PCI-standardin vaativuus vaihtelee sen mukaan, mitä enemmän yrityksellä on korttitapahtumia vuodessa. Kuviosta kolme nähdään, että kauppiaat luokitellaan neljään tasoon. Mitä matalampi taso on, sitä enemmän vaatimuksia PCI-standardilla on. Ensimmäisen tason kauppiaalla pitää olla yli 6 000 000 Visa tai MasterCard ostotapahtumaa vuodessa. Toinen taso vaatii vähintään 150 000 ostotapahtumaa vuodessa ja kolmas taso yli 20 000. Neljännellä tasolla ovat kauppiaat, joilla on alle 20 000 ostotapahtumaa vuodessa. He eivät ole pakotettuja toteuttamaan Pci-standardia, mutta se on heille kuitenkin suositeltavaa. (Luottokunta PCI-tietoturvastandardi, [viitattu 20.8.2009].)

Ensimmäisen tason kauppiailta vaaditaan enemmän PCI-standardin saavuttamiseksi, koska he käsittelevät useammin korttitietoja. Heidän velvollisuuksiinsa kuuluu vuosittainen auditointi ja neljännesvuosittainen tietoverkon skannaus. Toisen ja kolmannen tason kauppiaiden tulee täyttää vuosittainen itsearviointilomake yrityksen tietoturvasta sekä suorittaa neljännesvuosittainen verkon skannaus. Neljännen tason kauppiaiden tulee täyttää ainoastaan vuosittainen itsearviointi, mutta verkon skannaus on vain suositeltavaa. (Luottokunta PCI-tietoturvastandardi, [viitattu 25.8.2009].)



	Taso	Vuosittainen On Site -tarkastus	Itsearviointi-kysely	Neljännesvuosittainen ulkoinen haavoittuvuusskannaus[1]	Neljännesvuosittainen sisäinen haavoittuvuusskannaus[1]	Vuotuinen penetraatio-testi[2]	Neljännesvuosittainen WLAN-analyysi[2]
Kauppiaat							
Yli 6 miljoonaa maksukorttitapahtumaa[3]	1	nixu		nixu	nixu	nixu	nixu
1-6 miljoonaa maksukorttitapahtumaa	2		x	nixu			
20 000-miljoona sähköisen kaupan tapahtumaa	3		x	nixu			
Alle 20 000 Visa tai MasterCardilla tehtyä sähköisen kaupan tapahtumaa, tai alle miljoona Visa-tapahtumaa	4		x valinnainen	nixu valinnainen			
Palveluntarjoajat							
Yli 600 000 Visa-tiliä/tapahtumaa[3]	1	nixu		nixu	nixu	nixu	nixu
Muut palveluntarjoajat	2		x	nixu			

KUVIO 3. PCI tasot ja kelpoisuuden arviointi (Nixu PCI-auditoinnit ja -palvelut [viitattu 20.7.2009].)

2.4 PCI-standardin hakuprosessi

PCI-standardin hakeminen edellyttää auditoinnin suorittamista. Sen vaativuus vaihtelee yrityksen koon perusteella. PCI-standardissa on viisi erilaista auditointimallia. Ensimmäinen niistä on PCI self-Assesment Questionnaire, joka on yrityksen itsensä täyttämä itsearviointilomake. Sen tarkoitus on antaa kokonaiskuva yrityksen tietoturvasta sekä hahmottaa ongelma-alueita. Toinen on PCI-security scan, joka on standardeja hyväksyvän tahon tekemä julkisen verkon tietoturvaskannaus. Siinä tehdään haavoittuvuusskannaus kaikkiin yrityksen ip- osoitteisiin sekä palveluihin, jotka ovat julkisia. Se suoritetaan vähintään joka neljännesvuosi ja lisäksi jos yrityksen infrastruktuurissa tapahtuu ratkaisevia muutoksia, joiden seurauksena tietoturvataso laskee. Skannaus tulee suorittaa niin monta kertaa,

että lopputuloksesta tulee puhdas. Sen lopputulokset jäävät asiakkaan käyttöön, ja ne tarkastetaan vuosittaisen auditoinnin yhteydessä. (Kallio, [viitattu 20.7.2009].)

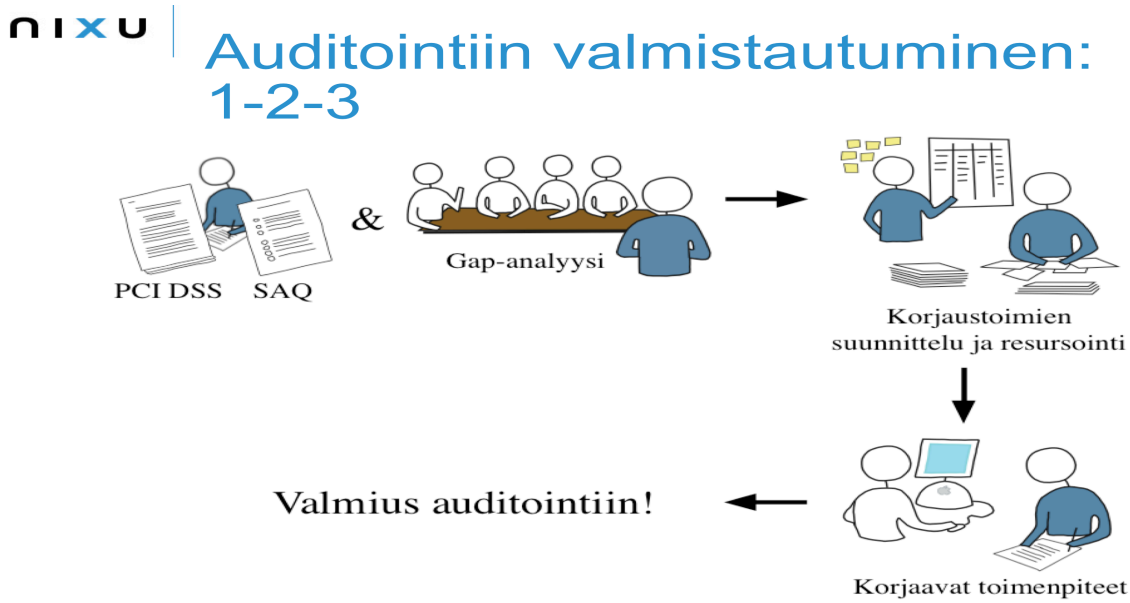
Kolmas auditointi on PCI DSS Security Audit, joka on myös hyväksytyn toimijan suorittama vuosittainen auditointi. Sen lopputuloksena saadaan sisällöltään vakiomuotoinen dokumentti, jossa on kerrattu standardin sisältö järjestelmällisesti ja verrattu yrityksen tekemiin ratkaisuihin. Neljäs auditointimuoto on PCI Payment Application Security Assessment, joka hyväksytyn toimijan laatima auditointi yhdelle ohjelmistolle, kuten kassaohjelmat. Viimeinen auditointimuoto on wlan-analyysi, joka tulee suorittaa neljännesvuosittain. Sen tarkoituksena on selvittää, että yrityksen langattomassa verkossa ei ole ylimääräisiä laitteita tai koneita. (Kallio, [viitattu 20.7.2009].)

2.4.1 Auditointiin valmistautuminen

Auditointiin valmistautumisessa paneudutaan standardin vaatimuksiin ja täytetään itsearviointilomake. Kuviossa neljä esitellään auditointiin valmistautumisen osavaiheet, joiden avulla saadaan hyvä kuva yrityksen vallitsevasta tietoturvallisuudesta.

Kartoituksen tarkoituksena on listata sovellukset ja järjestelmät, jotka tallentavat korttidataa sekä henkilöt, jotka pääsevät niihin käsiksi. Toinen tärkeä osa ennen auditointia on suorittaa Gap-analyysi, jolla saadaan selvitettyä toimenpiteet, PCI-standardin vaatimusten täyttämiseksi. Auditointiin valmistautumisessa apuna voidaan käyttää valtuutettua auditoijaa, joka auttaa prosessin läpiviemistä vaatimusten tulkitsemisessa sekä hyvien käytäntöjen tuntemisessa. Kun korjaavat toimenpiteet on määritelty, tulee niitä varten luoda resurssit, joilla tarkoitetaan osaavia ihmisiä, aikaa ja rahaa. Parhaita korjaavia toimenpiteitä eivät ole tekniset ratkaisut, vaan ihmisten toimintatapojen muutokset, koska ainoastaan niiden avulla voidaan saada aikaan pysyviä muutoksia tietoturvallisuudessa. Se vaatii kuitenkin sitoutumista, ohjausta sekä valvontaa, mutta tätä kautta työtavoista saadaan rutiininomaisia ja tietoturvallisuus paranee. Esimerkkinä korjaavista toimenpiteistä voidaan mainita toimintatapojen dokumentointi, jolloin ne saadaan kaikkien yrityksessä työskentelevien tietoisuuteen sekä helpommin ymmärrettävään muotoon. Do-

kumentoituja toimijatapoja tulee päivittää ahkerasti yrityksen muuttuessa, koska muuten ne menettävät merkityksensä. Tekniset ratkaisut voivat luoda myös parannuksia, mutta perimmäinen tarkoitus on, että tietoturvallisuus lähtee yrityksen sisällä toimivista henkilöistä. (Vehviläinen, [viitattu 20.8.2009].)



KUVIO 4. Auditointiin valmistautuminen. (Vehviläinen, [viitattu 20.8.2009].)

2.4.2 Yritysten raportointivelvollisuus

Yritysten raportointivelvollisuudet on paras selvittää Luottokunnan tekemien kaavakkeiden avulla. Niitä seuraamalla voi luoda kuvan, mikä itsearviointikaavake sopii heidän yritykselleen. Kaaviot ovat liitteinä 2 ja 3. Ensimmäinen askel raportointivelvollisuuden selvittämisessä on tarkastaa luottokorttitapahtumien määrä vuodessa. Sen perusteella määritetään, minkä tasoinen standardi yrityksen tulee täyttää. Standardin tasot on jaettu neljään ryhmään, joista ensimmäinen taso on vaativin ja neljäs taso suppein. Ensimmäisen tason kauppiaiden on raportoitava PCI-standardin noudattamisesta Luottokunnalle vuosittain antamalla paikan päällä tapahtuvaa turvallisuusauditointia koskeva raportti. Sen lisäksi Luottokunta vaatii PCI-verkkoskannausraportit neljännesvuosittain. Ne tulee olla auktorisoidun PCI-verkkoskannauksia tekevän yrityksen suorittamia. Toisen, kolmannen ja neljännen tason kauppiaiden on täytettävä itsearviointilomake sekä raportoitava sen tulokset

luottokunnalle. Sen lisäksi kauppiaiden on lähetettävä PCI-verkkoskannausraportit neljännesvuosittain.

Kun eri tasoisten kauppiaiden velvollisuudet on selvitetty, on aika valita kunkin tason kauppiaalle sopiva itsearviointilomake. Jos yritys käsittelee ainoastaan tapahtumia, joissa kortti ei ole läsnä tai ei tallenna ja käsittele korttitietoja, niin A-tason lomake riittää. Tämä on mahdollista siten, että yritys ei itse käsittele tietoja, vaan se käyttää ulkoista tahoa näiden toimien suorittamiseen. Kyseisten yritysten tulee kuitenkin dokumentoida paperiversiona kaikki kuitit, mutta sähköisesti se ei niitä saa tallentaa. B-tason lomaketta tulee täyttää, kun yritys käyttää maksukorttipäätettä, mutta ei kuitenkaan lähetä korttitietoja Internetin tai puhelinlinjan välityksellä. Kyseinen yritys ei saa myöskään tallentaa maksukorttitietoja sähköisesti, vaan kaikki kuitit ja raportit tulee olla paperimuodossa.

C-tason kauppiailla tietoturvataso tulee olla huomattavasti korkeampi, koska maksupäätteet toimivat tietokoneilla ja ne ovat yhdistetty Internetiin. Kassakoneet eivät saa olla kuitenkaan kytkettynä mihinkään muuhun järjestelmään, jotta mahdollisia tietoturvariskejä ei tule muista järjestelmistä. Tämän tason yritykset eivät myöskään voi tallentaa kortinhaltijoiden tietoja sähköisesti, vaan kaikki tulee olla paperimuodossa. D-tason yrityksissä erona muihin tasoihin on se, että ne saavat tallentaa korttitietoja sähköisesti, mutta PCI-standardin vaatimukset koskevat heitä kaikessa laajuudessaan. Tällöin tietoturvalta vaaditaan paljon.

2.4.3 Standardin hyväksyminen

Auditoinnin tuloksista tehdään täydellinen raportti, jossa on listattu kaikki virheet, mitä on löydetty sekä uudet toimintamallit niiden virheiden korjaamiseksi. Valtuutetun toimijan tulee lukea raportti ja hyväksyä se. Kun toimija hyväksyy raportin, niin sen tarkkuus sekä oikeellisuus voidaan todentaa ja raportti voidaan lähettää luottokorttiyhtiöön, joka tekee ratkaisun sen oikeanmukaisuudesta. Auditoijan tulee tallentaa auditoinnin todistusaineisto kolmen vuoden määräajaksi. Jos Luottokunta toteaa kauppiaan täyttäneen kaikki PCI-standardin vaatimukset, voidaan sertifikaatti myöntää. (Vehviläinen, [viitattu 20.8.2009].)

2.5 Tietoturvallisuus

Yritykset ovat alkaneet kiinnittää huomiota tietoturvallisuuteen vasta viime vuosina. Nykyään ymmärretään, että vahvan tietoturvan vaikutus on paljon muutakin kuin vain tietojärjestelmissä oleva suojattu tieto. Sen vaikutukset ulottuvat myös yrityksen liiketoimintaan, imagoon sekä taloudellisiin tappioihin. Yrityksen maine ja markkinoiden luottamus ovat joskus jopa tärkeämpiä kuin yrityksen hallussa olevat tiedot. Tietoturvallisuuteen on ryhdytty panostamaan resursseja enemmän kuin ennen, koska yritykset käyttävät paljon tietotekniikkaa. Sen takia on ajauduttu tilanteeseen, että yrityksistä on tullut riippuvaisia sen toiminnasta. (Laaksonen, Nevasalo ja Tomula 2006, 19.) Nykyään yritysten tiedot ovat yhteisissä tietojärjestelmissä eri puolilla maailmaa. Jos yritykset eivät pääse niihin käsiksi, niin toiminta lamaantuu täysin. Tämän takia tietoturvallisuuteen panostetaan nykyään paljon resursseja. (Miettinen 2002, 11.)

Tietoturvallisuus tarkoittaa tietojen, järjestelmien ja palveluiden suojaamista kaikissa olosuhteissa. Se on pieniä tekoja arkipäivän toiminnassa ja parhaimmillaan se saadaan osaksi organisaatiokulttuuria. Tärkeintä siinä on, että yrityksen kaikki henkilöt ymmärtävät sen tärkeyden ja työskentelevät sen edesauttamiseksi. Tietoturvallisuuteen kuuluu niin teknisiä kuin hallinnollisiakin keinoja, jotka tulee suunnitella huolella sekä toteuttaa lainsäädännön rajoitusten ja vaatimusten mukaisesti. Tietoturvallisuuden kehittämisen pitää olla jatkuvaa ja sen vaikutuksia on seurattava säännöllisesti, jotta toimintaa voidaan parantaa entisestään. (Laaksonen, 2006, 17.)

2.5.1 Tieto yrityksen kilpailutekijänä

Tieto on tärkeä resurssi liiketoiminnassa, mutta siihen ei silti kiinnitetä tarpeeksi huomiota. Usein näkee erityisesti pienten yritysten laiminlyövän tiedon suojaamista, koska he kuvittelevat, että muita yrityksiä ei kiinnosta yrityksen tiedot ja toiminta. Varsinkin tuotekehityksen tuomat tiedot ovat tärkeitä ja ne kiinnostavat suuresti kilpailijoita, sillä jos tiedot päätyvät heidän käsiinsä, he säästävät huomattavia summia. Tällöin heidän ei tarvitse itse panostaa tuotekehitykseen. (Kyrölä 2001, 38.)

Tieto, joka on aktiivista ja jatkuvasti yrityksen tarpeisiin mukautuvaa on käyttökelpoista. Sen määrä yrityksessä kasvaa koko sen eliniän ajan. Tämän takia tietoa pitää muokata ja päivittää koko ajan, ettei se pääse vanhenemaan. Tiedon oikeellisuus on tärkeää varsinkin asiakaspalvelussa, päätöksenteossa sekä tuotesuunnittelussa. Jos tieto on vääristynyttä, niin se johtaa virhepäätöksiin ja huonoihin valintoihin. Tiedon säilyttämiseenkin on syytä kiinnittää huomiota, koska yrityksen tietoja kuten asiakastietoja velvoittaa yrityksen suojaustahto. Se tarkoittaa, että asiakastietoja ei saa vuotaa yrityksen ulkopuolelle ilman asiakkaiden erityistä lupaa. (Kyrölä 2001, 39.)

Voidaan sanoa, että tiedosta on tullut keskeinen pääoma, kustannusten aiheuttaja ja ratkaiseva taloudellinen resurssi. Nykyään tietoa pidetään avaintekijänä tuottavuudelle, hyvälle kilpailukyvylle sekä taloudellisille saavutuksille. (Paavilainen 1998, 2.)

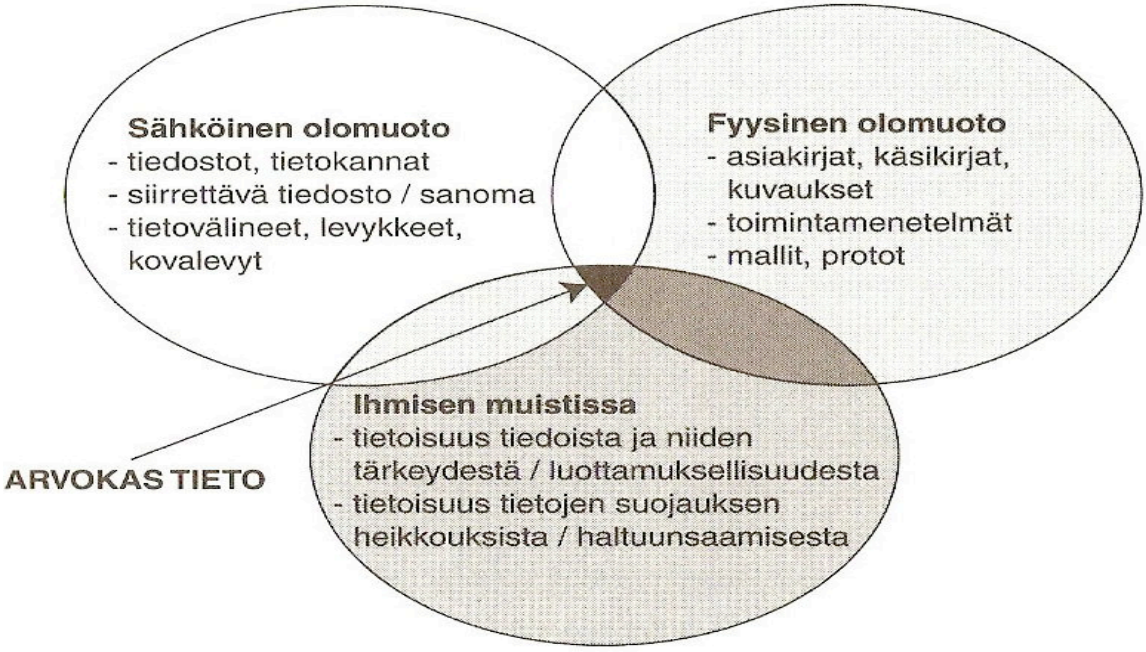
Yrityksen on suojeltava tieto-omaisuuttaan. Siihen luetaan kaikki yrityksessä luotu ja muokattu tieto. Tieto-omaisuus on aineistoa, joka on tietoa tuottavien ja käyttävien työntekijöiden hallussa. Kyseinen aineisto voi olla niin fyysisessä kuin sähköisessäkin muodossa olevaa dokumentoitua tietoa. Toinen tärkeä yrityksen pääoma on tietopääoma. Se sisältää työntekijöiden omistaman tiedon, joka on kertynyt vuosien saatossa kokemuksen myötä. Tietopääoma on työntekijöiden tietoa yrityksen toimintamalleista ja käytännöistä sekä niiden heikkouksista. Kyseisiä tietomuotoja tulee suojata sen mukaan, kuinka arvokasta ja tärkeää tietoa ne sisältävät. (Kyrölä 2001, 71.)

Yritysten velvollisuus on suojella yrityksen omaa tietoa, asiakastietoa sekä yhteisprojektien tietoa. Yrityksen omaksi tiedoksi voidaan lukea sisäpiiritieto sekä henkilötiedot, joita ei saa päästää ulkopuolisen käsiin. Asiakastiedoille on määriteltävä suojausmenetelmät sekä käyttötavat, ettei asiakkaiden henkilötiedot pääse leviämään yrityksen ulkopuolelle. Yhteisprojekteissa kuten organisaatioiden välisissä tuotekehityksissä tulee sopia tekijänoikeuspykälät, jotta tieto saataisiin pysymään asianomaisten piirissä. (Kyrölä 2001, 74.)

2.5.2 Tiedon eri olomuodot

Tietoa voi olla kolmessa eri olomuodossa. Siksi sen suojaamiseen tarvitaan useita eri suojausmenetelmiä tiedon olomuodosta riippuen. Tämän takia tiedon olomuodon tunnistaminen on otettava huomioon tiedon luokittelussa sekä suojauskeinojen käyttöönotossa. (Kyrölä 2001, 24.)

Kuviossa viisi on esitelty tiedon eri olomuodot. Ensimmäinen niistä on sähköinen olomuoto. Siinä tieto voi olla tallennettuna tietokantoihin, ulkoisille tallennusvälineille sekä kovalevyille. Toinen olomuoto on fyysinen, jossa tieto on käsin kosketeltavaa. Se voi sisältää asiakirjoja, käsikirjoja sekä erilaisia toiminnan kuvauksia. Kolmas olomuoto on ihmisenmuistissa oleva tieto. Se on kokemuksen kautta opittua tietoa. Näiden kolmen olomuodon välissä on arvokasta tietoa, joka on olomuotojen sekoitus. Se on ihmisten halussa olevaa tietoa, jossa on yhdistelty kaikkia eri tiedon olomuotoja ja siksi se on arvokasta tietoa. (Kyrölä, [viitattu 27.2.2009].)



KUVIO 5. Tiedon ja sen käsittelyketjun olomuodot (Kyrölä 2001, 25.)

Koska tieto on yrityksissä monissa eri muodoissa, on sen oikea käsittelytapa on elintärkeää. Tietojen tuottamisessa ja käsittelyssä tarvitaan erilaisia välineitä, ohjelmistoja sekä ulkoistamispalveluita, joiden avulla tieto saadaan dokumentoitua ja jaettua. Tietojen sisällön tunnistaminen on tärkeää, jotta yritys osaa suojata tiedot muuttumiselta, häviämiseltä sekä asiattomilta henkilöiltä. (Kyrölä 2001, 24-25.)

2.5.3 Tiedon ulottuvuudet

Tietoturvallisuus voidaan jakaa kuuteen ulottuvuuteen. Niiden tarkoitus on antaa perusvaatimukset, joilla pyritään varmistamaan:

- tietojen saatavuus
- tietojen hyödyllisyys
- tietojen luottamuksellisuus
- tietojen hallussapito
- tietojen eheys
- tietojen aitous

Tietojen saatavuudella tarkoitetaan sitä, että yrityksen tiedot ovat tarvittaessa käytössä ja niihin päästään käsiksi milloin vain. Jos yrityksen tietoja ei voida käyttää silloin, kun niitä päivittäisessä toiminnassa tarvitaan, voidaan tiedon saatavuuden sanoa olevan uhattu. Tiedon saatavuuteen voi vaikuttaa Atk- järjestelmän tekninen vika tai tietoliikenneverkon tukkeutuminen. Tietojen hyödyllisyydestä voidaan puhua silloin, kun yrityksen tiedot ovat sellaisessa muodossa, että niitä voidaan käyttää vaivattomasti päivittäisessä toiminnassa. Jos ilmenee, että yrityksen tiedot ovat syystä tai toisesta käyttökelvottomia, on hyödyllisyys menetetty. (Miettinen 1999, 27- 28.)

Tietojen luottamuksellisuudesta puhuttaessa tarkoitetaan, että yrityksen tiedot ovat ainoastaan niiden henkilöiden käytettävissä, jolla on lupa käyttää tietoa. Jos yrityksen tietoa pääsee ulkopuolisten käsiin, on tiedon hallussapitoa loukattu. Sen luottamuksellisuuden menettäminen voi aiheuttaa yrityksille suuria menetyksiä niin rahallisesti kuin imagonkin kannalta. (Miettinen 1999, 24.)

Tietojen hallussapidolla tarkoitetaan sitä, kuinka yksittäinen henkilö voi käsitellä yrityksen omistamaa tietoa. Hallussapidon voidaan katsoa olevan vaarantunut, jos yrityksen tietoa joutuu ulkopuolisen käsiin. Tyypillinen esimerkki tästä on yritykseen tehty murtovarkaus. Jos varastettuja tietoja ei saada takaisin yrityksen haltuun, voidaan puhua hallussapitoon kohdistuvasta menetyksestä. Jos taas tiedot palautuvat myöhemmin yritykseen, niin kyseessä on väliaikainen hallussapitoon kohdistuva menetys. (Miettinen 1999, 25.)

Tietojen eheydellä tarkoitetaan, että yrityksen tieto ei synny tai häviä itsestään. Tietojen eheys on kunnossa, kun tiedot ovat alkuperäisessä kunnossa ja niitä ei ole muokattu väärään muotoon. Tietojen eheys ja virheettömyys menetetään, jos esimerkiksi atk-häiriön vuoksi tieto pääsee muuttumaan alkuperäisestä. (Miettinen 1999, 26.)

Viimeinen tietojen ulottuvuus käsittelee tietoaineksen aitoutta. Sen perusolettamus on, että tieto on alkuperäistä, eikä sitä ole väärennetty. Yritys käyttää tietojaan erinäisiin päätöksiin. Jos ilmenee, että tieto ei ole aitoa, niin päätökset osoittautuvat

virheellisiksi. Tämän takia tietojen aitoudesta on pidettävä hyvää huolta. (Miettinen 1999, 27.)

2.6 Tietoriskit

Vastauksen antaminen tietoriskien olemukseen on vaikeaa, koska tietoriskit voivat olla esimerkiksi viruksia, hakkereita tai epäluotettavia työntekijöitä. Yleensä kuitenkin lähdetään siitä, että tietoriskit ovat tietoihin ja niiden käyttöön kohdistuvia uhkia. Tietoriskiksi voidaan määritellä tilanne, jolloin tieto on muuttunut. Siihen ei päästä käsiksi tai se on päässyt leviämään ulkopuolisten käsiin. Tietoriskien kattavaa tunnistamista vaikeuttaa se, että sen aiheuttajat voivat olla hyvin erilaisia sekä uhkien toteutumissyyt voivat vaihdella suureesti. Merkittävän riskin voi siis aiheuttaa niin ihminen, tekninen vika kuin myös luonnonkatastrofikin. (Suominen 2003, 80.)

Tietoriskit voivat tapahtua tahattomasti tai tahallisesti, mutta usein kuitenkin ihminen on syypää niiden tapahtumiseen. Tämän takia voidaan sanoa, että ihminen on isoin tietoriski, johon yrityksen tulee varautua. Tahallisesti tehdyt riskit voivat olla ilkivaltaa, sabotaasia tai yritysvakoilua. Esimerkiksi sopimusrikkomukset voivat tapahtua tahattomasti ihmisen itse tiedostamatta niitä.

Muita mahdollisia tietoriskejä ovat esimerkiksi tulipalo, joka tekee mittaamattomia vahinkoja tuhoamalla asiakirjoja ja atk-laitteistoja. Vesi ja muut nesteet voivat vahingoittaa myös atk-laitteita ja asiakirjoja, jolloin yrityksen tietoa häviää. Teknisiksi riskeiksi voidaan luokitella laitteiden vikaantumiset sekä atk-toiminnan keskeytymiset. Kyseisten riskien toteutuessa toiminta yrityksessä pysähtyy ainakin osittain, koska yritykset ovat nykyään suuresti riippuvaisia atk-toiminnoista. Ohjelmisto ja tietojärjestelmien pettäessä syntyy myös tietoriskejä, koska silloin suojaukset ovat haavoittuneessa tilassa ja tunkeutuminen yrityksen tietoverkkoon on helpompaa. (Pohjolayhtiöiden julkaisuja 1, 5.)

Viime vuosien aikana tekniikan kehittyminen on tuonut yrityksille paljon uusia riskejä. Enää tietokoneet eivät ole yhdessä huoneessa, vaan kannettavien laitteiden

ja langattoman tekniikan avulla tietokoneita voidaan käyttää missä ja milloin vain. Tämä on tuonut uusia riskejä, koska verkkoon ja toisten tietokoneiden kovalevyille pääsemiseen on avautunut uusia väyliä. Siitä esimerkkinä voidaan käyttää bluetooth sekä langattoman verkon tekniikkaa, joka on lisännyt valvonnan haastavuutta yritysmaailmassa. (Calder 2005, 8.)

2.7 Tietoriskien hallinta

Tietoriskien hallinta on yrityksen työntekijöiden yhteinen tehtävä. Johdon tehtävä on antaa puitteet sekä resurssit ja luoda tavoitteet, kuinka tietoriskejä vastaan toimitaan. Teknisen henkilöstön vastuulla on suunnitella ratkaisut tietoriskejä vastaan erilaisin menetelmin. Esimiehet opastavat alaisilleen oikeita toimintatapoja sekä vastaavat toiminnan turvallisuudesta. Työntekijät vastaavat työssään tietoriskien käytännön hallinnasta. Tietoriskien torjumiseen tarvitaan yhteistyötä. (PK-yrityksen riskienhallinta, [viitattu 27.2.2009].)

Tietoriskien hallinta on jatkuvaa tasapainottelua hyväksyttävän riskitason ja hyväksyttävien kustannusten välillä. Tämän takia oikean riskitason löytäminen on tärkeää, koska tieto on yksi tärkeimmistä organisaation suojattavista kohteista. Tiedot ja niiden käyttötapa liittyvät olennaisesti kaikkiin yrityksen toimintoihin ja osa-alueisiin. Yrityksestä itsestään riippuu, mitä tietoturvan sektoria se haluaa painottaa. On olemassa on myös universaaleja malleja kuten BS 7799, joka jaottelee tietoturvallisuuden seuraavasti:

1. tietoturvapolitiikka
2. tietoturvallisuuden organisointi
3. suojattavien kohteiden luokitus ja valvonta
4. henkilöstöturvallisuus
5. fyysinen - ja ympäristön turvallisuus
6. tietoliikenteen ja käyttötoimintojen hallinta
7. pääsyoikeuksien valvonta
8. järjestelmien kehittäminen ja ylläpito

9. liiketoiminnan jatkuvuuden hallinta
10. vaatimustenmukaisuus (Suominen 2003, 82.)

Tietoturvallisuuden haluttu taso saavutetaan, kun jokaiselle sektorille valitaan suojamekanismeja Ne voivat olla dokumentoituja toimintatapoja, ohjeita tai teknisiä ratkaisuja. Tarvittavien turvaratkaisuiden tunnistaminen edellyttää huolellista suunnittelua sekä paneutumista tietoturvallisuuden yksityiskohtiin. Suojamekanismien valitseminen perustuu johdon asettamiin turvallisuusvaatimuksiin siitä, kuinka paljon suojautumiseen halutaan panostaa ja siitä, mitkä riskit halutaan kantaa omalla vastuulla.

Turvallisuusvaatimusten täyttämisen apuna voidaan käyttää kolmea eri lähdettä. Niistä ensimmäinen on tietoriskienkartoitus, jossa tunnistetaan uhat ja arvioidaan niiden vaikutukset. Toisena lähteenä voidaan käyttää lakeja ja asetuksia, jotka antavat yritykselle tietoturvallisuuden rajat. Kolmantena lähteenä voidaan käyttää tietojenkäsittelyyn liittyvää periaatetta, jotka organisaatio on määritellyt toimintansa tueksi. Niiden tarkoituksena on täydentää tietoturvallisuutta erilaisin teknisin ratkaisuin. (Suominen 2003, 83.)

2.7.1 Fyysinen suojaus

Fyysinen suojaus on se tietoriskien alue, johon yleensä ensimmäisenä kiinnitetään huomiota. Kyseisen suojauksen suunnittelussa tulee huomioida rakennuksen sijaintipaikka sekä siihen käytettävät rakennustarvikkeet. Esimerkkinä voidaan käyttää varmuuskopioarkiston sijoittelua pois vilkkaasti liikennöidyiltä sekä paloherkiltä paikoilta. (Pohjola-yhtiöiden julkaisuja 1, 10.)

Kulunvalvontaan on myös kiinnitettävä huomiota, koska varmuusarkistot ja atk-keskukset sisältävät paljon yrityksen tärkeää tietoa, joten ne tulisi eristää yrityksen muista tiloista. Kaikki kulkeminen yrityksen tiloissa tulisi saada valvotuksi ja kulkijoiden henkilöllisyys tulisi olla jälkikäteen tarkistettavissa. Parhaassa tapauksessa strategisesti tärkeät paikat saataisiin eristettyä niin hyvin, että vain siellä työskentelevillä olisi pääsy sinne. (Kyrölä 2001, 122- 123.)

Yrityksen yleisilmeeseen on syytä kiinnittää myös huomiota. Kaikki kalusteet, laitteet ja tarvikkeet tulisi sijoittaa huoneisiin, joissa niitä tarvitaan työtehtävän suorittamiseen. Siisteys luo oleellisen osan turvallisuuteen. Kun mitään ylimääräistä ei ole esillä, niin varkauksilta ja ilkivallalta vältytään paremmin. (Kyrölä 2001, 124.) Koska sähköistä tietoa on paljon kovalevyillä ja muilla tiedonsiirtovälineillä, tulee myös niitä säilyttää oikein. Esimerkiksi tietokoneita ei tule sijoittaa kaikkien käytössä oleville kulkureiteille tai pölyisiin ja kosteisiin tiloihin. (Pohjola- yhtiöiden julkaisuja 1, 10.)

Strategisesti tärkeiltä paikkoja tulee poistaa kaikki kilvet, jotka paljastavat niiden olinpaikan. Kyseisiin tiloihin tulee myös asentaa ajantasainen hälytysjärjestelmä, joka käsittää savun, veden lämmön, kosteuden sekä liikkeen tunnistimet. (Pohjola-yhtiöiden julkaisuja 1, 11.)

2.7.2 Tietoliikenneturvallisuus

Tietoliikenteen turvaamisessa on tarkoitus suojata yrityksen tiedot, kun niitä siirretään, varastoidaan ja käsitellään. Siinä pyritään varmistamaan, että yrityksen tiedot eivät joudu ulkopuolisille ilman yrityksen lupaa ja että tiedonsiirto tapahtuu luotettavasti ilman häiriöitä. (Miettinen 1999, 20.)

Sähköistä tietoa suojaamaan on luotu käyttäjätunnuksia sekä salasanoja, joiden avulla pystytään rajaamaan työntekijöiden liikkumista yrityksen verkossa. Verkon rajaukset tulee suorittaa jokaisen työntekijän kohdalta henkilökohtaisesti ja heillä tulee olla pääsy ainoastaan omissa työtehtävissä tarvittaviin tietoihin. Työntekijöiden työsuhteen päätymisen jälkeen, käyttäjätilit on poistettava välittömästi käytöstä, koska ne aiheuttavat tietoturva riskiä. (Kyrölä 2001, 118.)

2.7.3 Ohjelmistot ja tietoaineistoturvallisuus

Yritykset tallentavat paljon arvokasta tietoa sähköisesti. Tämän takia tiedon suojaamisessa tulee perehtyä hyvin ohjelmistoihin sekä järjestelmiin, joihin ollaan in-

vestoimassa. Tämä on tärkeää, koska ne sisältävät usein puutteita tai virheitä, jotka altistavat yrityksen tietoliikenneverkon asiattomalle käytölle. Ohjelmistoissa on suuria eroja ja siksi niiden toimivuus on varmistettava kyseisessä yrityksessä ennen niiden käyttöönottoa. (Kyrölä 2001, 116.)

Ohjelmistoturvallisuudessa on kyse yrityksen tietokoneohjelmien suojaamisesta, ohjelmien lisensioinnista sekä rekisteröinnistä. Sitä voidaan jakaa sisäisiin suojausominaisuuksiin sekä erityisiin suojausohjelmistoihin. Sisäisiä suojausominaisuuksia ovat ohjelmistoon pääsyn valvonta, lokitietojen keruu ja salasanakäytännöt. Erityisinä suojausohjelmistoina voidaan pitää viruksentorjuntaohjelmistoja. (Miettinen 1999, 21.)

Tietoa tulee suojata hyvällä virustentorjuntaohjelmalla. Jos viruksia pääsee koneelle, se saattaa johtaa tietojen häviämiseen kovalevyltä tai tukkia tietoliikenneverkon. Kyseisten tilanteiden varalle on oleellista suunnitella ennalta toimintatavat, jos tietokonevirus pääsee tietoverkkoon. Kun toimintatavat on suunniteltu aikaisemmin, ei yrityksen toimintaa tarvitse välttämättä pysäyttää ollenkaan.

Pelkät virustentorjuntaohjelmat ja palomuurit eivät kuitenkaan aina auta suojamaan tietoverkkoja ja sen koneita. Siksi työntekijöillä tulee olla käsitys, miten tietokoneella toimitaan turvallisesti. Työntekijöiden täytyy miettiä, mitä sähköpostiliitteitä avaa ja mitä ohjelmia yrityksen koneelle asentaa, koska näiden toimintojen kautta saattaa viruksia päästä siirtymään tietoverkkoon. (Kyrölä 2001, 119- 120.)

Tietoaineiston turvallisuudessa tulee kiinnittää huomiota erityisesti tiedon oikeanlaiseen käsittelyyn. Se pitää sisällään tiedon säilyttämisen, varmistamisen, palauttamisen sekä tuhoamiseen liittyvät toimet. Näiden turvaamistoimenpiteiden tarkoituksena on estää tiedon tuhoutuminen, muuttuminen sekä luottamuksellisuuden menettäminen eri tiedonkäsittelyprosessien aikana. (Hakala, Vainio ja Vuorinen 2006, 11.)

2.7.4 Laitteisto

Paras tapa vaikuttaa laitteiston turvallisuuteen sekä yrityksen tietoturvallisuuteen on hankkia sellaisia laitteita, joissa suojaukset ovat tehtaasta lähtiessä kunnossa. Tätä kautta yritys vaikuttaa välillisesti laitteistoturvallisuustason paranemiseen. Laitteiston turvallisuuden kannalta tärkeimmät perussuojausmenetelmät ovat:

- tiukka pääsyn valvonta
- laitteiston käytön tapahtumatietojen kerääminen
- helppo varaosien saatavuus
- varalaitteiden hankkiminen
- laitteiden häiriötön sähkön saanti
- kattavat laitteisto dokumentaatiot
- kattavat ylläpito ja huoltosopimukset

Tärkeimpiä laitteistoturvallisuuden suojamenetelmiä ovat pääsyn valvonta. Sillä pyritään estämään asiattomien henkilöiden pääsy yrityksen tietojärjestelmään. Tapahtumatietojen keräämisellä saadaan havaittua henkilö, joka on mahdollisesti käyttänyt laitteistoa väärin. Helppo varaosien saatavuus on toiminnan kannalta tärkeää, jotta turhilta keskeytyksiltä vältyttäisiin ja laiteviat saataisiin korjattua mahdollisimman nopeasti. Varalaitteistolla pyritään varmistamaan toiminnan sujuvuus häiriötilanteessa ilman suuria keskeytyksiä. Sähkön saanti taas saadaan turvattua esimerkiksi polttomoottorijärjestelmillä, joita voidaan käyttää hätätapauksissa. Laitteistoista on hyvä olla kattavat dokumentaatiot ja niiden tulee sisältää kuvaus teknisistä ratkaisuista sekä yksityiskohtaiset käyttöohjeet. Niiden avulla ongelmatilanteet saadaan selvitettyä helpommin. Kaiken lisäksi yritysten kannattaa neuvotella hyvät huolto- ja ylläpitosopimukset, jotta laitteiden toimivuus olisi aina taattua. (Miettinen 2002, 168.)

2.7.5 Henkilöstö

Ihmisen toimintaa pidetään suurimpana uhkana tietoturvallisuudelle. Tiina Danilotschkin-Forsman on kiteyttänyt asian hyvin sanomalla, että *ihminen on suurin tietoriski, mutta virus tunnetuin* (Danilotschkin-Forsman, [viitattu 1.9.2003].)

Ihmisten muistissa on paljon tietoa, mitä ei ole saatu dokumentoitua yrityksen tietokantaan. Pitkäaikaisille työntekijöille on kertynyt paljon tietämystä ja osaamista vuosien aikana. Tämän takia heidän pitämisensä yrityksessä on sen toiminnan kannalta elinehto.

Tietoa voidaan kuitenkin suojata ja pitää osaksi yrityksessä, jos käytössä on toimivat varamiessuunnitelmat sekä laillisilla sopimuksilla toteutetut vaitiolovelvollisuudet. (Pohjola- yhtiöiden julkaisuja 1, 17.) Vaitiolovelvollisuudet voidaan tehdä yritysten sekä yrityksen ja henkilöstön välillä. Niissä on kyse siitä, että vastapuolet noudattavat yhteisiä menettelytapoja tiedonsuojaamisessa sekä luovuttamisessa ja vastaanottamisessa. Tällä pyritään varmistamaan kummankin osapuolen ymmärrys tietojen tärkeydestä sekä sitoutumisesta suojaamaan niitä. (Miettinen 1999, 165.)

Henkilöstöstä johtuvia riskejä minimoitaessa tärkein hetki on työntekijöiden rekrytointivaihe. Siinä tulee suurta huomiota kiinnittää henkilöiden taustoihin, koska sitä kautta työntekijöiden soveltuvuus työtehtäviin on mahdollista tarkistaa. (Pohjola-yhtiöiden julkaisuja 1, 17.) Henkilöstön taustojen selvittely kannattaa aloittaa viranomaistarkistuksella. Sen avulla saadaan selvitettyä, onko henkilö syyllistynyt rikolliseen toimintaan. Tämän jälkeen tulee tarkastaa työhistorian oikeellisuus ottamalla yhteyttä yrityksiin sekä mahdollisiin suosittelijoihin. Heiltä voi saada myös tarkempaa tietoa henkilöstä, mitä muilla taustaselvityksillä ei saa. Syytä on myös tarkastaa, onko tulevalla työntekijällä yrityskytkentöjä toisiin yrityksiin, jotta arkaluontoista tietoa ei pääse sitä kautta leviämään kilpailijoille. Nykypäivänä Internet tarjoaa loistavan tavan tutkia mahdollisia uusia työntekijöitä. Tätä kautta voi saada myös tietoa henkilön kiinnostuksen kohteista sekä toiminnasta, jossa hän on mukana. (Miettinen 1999, 162- 164.)

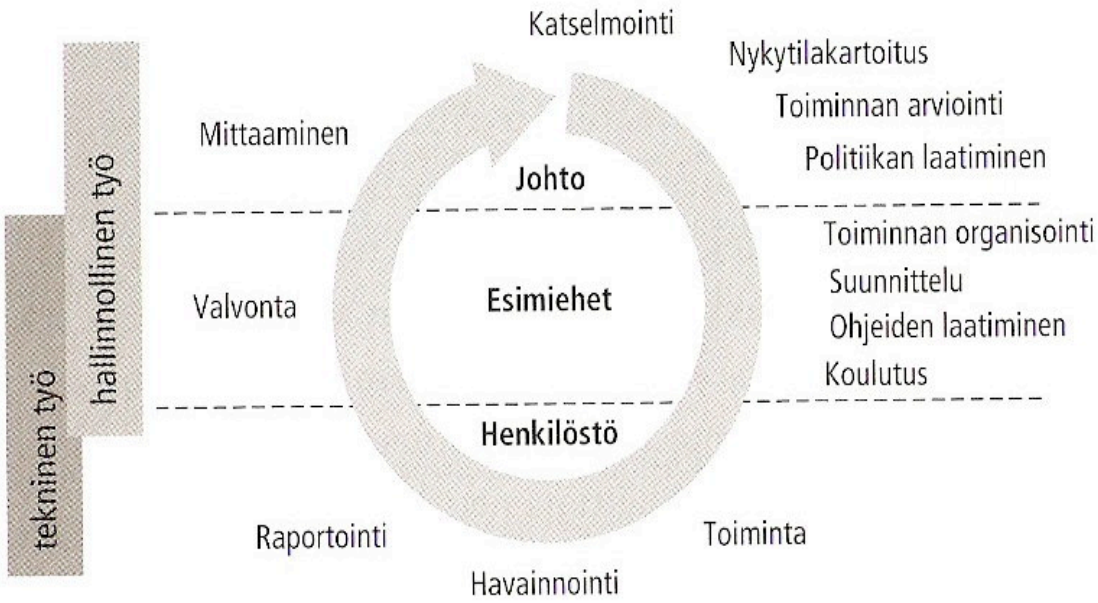
Kun henkilöstö on saatu valittua, heidän luotettavuuttaan ja pysyvyyttään voidaan parantaa oikeanlaisella motivoinnilla, joka sisältää sopivan palkkauksen sekä tarpeellisuuden tunteen yrityksen toiminnassa. Näillä keinoilla tytöntekijät saadaan pidettyä yrityksessä ja tietoa ei vuoda kilpaileviin yrityksiin. (Pohjola- yhtiöiden julkaisuja 1, 17.)

2.7.6 Rikollinen toiminta

Rikosriskejä vastaan voidaan suojautua ennaltaehkäisevästi. Se pitää sisällään näkyviä suojaustoimenpiteitä kuten vartiointi, tekninen valvonta, puomit ja aidat. Toinen tapa suojautua rikoksilta niiden tapahduttua on tehdä rajoittavia toimenpiteitä. Siinä pyritään heti rikoksen tapahduttua rajaamaan vahinkojen määrä minimiin. Siitä esimerkkinä pidetään yhteydenottoa viranomaisiin sekä vakuutusyhtiöön niin nopeasti kuin mahdollista. Kolmas ja suojautumistapa on korjaavat toimenpiteet, joilla pyritään puuttumaan riskejä aiheuttaviin tekijöihin kuten puutteelliseen vartiointiin tai valvontaan. Usein korjaavia toimenpiteitä tehdään kuitenkin, kun vahinko on tapahtunut eikä silloin kun ne havaitaan. (Miettinen 2002, 258.)

2.8 Tietoturvallisuuden vastuualueet

Ylimmän vastuun tietoturvallisuudessa kantaa johto. Se ei kuitenkaan tarkoita, että muiden ei siitä tarvitsisi välittää, vaan kaikille yrityksessä työskenteleville kuuluu omat vastuualueensa. Seuraavissa kappaleissa käsitellään vastuualueita kolmelta eri kannalta sekä sidosryhmien odotuksia ja lakien velvoituksia tietoturvallisuuden edistämisessä. Kuten kuviosta kuusi voi havaita, tietoturvariskejä tulee osata hallita kaikilla eri organisaatiotasoilla. Kun organisaation kaikki työntekijät eri hierarkiatasoilla noudattavat yhteistä tietoturvaohjetta ja käsittelevät tietoa sovittujen tapojen mukaisesti sekä tekniset suojaustavat toimivat oikein, niin yrityksen toimintataso kehittyy opittujen rutiinien kautta yhä paremmaksi. (Laaksonen 2006, 120.)



KUVIO 6. Tietoturvaohjelman pääelementit ja prosessin kulku. (Laaksonen 2006, 120.)

Jotta yrityksen riskikartoista saadaan mahdollisimman kattavia ja laajoja, tulee riskien kartoitukseen osallistua henkilöitä organisaation jokaiselta tasolta. Tällä tavalla saadaan mielipiteitä eri näkökulmista ja riskejä jää vähemmän tunnistamatta. Riskien tunnistamisessa kannattaa käyttää työryhmiä, joissa on henkilöitä kaikilta organisaation sektoreilta. Lisäksi ulkoiset asiantuntijat tuovat vielä oman näkökulmansa asiaan. (Laaksonen 2006, 121.)

2.8.1 Johdon vastuu tietoturvallisuudessa

Perustan luominen ammattimaiselle ja tehokkaalle tietoturvallisuudelle on johdon tehtävä. Ilman sitoutunutta ja määrätietoista johtoa tietoturva-asioiden hoitaminen ei ole mahdollista. Tietoturvallisuus tulee luoda liiketoimintaa tukevaksi menetelmäksi, joka onnistuessaan saa aikaan kilpailuetua kilpailijoihin nähden. (Miettinen 1999, 48.)

Kuvion kuusi mukaan johto vastaa tietoriskien hallinnan organisoinnista sekä tavoitteista ja toimintaa kuvaavista mittareista. Johtoryhmällä tulee sen lisäksi olla kokonaisvaltainen kuva tietojen suojaustarpeista ja -laajuudesta, tietoriskeistä sekä kehittämismenetelmistä, joka saavutetaan katselmoinnilla. Se on johdon työväline, jolla arvioidaan muutostarpeet. Katselmoinnin jälkeen laaditaan politiikka, jota yrityksen kaikki työntekijät noudattavat. Se on johdon strateginen työväline, jolla organisaation toimintaa voidaan ohjata johdon haluttuun suuntaan. Tässä yhteydessä politiikalla tarkoitetaan koko strategista ohjelmaa, jolla johto tiedottaa tietoturvallisuuden välttämättömyydestä. (Laaksonen 2006, 121.)

2.8.2 Esimiehen vastuu tietoturvallisuudessa

Esimiesten vastuu tietoturvallisuudessa on huomattava. Heille on asetettu kaksi tavoitetta tietoriskienhallinnassa. Ensimmäinen tavoite tietoriskien tiedostaminen on toimintayksikön toiminnassa. Toinen tavoite on tilanteiden tunnistaminen sekä toimintamenettelyjen kehittäminen niitä varten. Esimiesten tulee keskittyä sisäisten riskien torjumiseen, jota he suorittavat yrityksen vanhoja käytäntöjä muuttamalla turvallisempaan suuntaan. Sisäiset riskit ovat nimensä mukaisesti yrityksen sisältä tulevia kuten laiminlyönnit, vastuuntunnoton tiedonsiirto ja tietovuodot. Kun sisäiset toimintakäytännöt saadaan kuntoon, niin sitä kautta myös ulkoiset riskit vähenevät. Ulkoisista riskeistä esimerkkeinä voidaan pitää hakkerointia, laitteiden rikkoutumista sekä teollisuusvakoilua. Ulkoisiin riskeihin on myös laadittava toimintaohjeet sekä menettelyt, kuinka toimitaan niiden ilmaantuessa. Tällöin vältytään turhilta toiminnan keskeytyksiltä ja säästetään aikaa ja rahaa. (Kyrölä 2001, 41.)

Esimiesten tulee opettaa alaisilleen tietoturvallisuuteen liittyvät käytännöt ja toimintatavat. Tämä on tärkeää, koska kaikki toimintayksikössä tapahtuneet virheet ja väärinkäytökset ovat esimiehen vastuulla. (Kyrölä 2001, 219.) Tietoturvallisuuteen liittyvien resurssien organisointi ei ole pelkästään johdon tehtävänä, vaan käytännön järjestelyt kuuluvat esimiehille heidän toimintayksiköissään. Heidän tulee suunnitella ja luoda tarpeelliset raportointi- ja seurantajärjestelmät, joiden avulla valvotaan tavoitteisiin pääsemistä liiketoimintayksikön tasolla. Suunniteltaessa raportointi ja seurantajärjestelmiä, myös henkilöstön ajatukset kannattaa ottaa

huomioon, koska toiminnan muutos-vaiheessa vastarinta on vähäisempää ja siinä vaiheessa henkilöstö on jo sisäistänyt toiminnan tavoitteet. (Laaksonen 2006, 122.)

2.8.3 Henkilöstön vastuu tietoturvallisuudessa

Henkilöstön tulee noudattaa vaitiolovelvollisuutta sekä yhteisiä ohjeita ja toimintamenetelmiä. Heidän tulee myös kehittää aktiivisesti tietoriskien hallintaa. Se tapahtuu jokapäiväisten toimintojen kautta. Kun työntekijä huomaa jonkun epäkohdan, joka vaarantaa yrityksen tietoturvallisuutta, hän ottaa yhteyden esimiehiin ja lähtee sitä kautta selvittämään ongelmaa. Näin toimintaa kehitetään ja tietoturvallisuus paranee vähitellen. (Kyrölä 2001, 217.) Henkilöstöllä pitää olla kuva siitä, että tietoturvallisuus on kiinteä osa jokaisen työnkuvaa. Tätä kautta henkilöstön toiminta saadaan turvallisemmaksi sekä motivoituneemmaksi. (Laaksonen 2006, 122.)

2.8.4 Sidosryhmien odotukset tietoturvallisuudesta

Yritykset eivät ole olemassa vain itseään varten, vaan ne toteuttavat omistajien ja sijoittajien niille määräämää tehtävää. Tieto tulee suojella sidosryhmien kannalta sen takia, että se voidaan rinnastaa yrityksen arvoon. Jos tietoa käytetään huolimattomasti, yritys voi kokea taloudellista tai imagoa heikentäviä menetyksiä. Tämän takia yrityksen tavoitteena kuuluu olla tiedon säilyttäminen yrityksen sisällä sekä sen jakaminen vain oikeille sidosryhmille.

Yrityksen sidosryhmiä kiinnostaa eniten se, kuinka yritys pystyy suojaamaan heidän ydintietonsa. Niitä ovat tuotekehitystiedot sekä yrityksen tieto, omaisuuden arvo ja sen käsittelytavat. Johdon tehtävä taas on antaa markkinoille tietoa yrityksen tilasta, jonka perusteella sijoittavat määrittelevät sen arvon. Jotta sijoittajien kiinnostus on taattua tulevaisuudessa, täytyy johdon antaa kuva hyvästä riskitietoisuudesta ja sen valmiuksista. Sen lisäksi johdon täytyy hallita tiedon suojaaminen eri olomuodoissa sekä antaa kuva toiminnan jatkuvuuden hallintavalmiudesta. (Kyrölä 2001, 53- 54.)

2.8.5 Lakien velvoitukset tietoturvallisuudessa

Yritysten tietoturvallisuutta velvoittavat kotimaiset ja kansainväliset lait. Yleensä lait ovat hyvin yleisluontoisia ja todellinen käytännön tietoturvallisuudesta huolehtiminen jätetään yritykselle. Sen kannalta on tärkeää kartoittaa ne pakottavat lait, jotka ohjaavat tietoturvan suunnittelua, ylläpitoa ja kehittämistä. Kansainvälisten lakien tarkoituksena on taata tietoturvallinen yhteiskunta, jossa otetaan huomioon niin yrityksen kuin tavallisen ihmisenkin tietoturvaoikeudet.(Laaksonen 2006, 18.)

3 TUTKIMUSYMPÄRISTÖ

Työn tutkimusympäristönä toimii Suomen vähittäiskaupan ala. Kuten kuviosta seitsemän voidaan havaita sen myynti on laskenut 2,5 prosenttia vuoden 2009 aikana. Se on suhteellisen vähän verrattuna koko kaupan laskuun, joka on ollut 17,2 prosenttia. Vähittäiskaupan myynnin pientä laskua voidaan selittää päivittäistavarakaupan positiivisella kasvulla (2,4 %).

	Vuosimuutokset neljänneksittäin %				**Uusimman kuukauden vuosimuutos%***	**Kumulatiivinen vuosimuutos****
	07-09/08	10-12/08	01-03/09	04-06/09	08/09	01-08/2009
Kauppa yhteensä (G)	10,1	-2,4	-14,9	-18,9	-18,8	-17,2
Vähittäiskauppa (47)	5,4	2,2	-2,5	-2,9	-3,4	-2,5
päivittäistavara-kauppa	8,6	6,7	1,8	2,9	1,4	2,4

KUVIO 7. Liikevaihdon vuosimuutos kaupan eri aloilla neljänneksittäin- elokuussa 2009 ja koko alkuvuonna 2009. (Vähittäiskaupan myynti, [viitattu 5.11.2009].)

Vähittäiskaupan alalla tulos on painunut negatiiviseksi vuoden 2009 tammikuun sekä maaliskuun välisenä aikana, mutta laskuun se on lähtenyt jo vuoden 2008 loppu puolella. Kokonaiskaupan suurta laskua voidaan selittää lamanvaikutuksilla, joista esimerkkinä voidaan mainita kuluttajien varovainen ostaminen.

Suomen vähittäiskaupan alan suurimmat kilpailijat ovat Kesko ja S-ryhmä. Kummallakin konsernilla on melko samanlaiset liiketoimintamuodot ja pitkä historia alalla. Tämän johdosta ne esitellään työn toimintaympäristössä. PCI-standardin haasteet on otettu vastaan kummassakin konsernissa, mutta kumpikaan näistä toimijoista ei vielä ole standardia saavuttanut.

3.1 Kesko

Tutkimusympäristönä toimii Kesko-konserni, joka on pörssiyhtiö. Keskon ketjutoimintaan kuuluu noin 2000 kauppaa Pohjoismaissa, Baltiassa, Venäjällä sekä Valko-Venäjällä. Sillä on neljä tärkeää toimialaa: ruoka, käyttötavara, rauta sekä auto- ja konekauppa. (Kesko, yleiskuvaus toimialoista, [viitattu 1.9.2009].)

Työn kohdeyritys Indoor Group on Keskon omistama suomalainen kodinhuonekalujen ja sisustustuotteiden vähittäiskauppias. Yhtiöön kuuluvat Asko, Sotka sekä Insofa, joka on pehmustettujen huonekalujen kokoonpanoyksikkö. Insoffalla on myös tytäryhtiöt Virossa sekä Latviassa. Indoor Groupin liikevaihto vuonna 2008 oli 177,4 miljoonaa euroa ja henkilöstön lukumäärä 909. Vuonna 2005 Kesko ostin sen koko osakekannan S-ryhmältä, jolloin siitä tuli Indoor Groupin emokonserni. (Indoor Group, [viitattu 1.9.2009].)

Konsernin liikevaihto tammi-kesäkuussa 2009 oli 4 160 milj. euroa, mikä on 13,8% vähemmän kuin edellisen vuoden vastaavana aikana (4 824 milj. euroa). Liikevaihto laski kotimaassa 9,0 % ja ulkomailla 30,9 %. Viennin ja ulkomaisen toiminnan osuus liikevaihdosta oli 17,4 %. Konsernin liikevaihdon kehitykseen vaikuttivat talouden taantuman seurauksena voimakkaasti supistunut rakennusmarkkina sekä auto-, kone- ja käyttötavarakaupan myynnin lasku. Päivittäistavarakaupassa kasvu jatkui tasaisena. (Kesko pörssitiedote, [viitattu 1.9.2009].)

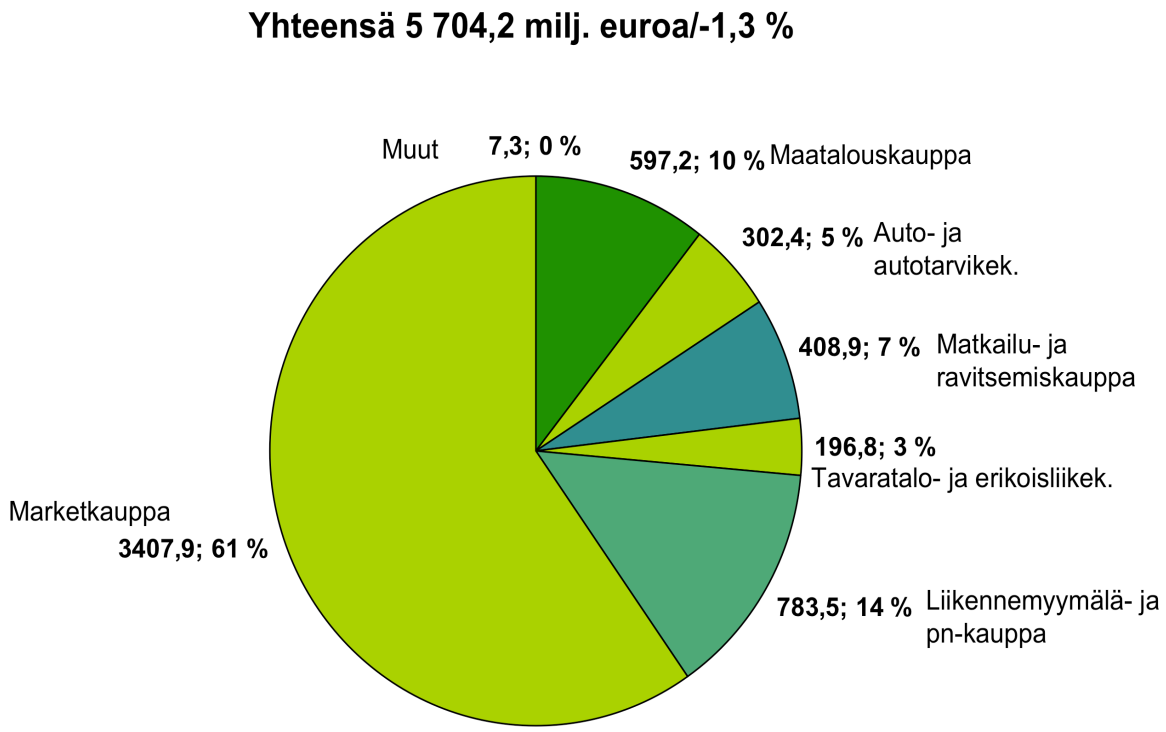
Keskon visio ja arvot on ylittää asiakkaiden odotukset jatkuvan uudistuksen ja yrittäjyyden avulla sekä olla alansa paras tarjoamalla markkinoiden parhaat tuotteet ja palvelut. Keskolle on tärkeää luoda hyvä työyhteisö, jonka avulla toiminta on aloitteellista sekä eettisten tapojen mukaista. Strategiana korostuu terve kannattava kasvu, kuluttaja- asiakaskauppa ja palvelut sekä vastuulliset ja kustannustehokkaat toimintamallit. (Kesko konserni, [viitattu 1.9.2009].)

Keskon tärkeimmät toimialat ovat ruoka- rauta- käyttötavara- sekä auto- ja konekauppa. Kuviossa seitsemän on esitelty toimialat sekä niiden prosentuaalinen osuus liikevoitosta. Ruokakapalla on suurin osuus liikevoitosta, joka on 51%. Seuraavana tulee rautakauppa, mikä on saanut 23% liikevoitosta ja perässä seuraavat käyttötavara ja auto- ja konekauppa 13 prosentilla. Keskon suurimmat toimialat ovat ruoka- ja rautakauppa, jotka yksistään kattavat 68% liikevaihdosta. Lama on vaikuttanut varsinkin käyttötavara sekä auto- ja konekauppaan ja sen takia niiden osuus liikevoitosta on laskenut. Vuoden 2009 alusta syyskuun loppuun käyttötavarakaupan myynnin lasku on ollut 5,3% ja auto- ja konekaupan 36,9%. Autokaupan suurta myynnin laskua selittää myös 1.4.2009 julkaistu uusi autoverolaki, jonka johdosta verotettujen autojen autovero ei sisälly myyntilukuihin. (Kesko pörssitiedote, [viitattu 23.10.2009]).

KUVIO 8. Keskon toimialat (Talma, [viitattu 6.10.2009].)

3.2 S-ryhmä

S-ryhmä on Keskon suurin kilpailija vähittäiskaupan alalla. Heidän liiketoimintansa on keskittynyt paljolti samoille liiketoiminta-aloille muutamaa poikkeusta lukuun ottamatta. S-ryhmän tärkeimmät liiketoimintamuodot ovat maatalous- ruoka- auto- tavaratalo- ja liikennemyymälä sekä polttonestekauppa. S-ryhmän vähittäismyynti on ollut 5 704,2 miljoonaa euroa tammi – kesäkuun välisenä aikana. Keskon ja S-ryhmän liiketoiminta eroja löytyy lähinnä liikennemyymälä- ja polttonestekaupassa sekä matkailu- ja ravitsemiskaupan aloilla. (S-ryhmän vähittäismyynti liiketoiminta-aloittain, [viitattu 10.11.2009].)



KUVIO 9.S-ryhmän liiketoiminta-alat 2009 (S-ryhmän vähittäismyynti liiketoiminta-aloittain, [viitattu 10.11.2009].)

Kuviossa yhdeksän on esitelty eri alojen vähittäismyynnin määrä sekä sen osuus koko liiketoiminnasta Kuten Keskollakin suurin tuotto S-ryhmällä syntyy market-kaupan alalta. Sen kehitys on ollut vahvin verrattuna muihin liiketoimintamuotoihin. Vuonna 2009 kehitystä on tapahtunut 6,5 prosenttia edellis vuoteen verrattuna. Marketkaupan osuus koko liiketoiminnasta on 61 prosenttia, joka on huomattavasti

enemmän kuin Keskolla, jolla se oli 38 prosenttia. Seuraavaksi isoin liiketoiminta-ala on liikennemyymälät- ja polttonestekaupat, joiden vuoden tulos on laskenut 4,2 %. Sen osuus kokonaisliiketoiminnasta on 14%. Kyseinen liiketoimintamuoto Keskolta puuttuu kokonaan, joka on osasyy S-ryhmän suurempaan liikevaihtoon. (S-ryhmän vähittäismyynti liiketoiminta-aloittain, [viitattu 10.11.2009].)

Kolmanneksi isoin liiketoiminta-ala löytyy maatalouskaupasta, jonka tulos on laskenut 17,9 prosenttia vuoden takaisesta tuloksesta. S-ryhmän muut liiketoimintamuodot ovat auto- ja autotarvikekauppa sekä tavaratalo- ja erikoisliikekaupat, jotka ovat noin 10 prosenttia kaikista liiketoimista. Autokaupan kehitys on ollut negatiivista 17,9 prosenttia ja taas tavaratalojen- ja erikoiskauppojen tulos niukasti positiivinen 1,4 prosentilla. (S-ryhmän vähittäismyynti liiketoiminta-aloittain, [viitattu 10.11.2009].) Lama on vaikuttanut suuresti kyseisten liiketoimintamuotojen kohdalla, koska ihmisistä on tullut varovaisempia kuluttajia ja siksi kulutushyödykkeiden kysyntä on laskenut.

4 PCI-STANDARDIN KOHDENTAMINEN

Ensimmäinen kosketus PCI-standardiin tapahtui opinnäytetyön tutkijan työpaikan kautta. Kyseinen työpaikka oli Asko, joka on Indoor Groupin omistama huonekalu ketju. Siellä siirryttiin sirukortinlukijoihin vuonna 2008, jonka ansiosta PCI-standardin hakeminen on jo hyvällä mallilla. Tätä kautta tutkija on päässyt näkemään kuinka PCI-standardia noudatetaan käytännössä ja mitä etuja sillä saavutetaan.

4.1 Aiheen valinta

Työ aloitettiin palaverilla kohdeyrityksen tietoturvasta vastaavien henkilöiden kanssa, jossa keskusteltiin PCI-standardista ja mahdollisista siihen liittyvistä tehtävistä. Palaveri käytiin Tampereen Lielahdessa uuden Asko-myymälän avajaisissa 20.3.2009. Mukana olivat Indoor Groupin tietoturvasta vastaavat henkilöt, joiden kanssa kehitettiin idea selkeyttää ja tulkita PCI-standardi uudella tavalla. Kohdeyritys Indoor Group oli jo päässyt standardin hakuprosesissa melko pitkälle, mutta emokonserni Keskolla se oli vielä monella eri liiketoimintamuodolla kesken tai alkutilassa. Tämän takia tulkitulle ja käännetylle PCI-standardille tulisi käyttöä tulevaisuudessa. Aihe osoittautui haasteelliseksi ja erittäin ajankohtaiseksi, jonka takia sitä ryhdyttiin tutkimaan. Tällä hetkellä Suomessa ei ole monia yrityksiä, jotka ovat PCI-standardi sertifikaatin saavuttaneet, mutta sen hakeminen on jo käynnistynyt monilla tahoilla. Sen käynnistymiseen johtuva syy on ollut Luottokunta, koska se on asettanut selkeät päämäärät, joihin mennessä isojen toimijoiden standardit tulee olla kunnossa. Muussa tapauksessa yritykset ovat osaltaan itse vastuussa menetyksistä, joita tietoriskien sattuessa yritys kohtaa.

4.2 Työn rajaus

Työn tarkoituksena on järkiperäistää sekä muokata priorisoitua PCI-standardi 1.2:sta selkeämpään muotoon, jonka myötä kohdeyrityksen on helpompi jatkaa

standardin hakemista. PCI-standardi sertifikaatin hakuprosessi olisi ollut aivan liian iso kokonaisuus opinnäytetyöaiheeksi, joten uuden priorisoidun standardin tulkitseminen suomeksi koettiin hyväksi ja riittäväksi rajaukseksi. Työ antaa sertifikaatin hakemiselle apuvälineet sekä yleiskäsityksen, kuinka se tulee suorittaa ja mitä asioita siihen kuuluu. Rajauksen suorittaminen on tehty opinnäytetyöohjaajan sekä Indoor Groupin yhteyshenkilöiden yhteisymmärryksellä. Vanha standardi on saanut paljon moitteita siitä, että se tulee täyttää ensimmäisellä kerralla täydellisesti, jotta sertifikaatti voidaan myöntää. Tämän takia uudessa standardissa on huomioitu kuusi eri tasoa, joita voi alkaa järjestelmällisesti suorittamaan lähtien kriittisimmistä asioista.

4.3 Teoriapohjan keräys

Aiheen rajauksen jälkeen alkoi teorianpohjan keräys. Siinä päämääränä tutkija piti sitä, että siinä tuli käsitellä laajasti asioita, jotka ovat yhteydessä PCI-standardiin. Tämän avulla lukija ymmärtää paremmin standardin vaatimukset ja sisäistää asian helpommin. Teorian tarkoituksena on myös antaa ideoita ja toimintatapoja yrityksille, kuinka he voivat täyttää sen vaatimukset.

Teorian keräämiseen ja siihen perehtymiseen tutkija varasi reilusti aikaa, koska aihe ei ollut entuudestaan tuttu. Teoriaa kerättiin ja prosessoitiin vuoden 2009 huhtikuusta elokuuhun saakka, jonka jälkeen siirryttiin työn muihin osioihin. Tutkija piti tätä kuitenkin erityisen tärkeänä, koska ilman selkeää käsitystä asiasta, työtä olisi ollut hyvin vaikea aloittaa kirjoittamaan.

Teoriaa löytyi PCI-standardin kohdalta erittäin paljon Internetistä, mutta kirjallisuudesta taas hyvin vähän. Tämä on kuitenkin selitettävissä sillä, että PCI-standardi on varsin uusi asia, koska ensimmäinen versio siitä on julkaistu 7.9.2006. (Kallio, [viitattu 20.7.2009]). Tämän takia siitä ei ole vielä ehditty tekemään tutkimuksia tai käsikirjoja, joita olisi voitu käyttää apuna opinnäytetyössä. Luetettavimpina lähteinä toimivat PCI Councilin, Nixun sekä Luottokunnan tekemät verkkojulkaisut, koska ne ovat valtuutettujen PCI-standardi toimijoiden tekemiä. PCI Council tarjoaa verkkosivuillaan myös viimeisimmät versiot standardeista, jotka toimivat osallaan teorian tukena. Viimeisin PCI Councilin standardi 1.2 on ilmestynyt 31.3.2009. Yri-

tysten aloittaessa standardin hakuprosessia, tulee heidän käyttää aina viimeisintä standardia, jonka PCI Council on julkaissut.

Käytännön läheistä teoriapohjaa sain myös kohdeyrityksen yhteyshenkilöiltä tapaamisessa Lahdessa Indoor Groupin toimitiloissa. (Meuronen, Nieminen&Halme 8.8.2009.) Yhteyshenkilöinä toimivat Pertti Meuronen, Jari Nieminen sekä Joonas Halme. He kertoivat PCI-sertifikaatin hakuprosessistaan sekä selvittivät vanhan standardin pykälät perusteellisesti. Palaverissa selvisi, että PCI-standardi 1.1, joka on aikaisempi versio tässä case osion pohjana käytettyyn standardiin 1.2 on monilta osilta hyvin samanlainen kuin vanha standardi. Suurimpana erona uuteen standardiin oli priorisoitu lähestymistapa standardin hakemista varten, jonka ideana oli saada kriittisimmät tietoturvallisuuteen vaikuttavat tekijät ensin kuntoon. Priorisoidun lähestymistavan avulla hakuprosessin kehitystä on helpompi seurata, joka edesauttaa prosessin aikatauluttamista. Palaverissa esiteltiin myös käytännön toimintatapoja, joilla kohdeyritys oli täyttänyt standardin mukaisen tietoturvatason. Tämä antoi hyvää käytännönläheistä pohjaa työn tekemiseen ja auttoi ymmärtämään standardia laajemmin. Käytännön toimintatavat antoivat tutkijalle selkeän käsityksen, kuinka standardi todellisuudessa haetaan ja mihin asioihin huomiota tulee kiinnittää.

Kirjallisuus ei tarjonnut PCI-standardista juurikaan tietoa, mutta tietoturvallisuudesta sitä löytyi vastaavasti hyvin. Tietoturvallisuutta pidetään PCI-standardin ytimenä ja se voidaan jakaa ulkoiseen ja sisäiseen tietoturvallisuuteen. Parhaina lähteinä toimivat yrityksen tietoturvaa käsittelevät kirjat, joita oli hyvin saatavilla niin englanniksi kuin suomeksikin. Kirjoja löytyi hyvin niin Tampereen kaupungin kirjastosta kuin Tampereen ammattikorkeakoulunkin kirjastosta. Ongelmaksi tietoturvallisuudesta kirjoittaessa osoittautui teorian runsaus, koska kaikkea ei pystynyt kertomaan yhdessä opinnäytetyössä. Indoor Groupin yhteyshenkilöt painottivat sähköposti keskusteluissa (28.8.2009) tietoturvallisuuden teoriassa sitä, että esimerkiksi fyysisiä suojauskeinoja ei voida käsitellä kaikessa laajuudessaan, vaan ainoastaan yleisellä tasolla, koska muuten teorian laajuus kasvaa liian isoksi. Tämä vaikeutti suuresti tietoturvallisuusosion tekemistä, koska tutkijan tuli käyttää paljon aikaa miettimiseen, mitä asioita työhön kannattaa laittaa ja mitä jättää pois. Lopul-

ta kuitenkin oikeanlainen tasapaino saatiin tehtyä ja PCI-standardiin liityvät asiat saatiin esitettyä.

Tietoturvallisuuden teoriassa selvitettiin tekijöitä, jotka vaikuttavat negatiivisesti tietoturvallisuuteen sekä tapoja, joilla ne voidaan pitää hallinnassa. Tietoriskeihin on vasta viime vuosina alettu kiinnittää huomiota yrityksissä, vaikka ne ovat olleet aina olemassa. Tämä on johtunut lähinnä siitä, että hyvällä tietoturvalla ei ole saatu suoranaisia liikevoittoja, vaan sillä on saatu ainoastaan minimoitua tappioita. Yritykset eivät ole halunneet panostaa siihen, että tappioita olisi minimoitu, vaan ne ovat keskittyneet luomaan parempia tuloksia. Nykyään on kuitenkin ymmärretty, että tietoturvallisuuteen panostamalla liiketoimintaa on saatu tuottoisammaksi, koska tappiot ovat vähentyneet suhteessa tietoturvainvestointeihin. Tämä on myös PCI-standardin tarkoitus. Näin paljon lisääntyneitä luottokorttien väärinkäyttöjä saadaan vähennettyä sekä yritykselle elintärkeitä tietoja saadaan suojattua.

4.4 Työn rungon luominen ja kirjoitusprosessi

Kun teoriapohja oli hankittu ja käsitelty, alkoi työn rungon luominen. Koska teoriaan oli perehdytty hyvin, osoittautui rungon luominen kohtuullisen helpoksi prosessiksi. Vaikka runko on muuttunutkin kirjoitusprosessin aikana, on siinä silti säilynyt sama perusidea, joka jo työn alkuvaiheessa tehtiin.

Kirjoittamisprosessi aloitettiin elokuun alussa ja se kesti noin syyskuun puoleen väliin saakka. Siinä lähdettiin liikkeelle johdannosta sekä tutkimusmenetelmistä, jonka jälkeen kerrottiin työn rajaukset. Ensimmäisen kappaleen tarkoitus on antaa lukijalle kuva, siitä mitä työ pitää sisällään sekä saada hänet kiinnostumaan aiheesta. Lisäksi kerrottiin tutkimusmenetelmistä, jotka toiminnallisessa opinnäytetyössä olivat sähköposti- ja puhelinkeskustelut sekä yritysvierailut.

Toinen kappale käsitteli puhtaasti teoriaa, jonka tarkoituksena on täsmentää PCI-standardin tarkoitusta sekä antaa selkeä kuva siitä, mihin sillä pyritään ja mitä etuja sillä saavutetaan. Sen lisäksi teorian tehtävä oli perehdyttää lukija PCI-standardin hakemiseen sekä standardin hyväksymiseen, jotta PCI-sertifikaatti voidaan saada. Kun PCI-standardi oli käsitelty, oli aika kertoa kauppiaiden raportoin-

tivelvollisuudesta. Siinä käytiin läpi eri kokoisten yritysten vuosittaiset toimenpiteet, joita heidän tulee raportointiaan varten tehdä. Kappaleen apuna käytettiin Luottokunnan tekemiä kaavioita, jotka löytyvät liitteistä 2 ja 3. Niiden avulla yritysten on helppo luokitella itsensä oikeaan kategoriaan, josta nähdään mitä tietoja heidän tulee raportoida.

Sen jälkeen käsittelyn kohteena oli PCI-standardin ydin eli tietoturvallisuus. Siihen kuului asiakokonaisuuksia tiedon tärkeydestä yritykselle tietoriskien hallintaan. Tiedon tärkeys yrityksille-kappaleessa käsiteltiin, miksi yritysten tulee suojata tietoaan ja mikä on suojeltavaa tietoa. Tämä kappale on erityisen tärkeä siksi, että monet yritykset käyttävät tietopääomaansa pääliiketoimintana. Tämän vuoksi heidän tulee tietää, kuinka kyseinen tieto saadaan pidettyä yrityksen sisällä ja miten siihen tulee pyrkiä. Kappaleessa painotettiin, että tieto on avaintekijä tuottavuudelle, kilpailukyvylle sekä taloudellisille saavutuksille, jonka takia sitä ei saa päästää leviämään yrityksen ulkopuolelle.

Tietoturvallisuus kappaleessa tutkittiin tiedon olomuotoja sekä sen ulottuvuuksia. Kappaleen tarkoituksena oli kertoa, että tieto ei aina ole selkeästi dokumentoitua, vaan se voi olla yksittäisten työntekijöiden hallussa. Siksi se tulee ottaa huomioon yrityksen tietoturvan suunnitteluvaiheessa. Kappaleessa paneuduttiin tapoihin, joilla eri olomuodissa oleva tieto saadaan pidettyä yrityksen sisällä ja kuinka se saadaan kaikkien tietoisuuteen ja käyttöön. Tämä asettaa yrityksen tietoturvalle suuria haasteita, mutta oikeanlaisilla sopimuksilla ja tiedon käsittelytavoilla tämäkin tietovaranto saadaan pidettyä hallinnassa.

Tietoturvallisuuden vastuita käsiteltiin monesta eri näkökulmasta. Vaikka tietoturvallisuuden ylimmän vastuun kantaakin yrityksen johto, niin se ei tarkoita sitä, että he ovat yksistään vastuussa siitä. Kappaleessa selvisi, että tietoturvallisuus on yrityksen yhteinen vastuu, joka koskettaa kaikkia siinä työskenteleviä henkilöitä. Lisäksi yritysten on oltava vakuuttuneita, että myös yhteistyökumppanit suhtautuvat tietoturvaan sen vaatimalla vakavuudella. Jos heidän tietoturvansa ei ole kunnossa, niin silloin myös oman yrityksen tiedot ovat vaarassa. Tämän takia PCI-standardi koskettaa myös alihankkijoita ja muita yhteistyökumppaneita. Yrityksiä sitovat myös lait, mutta niistä voidaan todeta, että ne ovat melko yleisluonteisia,

jonka johdosta todellinen tietoturvallisuuden vaaliminen jää viime kädessä aina yrityksille.

4.5 Toimintaympäristön esittely

Toimintaympäristön esittelyssä selvitettiin Keskon tämän hetkistä tilaa sekä sen eri liiketoimintamuotojen yhteyksiä toisiinsa. Siinä selvitettiin myös kohdeyrityksen yhteyttä Kesko-konserniin sekä käytiin läpi liiketoiminnan tärkeimpiä tunnuslukuja.

Toimintaympäristön esittelyssä kerrottiin myös Suomen vähittäiskaupan muutoksista viime vuosina sekä esiteltiin toinen suuri vähittäiskaupan kilpailija S-ryhmä. Kappaleen tarkoituksena oli myös vertailla näiden kahden suuren toimijan liiketoimintamuotoja sekä sitä, kuinka heidän osuutensa eri liiketoimintamuojen kesken rajautuu.

Toimintaympäristö kappaleesta voidaan huomata selkeästi laman vaikutukset Keskon ja S-ryhmän eri liiketoimintamuotojen välillä. Ne näkyvät varsinkin autorauta- sekä käyttötavarakaupan aloilla. Kummankin konsernin päivittäistavarakauppa on lamasta huolimatta päässyt positiiviseen tulokseen ja jopa kasvanut muutaman prosenttiyksikön.

4.6 Toiminnallisen osuuden tekeminen

Toiminnallisen osuuden lopputulemana saatiin produkti eli kohdennettu PCI-standardi Indoor Groupille, joka löytyy liitteestä yksi. Kyseinen prosessi vaati paljon aikaa, koska sen tekemiseen kuului monia eri työvaiheita. Toiminnallisen työn tekeminen aloitettiin syyskuun puolesta välistä ja se saatiin valmiiksi marraskuun alkuun mennessä.

Sen tekemisessä lähdettiin liikkeelle aikaisempien standardien prosessoinnilla ja tulkinnalla. Ongelmana ensimmäisessä PCI standardi 1.1:ssä oli se, että siihen ei oltu tehty ollenkaan välivaiheita, joilla yritys voi lähteä standardia hakemaan. Standardissa oli ainoastaan listattuna sen vaatimukset, jotka tuli kaikki täyttää yhdellä kertaa, jotta standardi saadaan lunastettua. PCI-standardi 1.2:ssa tämä on

kuitenkin huomioitu priorisoidussa tehtäväjärjestyksessä, mutta ne on kuitenkin sijoitettu standardiin sekaisin eri kappaleisiin. Tämän takia standardi on käytännössä työläs täyttää ja se hankaloittaa standardin ymmärtämistä. Toinen ongelma on, että hakuprosessin edistymistä vaikea seurata, jolloin prosessin aikatauluttaminen on haasteellista. Kummassakin standardissa on myös vaara ymmärtää pykälät väärin, koska ne on joiltain osin selitetty melko suppeasti.

Kun aikaisempien standardien ongelmat oli löydetty, oli aika ryhtyä luomaan uutta toimivampaa ratkaisua. Siinä lähdettiin liikkeelle priorisoidun standardin 1.2 kääntämisellä suomeksi. Kääntämistyössä vierasperäiset termit osoittauivat alussa ongelmaksi, mutta sanakirjan avulla ne saatiin kuitenkin suomennettua ja tulkittua uuteen standardiin. Suomennoksen myötä standardista saatiin entistä ymmärrettävämpi ja tulkinnanvaraisuuksia saatiin karsittua. Standardin tueksi on tehtiin termistö, jonka tarkoituksena on auttaa lukijaa ymmärtämään hankalat pykälät, jos niitä ei standardissa oltu pystytty erikseen tulkitsemaan. Suomenkielisen standardin avulla hakuprosessi nopeutuu, koska hakuprosessin työvaiheista saadaan poistettua sen suomentaminen ja pykälien tulkitseminen.

Kun työ oli suomennettu, se järjestettiin uudelleen siten, että standardiin muodostui ainoastaan kuusi päälukua vanhan 12 luvun sijaan. Vanhassa standardissa asiat olivat merkitty tärkeysjärjestyksiin, mutta ne olivat sekaisin kaikissa 12 pääluvussa. Toiminnallisessa työssä lähdettiin liikkeelle siitä että vanha standardi aukaistiin ja jäsennettiin uudestaan sen mukaan mihin priorisoituun tehtävä järjestykseen kukin pykälä kuuluu. Kun pykälät oli järjestetty tärkeysjärjestykseen, tuli ne koota yhteen ja jakaa kuuteen lukuun siten, kuinka akuutti mikäkin asia oli. Koska standardi eteni tärkeysjärjestyksen mukaan, saatiin siihen selkeä parannus käytännön hakuprosessia varten. Uuden järjestyksen johdosta sitä ei tarvitse enää selailla, vaan standardia voidaan lukea ja täyttää alusta alkaen. Tämän takia hakuprosessin valmistumista on helpompi seurata ja kokonaisprosessia aikatauluttaa.

Kun standardi oli käännetty ja tulkittu uusiksi siihen lisättiin vielä jokaisen pääluvun alkuun tiivistelmä, jossa käsitellään kappaleen tärkeimmät asiat. Niiden tarkoitus on antaa yleiskatsaus kuhunkin tasoon, jonka ansiosta standardia on helpompi

lähestyä. Produktissa pyrittiin antamaan myös toimivia käytännön toimintamalleja, joita hakuprosessissa voitaisiin käyttää. Käytännön toimintamallit ovat peräsin Indoor Groupin tekemistä ratkaisuista heidän standardin hakuprosessissaan. Tätä kautta standardiin on saatu uusia ulottuvuuksia, joita tulevat hakijat voivat käyttää apuna omassa toiminnassaan. Sen takia kaikkia toimintatapoja ei tarvitse itse keksiä, vaan voidaan käyttää hyväksi havaittuja toimintatapoja täyttää jokin pykälä. Kaikki toimintatavat eivät toimi jokaisessa yrityksessä, mutta se auttaa yrityksiä ymmärtämään mahdollisia ratkaisumalleja ongelmatilanteisiin.

Yrityksiä koskevan standardin jälkeen on sijoitettu palveluntarjoajia koskeva PCI-standardi, jossa on jäsennettynä heitä koskevat vaatimukset. Sen tarkoituksena on varmistaa, että myös palveluntarjoajien tietoturva on tarpeeksi vahva ja se kohtaa PCI-standardin yleiset vaatimukset. Jos yhteistyökumppaneiden tietoturva ei ole yhtä vahva kuin standardia noudattavan yrityksen, niin tällöin myös kyseisen yrityksen tietoturva on uhattuna. Tämän takia palveluntarjoajien kohdalta tulee olla varmuus, että he noudattavat sovittuja toimintatapoja sekä vaalivat omaa tietoturvaansa.

Palveluntarjoajia koskevan osion jälkeen käsiteltiin vaihtoehtoisia suojausmenetelmiä, joita voidaan käyttää standardin 5.2 pykälissä. Vaihtoehtoisilla suojausmenetelmillä annetaan yrityksille tapoja päästä hyvään tietoturvatasoon, vaikka he eivät pystyisikään täyttämään PCI-standardin vaatimia teknisiä suojausmekanismeja. Esimerkkeinä vaihtoehtoisista suojaustavoista voidaan pitää pääsyn rajoittamista tietokantaan sekä sellaisten sovelluksien käyttämistä, jotka estävät tai havaitsevat tietokantoihin kohdistuvat hyökkäykset. Vaihtoehtoisten suojausmenetelmien toimivuus tulee kuitenkin varmistaa perusteellisesti käyttöönoton jälkeen, koska ne eivät suoranaisesti täytä PCI-tietoturva standardin vaatimuksia.

4.7 Tominnallisen osuuden merkitys kohdeyritykselle

Aiheen merkitys kohdeyritykselle on suuri, koska sen PCI-standardin hakuprosessi on kesken sekä emokonserni Keskon hakuprosessi vasta alkutilassa. Tämän takia kiinnostusta löytyi niin Indoor Groupin kuin Keskonkin puolelta. Työn tarkoituksena on auttaa standardin hakemista tulevaisuudessa, koska jossain vaiheessa uuteen

standardiin siirtyminen tulee kuitenkin ajankohtaiseksi. Tämän työn avulla uusi standardi on helpompi sisäistää sekä sen tärkeimmät tietoturvaan vaikuttavat seikat ovat helposti löydettävissä. PCI-standardi auttaa yritystä myös ymmärtämään tietoturvallisuutta laajemmin. Yritykset oppivat ymmärtämään, että tietoturvallisuus ei ole pelkästään teknisiä ratkaisuja vaan myös fyysisiä toimenpiteitä. Niistä esimerkkinä voidaan pitää ihmisten jatkuvaa kouluttamista sekä parempaa tilojen ja turvallisuustekijöiden suunnittelua yritysten tiloissa. Kohdennetun standardi myös nopeuttaa hakuprosessia sekä helpottaa yritystä aikatauluttamaan sen kestoa. Sen etuina voidaan todeta olevan suomenkielinen käännös sekä uudelleen järjestetty runko, joka helpottaa projektin edistymisen tarkkailua.

5 JOHTOPÄÄTÖKSET

Aiheena PCI-standardin kohdentaminen Indoor Groupin tarpeisiin oli erittäin haastava. Haastavaksi aihe osoittautui sen takia, että tutkijalla ei ollut juurikaan tietoperustaa aiheesta ennen sen aloittamista. Kuitenkin työn edetessä ymmärrys PCI-standardia kohtaan kasvoi ja sen idea yrityksille tarkentui. Aluksi kyseinen standardi tuntui ainoastaan tavalta rahastaa yrityksiä tekemään suuria uhrauksia tietoturvaan, mutta lopuksi kuitenkin selvisi, että standardin tarkoitus on suojella yritysten ja Luottokunnan välistä maksutoimintaa, josta hyötyvät kummatkin osapuolet. Standardi tuo myös huomattavaa kilpailuetua, koska vain harva yritys Suomessa on sen saanut lunastettua. Tämän takia PCI sertifikaatin saaminen on yrityksille tärkeää.

PCI-standardi auttaa yrityksiä ymmärtämään omaa tietoturvaansa laajemmin. Sen tarkoitus ei ole tarjota vain teknisiäratkaisuja, vaan antaa vastuu tietoturvallisuudesta yrityksessä työskenteleville ihmisille. Tällä tavoin sen kehittämisestä saadaan jatkuvaa toimintaa. PCI-standardin etuna voidaan pitää sen tarjoamaa maksukorttijärjestelmän globaalia yhdenmukaistamista. Tämän avulla ostaminen helpottuu ja asiakkaat voivat olla varmoja, että maksutapahtumat ovat turvallisia, olivatpa he sitten missäpäin maailmaa tahansa. Standardin saavuttamisen myötä luottokortti väärinkäytökset vähenevät, aikaisempaa vaativamman tietoturvan seurauksena.

PCI-standardista hyötyvät myös pienet yritykset, vaikka sen suorittamista ei heiltä vaadittaisikaan. Sen avulla he voivat tarkastaa oman yrityksensä tietoturvallisuustason itsearvinointikaavakkeita hyväksi käyttäen. Siten yritykset oppivat ymmärtämään mahdollisia riskejä ja suojautumaan niitä vastaan ennaltaehkäisevästi. Jos yritykset päättävät suorittaa standardin hyväksytysti, niin se antaa myös elintärkeää kilpailuetua markkinoilla toimiviin muihin yrityksiin verrattuna.

Suuren edun työn onnistumiseen antoi sen kohdeyritys Indoor Group. He antoivat perusteellisen pohjustuksen itse PCI-standardista sekä sen lisäksi elintärkeitä käytännön toimintatapoja, jotka auttoivat ymmärtämän PCI-standardin hakuprosessia. Näin tutkijan oli helpompi aloittaa työn prosessointi, koska kohdeyritys oli vahvasti mukana tukemassa sitä. Käytännön toimintatapojen kautta oikea ajatusmalli PCI-standardista tarkentui ja kohdennetusta standardista saatin tehtyä tarkoituksen mukainen palvelemaan kohdeyrityksen tarpeita.

Toiminnallisen työn tuloksena saatiin produkti eli kohdennettu standardi Indoor Groupin tarpeisiin. Uuden PCI-tietoturvastandardin vahvuudet pidettiin työssä ja heikkouksia kohennettiin. Parannuksien avulla kohdeyrityksen on entistä helpompi jatkaa standardin hakua. Kohdennettu standardi säästää yritysten aikaa sekä uuden järjestyksensä avulla yritykset pystyvät seuraamaan standardin hakuprosessin kehitystä tarkemmin. Toiminnallisen osuuden onnistumista kohdeyritys kommentoi sähköpostikeskustelussa 16.10.2009 siten, ”*että olisipa heilläkin ollut kohdennettu standardi, silloin kun PCI-standardin hakuprosessi käynnistyi”*. Vaikka Indoor Group ei itse päässyt käyttämään kohdennettua standardia hakuprosessinsa käynnistymisessä, niin he voivat silti käyttää sitä apunaan prosessin loppuun viemisessä. Indoor Group uskoo työn olevan lisäksi suureksi avuksi emokonserni Keskolle, jolla PCI-standardin hakuprosessi on vielä kesken monilla muilla liiketoimintamuodoilla. Indoor Group uskoo kohdennetun standardin säästävän aikaa sekä helpottavan hakuprosessin eri vaiheita, jotka olivat työn tärkeimpiä tavoitteita. Sen lisäksi työn tarkoituksena oli tulkita pykälät siten, että ne olisivat ymmärrettävämmässä muodossa. Kohdeyrityksen mielestä tässäkin asiassa onnistuttiin, koska standardi saatiin käännettyä suomeksi ja siinä tarjottiin myös mahdollisia toimintamalleja sen eri vaatimuksissa. Näiden seikkojen myötä standardista saatiin selkeämpi ja parempi kokonaisuus, jonka uskotaan antavan apua tulevaisuudessa PCI-standardin hakuprosessissa.

LÄHTEET

Calder, A. 2005. A business guide to information security. London: Kogan Page

Danilotschkin-Forsman, T. 2003. IF vahinko vakuutus lehdistötiedote. [Verkkojulkaisu]. [Viitattu 1.9.2003].Saatavana: http://www.if.fi/web/fi/corporate.nsf/noframes/8DEA6E6F8D8F5D97C1256D94003C3A37/$FILE/LEHDIST%C3%96TIEDOTE%201.9.%20tietoriskit.pdf

Hakala, M, Vainio, M & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Porvoo: WS Bookwell

Hämäläinen, P. 2009. Turvallisen korttimaksun teoria ja käytäntö. [Verkkolehtiartikkeli] Tietokone [Viitattu 10.9.2009] Saatavana: http://www.tietokone.fi/lukusali/artikkelityyppi.asp?articletype_id=18

Indoor Group.[Viitattu 1.9.2009] [WWW-dokumentti]. Saatavana: http://www.indoorgroup.fi/

Kallio, J. PCI vaatimukset ja tilanne suomessa.[Verkkojulkaisu]. [Viitattu 20.7.2009]. Saatavana: http://www.nixu.com/news/events/download/PCI_Nixu_v2_jakelu.pdf

Kesko. Konserni. [24.7.2009]. [Viitattu 1.9.2009]. [WWW- dokumentti]. Saatavana: http://www.kesko.fi/index.asp?id=FF60B08E63C34667A8261A0B08FC2365

Kesko. Pörssitiedote 24.7.2009. [Viitattu 1.9.2009]. [WWW-dokumentti]. Saatavana:http://www.kesko.fi/index.asp?id=C8F926B0E7054CFE8893C73D379DAF27&data=1,00308B787886459385F296A5AFD4FA74,53612341837D41C69C604620F289AA5C

Kesko. Yleiskuvaus toimialoista. [Viitattu 1.9.2009]. [WWW-dokumentti]. Saatavana:http://www.kesko.fi/index.asp?id=FF60B08E63C34667A8261A0B08FC2365

Korttimaksamisen turvastandardit. [Viitattu 21.10.2009]. [WWW-dokumentti]. Saatavana: http://www.point.fi/Finland/Palvelut/point_ssl_reitityspalvelu/pci/

Kyrölä, T. 2001. Esimies ja tietoriskien hallinta. Juva: WS Bookwell OY

Kyrölä, T. Tietoturvallisuuden kehittäminen. [verkkojulkaisu]. [Viitattu 27.2.2009]. Saatavana: http://www.tml.tkk.fi/Opinnot/T110.454/2005/C10Suojattava_tieto.pdf

Lahti, J. 2009. IT Viikko.Tietoturvaosaamista vakuutetaan sertifikaatilla. [verkkojulkaisu]. [Viitattu 16.11.2009] Saatavana: http://m.itviikko.fi/?page=showSingleNews&newsID=20099782

Laaksonen, M, Nevasalo, T ja Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Oy Nordprint Ab

Luottokunta. PCI-tietoturvastandardi [Verkkojulkaisu]. [Viitattu 20.8.2009] Saatavana: http://www.luottokunta.fi/fi/pci/

Luottokunta.Kauppiaan raportointivelvollisuus PCI-tietoturvastandardin noudattamisesta. [Verkkojulkaisu]. [Viitattu 20.8.2009]. Saatavana: http://www.luottokunta.fi/midcom-serveattachmentguid-68bcaadc1dc011dd9734e527878f0c7c0c7c/kauppiaan_pci-raportointivelvollisuudet.pdf

Meuronen, P. [Sähköposti keskustelu]. [Viitattu 16.10.2009]

Meuronen, P, Nieminen, J & Halme, J. [Haastattelu]. [Viitattu 8.8.2009]. Lahti

Miettinen, J. 1999. Tietoturvallisuuden johtaminen. Jyväskylä: Gummerus Kirjapaino Oy

Miettinen, J. 2002. Yritysturvallisuuden käsikirja. Jyväskylä: Gummerus Kirjapaino Oy

Nixu.PCI-auditoinnit ja -palvelut. [Verkkojulkaisu]. [Viitattu 20.7.2009]. Saatavissa:http//www.nixu.fi/is/pci

Nixu. Web Journal [Viitattu 8.9.2009]. [WWW-dokumentti]. Saatavana:http://blog.nixu.fi/category/pci/

Paavilainen, J. 1998. Tietoturva. Jyväskylä: Suomen Atk-kustannus Oy

PCI Security Standards Council. PCI Quick Reference Guide. [Verkkojulkaisu]. [Viitattu 20.8.2009]. Saatavana: https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf

PCI Security Standards Council, PCI-standardi 1.1, [Verkkojulkaisu]. [Viitattu 20.10.2009].)Saatavana: https://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf

PCI Security Standards Council, Priorized approach for DSS 1.2, [Verkkojulkaisu]. [Viitattu 16.10.2009].) [PDF- dokumentti]. Saatavana: https://www.pcisecuritystandards.org/education/prioritized.shtml

PK-yrityksen riskienhallinta. Tietoriskien hallinta [Verkkojulkaisu]. [Viitattu 27.2.2009]. Saatavana: http://www.pk-rh.fi/pdf/kalvot/tietoriskien-hallinta-kalvosarja-pdf

Pohjola- yhtiöiden julkaisuja 1. Tietoriskit

Siltala, T. 25.2.2008. Tietoviikko.Kauppa pleaa riskillä. [Verkkoartikkeli].[Viitattu 30.9.2009] Saatavana: http://www.tietoviikko.fi/taustat/kaikki_jutut/article135796.ece

S-ryhmän vähittäismyynti liiketoimintalaoittain. [Verkkojulkaisu]. [Viitattu 10.11.2009].Saatavana:http://mediapalvelu.s-kanava.fi/s-ryhma/s-ryhma_lukuina/fi_FI/sryhman_vahittaismyyntilukuja/_files/82049925913249721/default/MY2009_1_6.pdf

Suominen, A. 2003. Riskienhallinta.3.uud.p. Helsinki: WSOY

Talma, A. Kesko - Presentaatiot, [Ppt-esitys]. [Viitattu 6.10.2009].)Saatavana: http://www.kesko.fi/index.asp?id=91E0B299355C4D049C3B375DB31894D2&data=1,00308B787886459385F296A5AFD4FA74,34FF79D6849A460BAD0B8FFDAE4DCD12

Tilastokeskus. Vähittäiskaupan myynti.[Verkkojulkaisu]. [Viitattu 5.11.2009]. Saatavana:http://www.stat.fi/til/klv/2009/08/klv_2009_08_2009-10-15_tie_002.html

Vehviläinen, T. Pci-auditointiprosessi ja käytännön kokemuksia auditoinneista. [Verkkojulkaisu]. [Viitattu 20.8.2009]. Saatavana: http://www.nixu.fi/is/pci/PCI-auditointiprosessi.pdf

LIITTEET

1 (1)

LIITE 1

PCI-standardin kohdentaminen Indoor Groupin tarpeisiin

Tämän luvun tarkoituksena on selventää PCI-standardin hakemiseen sekä täyttämiseen liittyviä seikkoja. Standardin hakeminen ei ole yksinkertainen prosessi, vaan siinä tulee perehtyä hyvin yrityksen sisäiseen ja ulkoiseen tietoturvaan.

Ensimmäisenä tulee lähteä liikkeelle siitä mitä standardi käsittelee ja ketkä kohde yrityksessä ovat tekemisissä näiden asioiden kanssa. Kuten aikaisemmin on jo selvinnyt, standardin vaativuus on suhteessa yrityksen maksukorttitapahtumien määrän kanssa. Case yritystä ajateltaessa standardi on laajimmassa muodossa, koska maksukorttitapahtumiem määrä ylittää kuuden miljoonan rajan vuodessa.

Standardi koostuu 12 eri vaatimuksesta, jotka on priorisoitu kuuteen eri tärkeysjärjestykseen. Kohdennetussa standardissa on 12 pääluvun sijaan kuusi lukua, jotka on muodostettu niiden tärkeysjärjestyksen mukaan. Tämän ansiosta standardia voidaan lähteä täyttämään alusta alkaen ja sen etenemistä on helppo seurata. Standardin tarkoituksena on suojata aluksi tietoturvallisuuden kriittisimmät osiot, jonka jälkeen voidaan jatkaa täyttämään tietoturvallisuuden muita vaatimuksia. Kohdennetun standardin ansiosta Indoor Groupin on helpompi jatkaa PCI-sertifikaatin hakuprosessia, koska he voivat käyttää kyseistä standardia työkaluna sen saavuttamiseksi.

1 TASO

Ensimmäisellä tasolla perehdytään asioihin, jotka tulee saada heti kuntoon haettaessa PCI-standardia. On tärkeää muodostaa yritykselle täydellinen verkkokaavio, jonka avulla selvitetään kaikki yhteydet, joilla on pääsy kortinhaltioiden tietoihin.

Yrityksen tulee välttää myös tallentamasta ylimääräistä kortinhaltijoita koskevaa tietoa, koska niiden suojelemiseen joutuu käyttämään paljon resursseja. Tämän takia kannattaa säilyttää vaan tieto, josta on yritykselle hyötyä tai jos se on lain velvoittama.

Suojaa kortinhaltijatiedot asentamalla palomuuriohjelma ja ylläpitämällä sitä

1.1 Päivitetty verkkokaavio, jossa on merkittu kaikki yhteydet kortinhaltijoidentietoihin. Verkkokaavion tulee myös sisältää langattomat yhteydet, jos niitä käytetään.

Suojaa tallennetut kortinhaltijatiedot

1.2 Pyri tallentamaan kortinhaltijoiden tietoja, niin vähän kuin mahdollista. Luo yleisesti tiedossa olevat käytännöt, kuinka tietoja käsitellään (säilyttäminen/ tuhoaminen). Tallenna ainoastaan ne tiedot, jotka vaaditaan juridisista syistä.

1.3 Älä tallenna käyttöoikeuksien todennustietoja edes salattuina, koska niiden päästessä vääriin käsiin tietomurron riski kasvaa.

1.3.1 Älä tallenna kortin tietoja magneettiraidalta tai sirulta kokonaisuudessaan mihinkään. Paras tapa tallentaa tietoa on maskata sitä eli näyttää ainoastaan esimerkiksi kortin viisi viimeistä numeroa ja peittää loput. Tällä tavoin henkilöllisyys voidaan tarkastaa, mutta kortin tiedot eivät pääse leviämään.

1.3.2 Älä tallenna kortin kolme- tai neljänumeroisia varmennenumeroita kokonaisuudessaan yhteen paikkaan, koska se luo suuren tietototurvariskin.

1.3.3 Älä tallenna henkilökohtaista tunnuslukua mihinkään.

Rajoita fyysinen pääsy kortinhaltijan tietoihin

1.4 Tuhoa kortinhaltijoiden tiedot, kun ne eivät enää ole yritykselle relevantteja liiketoiminnallisista tai juridisista syistä. Näin vältytään uhraamasta kallisarvoisia resursseja tietojen suojaamiseen.

1.4.1 Paperit tulee silputa, polttaa tai hävittää kemiallisesti, jotta niiden sisältö ei pääse leviämään yrityksen ulkopuolelle.

1.4.2 Sähköisessä muodossa oleva tieto tulee tuhota kovalevyltä esimerkiksi magneetin avulla tai jollain muulla tavalla, jotta kortinhaltijan tietoja ei voida koostaa uudestaan.

2 TASO

Toisella tasolla on syytä kiinnittää huomiota palomuurien toimintaan. Ne tulee määrittää tarkasti, jotta asiattomat tahot eivät pääse käsiksi kortinhaltijoiden tietoihin. Tärkeintä verkkoliikenteen rajoittamisessa palomuurein on se, että maksukorttiliikenne toimii moitteettomasti, mutta muu liikenne on tarkoin vartioitua.

Asennettaessa uusia komponentteja verkkoon on tärkeää kiinnittää huomiota siihen, että oletusasetuksia tulee muuttaa välittömästi. Tämä parantaa tietoturvaa huomattavasti, koska oletussalasanat ovat kaikkien saatavilla. Toinen tärkeä seikka verkon muuttamisen jälkeen on sisäisen ja ulkoisen verkon haavoittuvuustarkistus. Tämä on syytä toteuttaa kolmen kuukauden välein, vaikka verkkoympäristö pysyisikin muuttumattomana.

Suojaa kortinhaltijatiedot asentamalla palomuuriohjelma ja ylläpitämällä sitä

1.1 Palomuureihin tulee asentaa tarvittavat vaatimukset kaikkien Internet yhteyksien sekä sisäverkkoalueiden välisten yhteyksien kohdalta.

1.2 Tulee luoda dokumentoitu luettelo liiketoiminnan kannalta tarpeellisista palveluista, porteista ja protokollista.

1.3 Määritä palomuurin asetukset siten, että se estää liikenteen epäluotettavista verkoista tietojärjestelmään, jossa on tallennettuna kortinhaltijoiden tietoja.

1.3.1 Rajaa saapuva ja lähtevä liikenne niin tarkasti, että kortinhaltijoiden tietoihin pääsy on mahdotonta.

1.3.2 Turvaa ja synkronoi kaikkien reitittimien asetukset.

1.3.3 Asenna verkon ulkokehän palomuurit langattoman verkon ja kortinhaltijatietojen välille siten, että verkkoa voi käyttää vain niihin tarkoituksiin, joita tarvitaan kaupankäynnin yteydessä.

1.4 Palomuurin asetukset tulee asettaa siten, että se estää kaiken liikenteen verkoista ja palvelemista, joihin ei luoteta lukuun ottamatta maksukorttiympäristön tarvitsemia yhteyksiä.

1.4.1 Yrityksen sisälle tuleva liikenne ohjataan DMZ-vyöhykkeelle, joka tarjoaa lisäsuojausta yrityksen sisäiseen verkkoon.

1.4.2 Sisäinen Internet-liikenne tulee estää pois DMZ-vyöhykkeeltä.

1.4.3 Älä salli sisään tai ulospäin suuntautuvaa liikennettä samassa verkossa, jossa on kortinhaltijoiden tietoja.

1.4.4 Sisäisten osoitteiden siirtymisen estäminen DMZ-vyöhykkeelle.

1.4.5 Sisäänpäin suuntautuvan Internet-liikenteen rajoittaminen DMZ-vyöhykkeen sisäisiin IP-osoitteisiin.

1.4.6 Tilallinen tarkastus, jota kutsutaan myös dynaamiseksi pakettien suodattamiseksi (vain muodostetut yhteydet verkkoon sallitaan.)

1.4.7 Tietokannan sijoittaminen DMZ-vyöhykkeestä erotettuun sisäiseen verkkovyöhykkeeseen, jonka ansioista tärkeät tiedot saadaan suojattua paremmin.

1.4.8 Ota käyttöön IP-osoitteiden peittäminen, jotta niitä ei paljasteta Internetissä. Siinä tulee käyttää protokollia kuten PAT tai NAT.

1.5 Asenna kaikkiin työntekijöiden tietokoneisiin oma palomuuriohjelmisto, joiden avulla päästään käyttämään yrityksen verkkoa.

Älä käytä ohjelmistotoimittajan määrittämiä oletussalasanoja tai muita tietoturva-asetuksia

1.6 Valmistajien määrittämät oletussalasanat tulee muuttaa ennen kuin asennetaan uusia komponentteja yrityksen verkkoon. Käyttäjätilit tulee pitää ajan tasalla poistamalla ylimääräiset tilit aika ajoin. Salasanan muuttaminen on tärkeää, koska oletussalasanat on saatavissa Internetistä, joka tekee tietomurrosta helppoa.

1.6.1 Kaikkien langattomien yhteyksien oletusasetukset, jotka ovat yhteydessä kortinhaltijoiden tietoihin tai lähettävät niitä tulee vaihtaa. Oletusasetuksia ovat WEP-avaimet, SSID-oletustunnukset, salasanat sekä SNMP-protokollan tunnistemerkkijonot.

1.7 Kaikki hallintayhteydet, joita ei muodosteta konsolin kautta tulee salata. Siihen voidaan käyttää esimerkiksi teknologioita SSH, VPN tai SSL/ TLS.

Siirrä kortinhaltijan tiedot avoimissa ja julkisissa tietoverkoissa salattuina

1.8 Kun siirretään kortinhaltijoiden tietoja julkisissa ja avoimissa tietoverkoissa, tulee käyttää vahvaa salausta kuten SSL-, TLS- tai IPSEC-protokollia.

1.8.1 Takaa langattoman verkon turvallisuus käyttämällä parhaita suojauksia sekä käyttäjäntunnistuksia.

1.9 Älä koskaan lähetä salaamattomana asiakkaan kortin tietoja.

Käytä virustorjuntaohjelmaa ja päivitä sitä säännöllisesti

1.10 Käytä virustorjuntaohjelmaa kaikissa viruksille alttiissa järjestelmissä sekä erityisesti käyttäjien koneissa

1.10.1 Tarkista, että virustorjuntaohjelmat pystyvät tunnistamaan, poistamaan sekä suojautumaan vihamielisiä ohjelmistoja vastaan. Esimerkkejä ovat vakoilu- ja mainosohjelmat.

1.10.2 Varmista, että kaikissa virustorjuntaohjelmissa on käytössä uusimmat versiot, ja että ne pystyvät luomaan tarkistuksista lokitiedostot.

Testaa tietoturvajärjestelmät ja prosessit säännöllisesti

1.11 Tee sisäinen ja ulkoinen verkon haavoittuvuustarkistus vähintään kolmen kuukauden välien sekä myös silloin, kun yrityksen verkkoa muutetaan tai siihen lisätään jotain.

1.12 Ota käyttöön järjestelmä, joka tarkkailee verkkoliikennettä, jossa on kortinhaltijoiden tietoja. Sen tarkoituksena on huomata, kun verkkoon murtaudutaan ja estää se. Pidä kyseinen järjestelmä aina ajan tasalla.

Tietoturvakäytännöt

1.13 Jos kortinhaltijoiden tiedot ovat palvelun tarjoajien käytössä, pidä yllä käytäntöjä ja toimintatapoja, kuinka heidän tulee tietoa käsitellä.

1.14 Pidä yllä listaa palveluntarjoajista.

1.15 Tee sopimus, jossa palveluntarjoajat hyväksyvät, että ovat osaltaan myös vastuussa tietoturvasta.

1.16 Varmista, että palvelun tarjoajat sitoutuvat toimimaan asiaan kuuluvalla tavalla.

1.17 Pidä yllä ohjelmaa, joka tarkkailee, että palvelun tarjoajat noudattavat PCI- tietoturvastandardia.

2 TASO

Kolmannella tasolla keskitytään parantamaan verkon turvallisuutta karsimalla siitä kaikki käyttämättömät toiminnot sekä määrittämällä niiden asetukset standardin vaatimalla tavalla. Toinen tärkeä asia on pitää järjestelmä ajan tasalla. Siinä voidaan käyttää apuna ohjelmistotarjoajan uutislehtisiä, jotka ilmoittavat uusista päivityksistä sekä tietoturvauhkista. Kolmas asia on kehittää turvallisia ja toimivia käytäntöjä, jotka tulee tuoda esille kaikille yrityksen työntekijöille.

Älä käytä ohjelmistotoimittajan määrittämiä oletussalasanoja tai muita tietoturva- asetuksia

2.1 Luo kaikille järjestelmäkomponenteille määritysstandardit ja varmista, että ne kattavat kaikki tiedossa olevat tietoturvariskit ja noudattavat alan parhaita käytäntöjä.

2.1.1 Käytä yhtä palvelinta vain yhteen tarkoitukseen, koska silloin palvelimen kaatuessa kaikki toiminnot eivät kaadu. Esimerkiksi WWW-palvelimien sekä tietokantapalvelimien tulisi olla omia palvelimiaan.

2.1.2 Poista kaikki tarpeettomat sekä suojaamattomat palvelut ja protokollat pois käytöstä, jolloin niitä ei voida käyttää hyväkseen tunkeutumisessa yrityksen verkkoon.

2.1.3 Määritä järjestelmän tietoturva-asetukset siten, että järjestelmää ei pystytä käyttämään väärin.

2.1.4 Poista käytöstä kaikki tarpeettomat toiminnot kuten komentosarjat, laiteohjaimet, alijärjestelemät, tiedostojärjestelmät sekä tarpeettomat web-palvelimet, jonka ansiosta ne eivät rasita järjestelmää turhan takia.

2.2 Hosting-palveluiden tarjoajien on suojattava kunkin organisaation hosting-ympäristö ja tiedot. Kyseisten palveluntarjoajien on täytettävä PCI-standardin vaatimukset hosting-palveluntarjoajille.

Kehitä turvallisia järjestelmiä ja sovelluksia sekä ylläpidä niitä

2.3 Varmista, että kaikissa järjestelmäkomponenteissa ja ohjelmistoissa on käytössä viimeisimmät toimittajalta saatavat tietoturvapäivitykset. Tärkeimmät päivitykset tulee asentaa kuukauden kuluessa niiden ilmestymisestä.

2.4 Luo prosessi, jonka avulla uudet tietoturvariskit voidaan löytää. Nämä tietoturvauutiset voidaan esimerkiksi tilata ilmaiseksi ohjelmistotuottajalta. Näin omat tietoturvakäytännöt voidaan päivittää siten, että ne kattavat uudet riskit.

2.5 Kehitä ohjelmisto, joka on tasapainossa PCI-standardin kanssa. Noudata ohjelmistokehityksessä alan parhaita käytäntöjä ja huomio tietoturva kaikissa ohjelmistojen elinkaaren vaiheissa.

2.5.1 Testaa kaikki tietoturvapäivitykset, järjestelmä- ja ohjelmistoasetukset ennen kuin otat uusia käyttöön kuten:

2.5.1.1 Kaikkien sisääntulojen varmennus

2.5.1.2 Kunnollinen ongelmien ratkaisun varmennus

2.5.1.3 Salaustekniikan varmennus

2.5.1.4 Turvallisen yhteydenottojen varmennus

2.5.1.5 RBAC:n (Role-Based Access Control) varmennus, joka estää pääsyn tietokantaan ilma erillistä lupaa järjestelmänvalvojalta.

2.5.2 Ohjelmistokehityksen sekä testausympäristön erottaminen varsinaisesta tuotantoympäristöstä.

2.5.3 Ohjelmistokehityksen sekä testausympäristön vastuiden erottaminen varsinaisista tuotantoympäristön vastuista.

2.5.4 Tuotantotietoja kuten maksukorttien numeroita ei saa käyttää testaus- tai kehitystyössä.

2.5.5 Testitiedot ja tilit tulee poistaa ennen tuotantoympäristöön siirtymistä.

2.5.6 Mukautetut sovellustilit, käyttäjätunnukset sekä salasanat tulee poistaa ennen sovelluksen käyttöön ottamista tai julkaisua asiakkaille.

2.5.7 Yrityksen tarpeisiin mukautetun ohjelmakoodin katselmointi ennen sen siirtämistä tuotantoon tai asiakkaille, jotta mahdolliset tietoturvariskit koodissa saadaan määriteltyä.

2.6 Kaikki WEB-sovellukset tulee kehittää suojattujen ohjelmointikäytäntöjen mukaisesti, josta esimerkkinä voidaan käyttää Open Web Applicationia Security Projectia. Tarkista yrityksille mukautettujen sovellusten koodi siinä olevien haavoittuvuuksien löytämiskesi. Käsittele dokumentaatiossa suojautuminen yleisiltä ohjelmointiin liittyviltä tietoturvariskeiltä:

2.6.1 Tarkistamattomat syötteet

2.6.2 Käyttöoikeuksien hallinnan virheet, jotta käyttäjätunnuksia ei päästäisi käyttämään vahingollisesti

2.6.3 Vahingollinen tiedoston käsittely

2.6.4 XSS –hyökkäykset

2.6.5 Tietovuoto tai vajavainen virheen käsittely

2.6.6 Käyttöoikeuksien tarkistuksen tai istunnonhallinnan virheet

2.6.7 Suojaamaton tallennus

2.6.8 Suojaamaton tiedonvälitys

2.6.9 Epäonnistuminen URL (Uniform Resource Locator) käytön rajoittamisessa. URL kertoo täsmälleen, mistä osoitteesta tieto löytyy.

2.7 Varmista, että kaikki Internetiin yhteydessä olevat sovellukset on suojattu tunnettuja uhkia vastaan käyttäen näitä keinoja:

2.7.1 Kaikki kirjoitettu sovelluskoodi tarkistetaan organisaatiolla, joka on erikoistunut sovellusten tietoturvaan.

2.7.2 Internetin yhteydessä olevien sovellusten turvaksi asennetaan sovelluskerrospalomuuri.

3 TASO

Neljännessä tasossa huomiota tulee kiinnittää käyttäjien valvontaan. Tärkeää on antaa kaikille työntekijöille henkilökohtaiset tunnukset, jotta heidän toimintaansa voidaan seurata yrityksen verkossa. Heitä tulee myös opettaa luomaan vahvat salasanat, jotta tietoturvataso saadaan mahdollisimman korkeaksi. Työntekijöillä ei tarvitse olla pääsyä kaikkeen yrityksessä olevaan tietoon, vaan heidän pääsynsä yrityksen verkossa voidaan rajoittaa ainoastaan tietoihin, joita he tarvitsevat työnteossaan.

Kaikesta verkkoliikenteestä tulee pitää yllä lokia, jotta voidaan tarkastaa, kuka on mitäkin tietoa käyttänyt. Tietomurtojen ilmaantuessa lokitiedoista nähdään, mihin jäljet johtavat, jotta oikeat ihmiset saadaan vastuuseen niiden syntymisestä.

Rajoita pääsy tietoihin koskemaan vain niitä, jotka tarvitsevat niitä liiketoiminnallisiin tarkoituksiin

3.1 Rajoita pääsy tietokantaan vain niille, jotka tarvitsevat sitä jokapäiväisessä työnteossa.

3.1.1 Pääsy tietoihin tulee rajoittaa vain etuoikeutetuille työntekijöille, jotka tunnistautuvat omalla salasanalla päästäkseen tietoihin käsiksi.

3.1.2 Käyttöoikeuksien jakaminen tulee määritellä jokaisen työntekijän henkilökohtaisen työtehtävän mukaan.

3.1.3 Johto pystyy antamaan hyväksynnän tiettyjen tietojen antamiseen, jos työntekijän oikeudet eivät niihin riitä.

3.1.4 Automaattinen käyttäjän valvontasysteemi tulee ottaa käyttöön.

3.2 Luo käytön hallintajärjestelmä jossa on käyttäjiä, jolla on pääsy tietoihin joita heidän tulee työtehtävässään tietää. Käytön hallintajärjestelmä tulee sisältää seuraavat asiat:

3.2.1 Selostus järjestelmäkomponenteista.

3.2.2 Selvitys jaetuista oikeuksista työntekijöille riippuen työn laadusta ja tehtävästä.

3.2.3 Järjestelmän oletuksena on kieltää kaikki sisäänpääsyt, jos kirjautuminen järjestelmään epäonnistuu.

Luo jokaiselle tietojärjestelmän käyttäjälle yksilöllinen käyttäjätunnus

3.3 Kaikilla käyttäjillä tulee olla yksilöllinen käyttäjätunnus ennen kuin he voivat mennä tietojärjestelmiin. Tietojärjestelmä tekee myös lokia käyttäjistä, jolloin tiedon väärinkäyttötilanteissa syylliset ovat helposti löydettävissä.

3.4 Käytä käyttäjien käyttöoikeuksien tarkistamiseen ainakin yhtä seuraavista menetelmistä:

- Salasana
- Tunnistevälineet kuten SecureID- kortti, sertifikaatit tai julkiset avaimet
- Biotermiset tunnisteet

3.5 Ota käyttöön kaksivaiheinen käyttöoikeuksien tarkistamismenetelmä työntekijöiden, järjestelmävalvojien sekä kolmansien osapuolten edustajien muodostaessa etäyhteyksiä järjestelmään. Siinä voidaan käyttää apuna RADIUS- palvelua, TACACS- protokollaa tunnisteiden kanssa tai VPN- protokollaa ja yksilöllisiä sertifikaatteja.

3.6 Salaa kaikki salasanat niitä siirrettäessä ja tallennettaessa järjestelmän eri osissa.

3.7 Varmista, että käyttöoikeuksien tarkistaminen ja salasanojen hallinta on hoidettu huolellisesti sellaisten käyttäjien osalta, jotka eivät ole kuluttajia tai jotka ovat järjestelmänvalvojia, kaikissa järjestelmäkomponenteissa:

3.7.1 Valvo käyttäjätunnusten, käyttöoikeusmääritysten ja käyttäjän muiden tunnistetietojen lisäämistä, poistamista ja muuttamista.

3.7.2 Varmista käyttäjän henkilöllisyys ennen salasanojen muuttamista.

3.7.3 Aseta käyttäjille yksilöllinen salasana ensimmäisellä kerralla, kun he kirjatuvat järjestelmään. Sen jälkeen salasana tulee välittömästi vaihtaa uuteen, jotta kukaan ei pääse käsiksi vanhaan salasanaan.

3.7.4 Käyttäjätilejä tulee päivittää usein ja poistaa välittömästi tilit käyttäjiltä, joilla ei ole enää lupaa päästä tietoihin.

3.7.5 Käyttämättömät tilit tulee poistaa viimeistään 90 päivän jälkeen, mutta mieluiten jopa aikaisemmin.

3.7.6 Tee järjestelmän etäkäyttäminen mahdolliseksi myös toimittajille, mutta ainoastaan siksi ajaksi, kun sille on tarvetta.

3.7.7 Tee selväksi kaikille käyttäjille, kuinka vahva salasana muodostetaan ja kuinka niitä tulee säilyttää.

3.7.8 Älä käytä yhteisiä tai tietyille ryhmille tarkoitettuja salasanoja, vaan jokaisella käyttäjällä tulee olla omansa.

3.7.9 Vaadi salasanan vaihtoa viimeistään 90 päivän käyttämisen jälkeen.

3.7.10 Salasanan pituus tulee olla vähintään seitsemän merkkiä.

3.7.11 Salasannassa tulee olla niin kirjaimia kuin numeroitakin, jotta se olisi tarpeeksi vahva.

3.7.12 Älä salli käyttäjän asettaa salasanaa, joka on ollut aikaisemmin käytössä.

3.7.13 Rajoita peräkkäisten sisäänkirjautumisten määrä lukitsemalla käyttäjätunnus, jos salasana kirjoitetaan väärin yli kuusi kertaa.

3.7.14 Määritä lukitus kestämään vähintään 30 minuuttia tai kunnes järjestelmänvalvoja avaa tilin uudestaan.

3.7.15 Jos istunto ei ole ollut aktiivinen 15 minuuttiin, vaadi uutta kirjautumista siihen. Tämän avulla voidaan estää inhimillisten tietoriskien syntyä, koska käyttäjä saattaa unohtaa kirjautua pois palvelusta.

3.7.16 Tarkista kaikkien käyttäjien käyttöoikeudet, jotka ovat voivat päästä käsiksi tietokantoihin, jossa on tallennettuna kortinhaltijan tietoja. Tähän sisältyvät kaikki tietokantaa käyttävät sovellukset, järjestelmänvalvojat sekä muut käyttäjät.

Seuraa ja valvo kaikkea verkkoresurssien ja kortinhaltijoiden tietojen käyttöä

3.8 Luo prosessi järjestelmän kaikkien osien käyttöoikeuden yhdistämiseen yksittäisiin käyttäjiin, jolla on järjestelmänvalvojan käyttöoikeudet.

3.9 Ota käyttöön jäljitys, jonka avulla seuraavat tapahtumat voidaan toistaa kaikkien järjestelmäkomponenttien osalta:

3.9.1 Kaikkien yksittäisten käyttäjien pääsyt kortinhaltijoiden tietoihin.

3.9.2 Kaikki toimenpiteet, jotka on tehty järjestelmänvalvojan käyttöoikeuksilla.

3.9.3 Kaikki jäljitystietojen käyttö

3.9.4 Epäonnistuneet loogiset käyttöyritykset

3.9.5 Tunniste- ja käyttöoikeuksien tarkistamismekanismien käyttö

3.9.6 Jäljityslokitiedostojen uudelleen käyttöönotto

3.9.7 Järjestelmätason objektin luominen ja poistaminen

3.9.8 Tallenna kunkin tapahtuman osalta vähintään seuraavat tiedot jäljityslokitiedostoon järjestelmän kaikissa osissa:

- Käyttäjätunnus
- Tapahtuman tyyppi
- Päivä ja aika
- Tieto siitä onnistuuko vai epäonnistuuko tapahtuma
- Tapahtuman syy
- Tunnista tai nimeä tieto- tai järjestelmäkomponentti, johon tapahtuma vaikutti.

3.9.9 Synkronoi kaikki tärkeät järjestelmän kellot ja ajat

3.9.10 Tarkista kaikkien järjestelmän osien lokitiedostot vähintään kerran päivässä. Lokitiedostojen tarkistuksen tulisi sisältää lokitiedostot tietoturvaan liittyviin tehtäviin, kuten tunkeutumisen havaitsemiseen (Intrusion Detection System, IDS) käytettäviin palvelimiin, käyttöoikeuksien todentamiseen, käyttäjien valtuuttamiseen ja käyttäjien toimien kirjaamiseen (Authentication, Authorization and Accounting, AAA) käytettäviin palvelimiin.

3.9.11 Säilytä jäljitystiedostot vähintään yhden vuoden ajan ja vähintään kolme kuukautta sähköisessä muodossa Internetissä.

Testaa tietoturvajärjestelmät ja –prosessit säännöllisesti

3.10 Käytä tiedostojen eheyden tarkastusjärjestelmää, jotta yrityksen henkilökunta on perillä kaikista luvattomista muutoksista kriittisissä järjestelmätiedostoissa tai kriittisiä tietoja sisältävissä tiedostoissa. Suorita kriittisten tiedostojen vertailu vähintään kerran viikossa.

4 TASO

Viidennessä tasossa painotetaan kortinhaltijoiden tietojen suojaamista sekä fyysisen pääsyn rajausta kortinhaltijoiden tietoihin. Tietojen suojaamis-menetelmistä nostettiin esiin kortin maskaus, jossa tarkoitus on peittää osa kortin numeroista, jotta korttia ei voida käyttää ilman kaikkia numeroita. Fyysisen pääsyn rajauksessa taas painotettiin oikeanlaista valvontaa sekä toimitilojen suunnittelua. Suunnittelussa tulee varmistaa, että vierailijat eivät pääse lähelle fyysisesti dokumentoituja tietoja, jotta tietomurtoja ei pääse tapatumaan. Tätä voidaan valvoa videokameroilla sekä kulunvalvontapisteillä.

Suojaa tallennetut kortinhaltijan tiedot

4.1 Peitä korttien numerot. Jos ne sattuvat pääsemään vääriin käsiin, niin niitä ei kuitenkaan pysty käyttämään vääriin tarkoituksiin. Kortin numeroista näkyvissä saa olla enintään kuusi ensimmäistä tai neljä viimeistä numeroa.

4.2 Salaa kortinnumero siten, että sitä ei pysty lukemaan mistään niiden tallennuspaikoista kuten siirrettävistä tallennusvälineistä, varmuuskopioista, lokitiedostoista tai langattoman verkon kautta vastaanotetuista tiedoista jollain seuraavista tavoista:

- Yksisuuntainen hajautustaulukko (Hashing)
- Merkkijonojen katkaiseminen
- Indeksitunnukset ja PAD- tietojen suojattu tallentaminen
- Vahva salaus ja siihen liittyvät avaintenhallintamenetelmät

4.2.1 Jos käytetään levysalausta tiedosto- tai saraketason tietokantasalauksen sijaan, looginen pääsynhallinta on erotettava käyttöjärjestelmän omista pääsynhallintamekanismeista olemalla käyttämättä paikallisen järjestelmän tilejä. Salauksenpurkuavaimia ei saa myöskään yhdistää käyttäjätileihin.

4.3 Suojaa salausavaimet niin väärinkäytöltä kuin paljastumiseltakin

4.3.1 Rajaa avainten haltijajoukko mahdollisimman pieneksi.

4.3.2 Pidä avaimet yhdessä paikassa ja käytä mahdollisimman pientä määrää tallennusmuotoja.

4.4 Dokumentoi ja ota käyttöön avaintenhallintaan liittyvät prosessit ja käytännöt. Mukaan lukien:

4.4.1 Vahvojen avainten tuottaminen

4.4.2 Avainten suojattu jakelu

4.4.3 Avainten suojattu tallentaminen/ varastoiminen

4.4.4 Ajoittainen avainten vaihtaminen:

- Tarvittaessa tai jos ohjelmisto katsoo sen aiheelliseksi
- Vähintään vuosittain

4.4.5 Vanhojen avainten hävittäminen

4.4.6 Avainten ei tule olla yhden ihmisen hallussa, vaan avain tulee jakaa vähintään kahteen tai kolmeen osaan, joista kukin henkilö tietää vain oman osuutensa.

4.4.7 Avainten luvattoman korvaamisen estäminen.

4.4.8 Vaatimus siitä, että avainten haltijat kirjoittavat sopimuksen, jossa he toteavat hyväksyvänsä ja ymmärtävänsä vastuun, jotka heille on asetettu.

Rajoita fyysinen pääsy kortinhaltijan tietoihin

4.5 Käytä asianmukaista laitteistoa rajoittamaan ja tarkkailemaan kulkua kortinhaltijoiden tietojen ympäristöön.

4.5.1 Käytä videokameroita tai muita laitteita valvomaan ja tarkkailemaan kulkua tärkeisiin paikkoihin. Tarkastele kerättyjä tietoja ja vertaa niitä muihin tietoihin, joita laitteet ovat keränneet eri sisäänkäynneillä. Säilö kyseisiä tietoja vähintään kolme kuukautta, jos laki ei määrää pidempää säilytystä.

4.5.2 Rajoita fyysinen pääsy julkisesti käytettävissä oleviin verkkopistokkeisiin.

4.5.3 Rajoita pääsy langattomien verkkojen tukiasemiin, yhdyskäytäviin ja kannettaviin laitteisiin.

4.6 Kehitä käytäntö, jolla voidaan helposti erottaa yrityksessä työskentelevät henkilöt vierailijoista, jos heillä on pääsy tiloihin missä on tallennettu kortinhaltijoiden tietoja.

4.7 Varmista, että kaikkien vierailijoiden kohdalla täyttyvät seuraavat asiat:

4.7.1 Vierailijoiden oikeudet tulee tarkistaa aina ennen kuin heidät päästetään tiloihin, joissa on tallennettuna kortinhaltijoiden tietoja.

4.7.2 Vierailijoille annetaan jokin tunnus kuten vierailijakortti tai pääsyn mahdollistava laite, joka kertoo, että he eivät työskentele kyseisessä yrityksessä, ja heillä on tietty aika jolloin voivat vierailla siellä.

4.7.3 Heidän tulee myös antaa tunnistevälineet pois, kun vierailu päättyy, ettei niitä voida käyttää hyväksi myöhemmin.

4.8 Vierailijoista pidetään kirjaa, jotta voidaan luoda jäljitysketju. Tämä loki tulee säilöä vähintään kolme kuukautta, jos lainsäädännössä ei ole muuta määrätty.

4.9 Säilö sähköisessä muodossa olevia varmuuskopioita suojatuissa tiloissa. Parhaassa tapauksessa ne ovat yrityksen tilojen ulkopuolella, jollain kaupallisen varastopalveluja tarjoavan yrityksen tiloissa.

4.10 Suojaa myös kaikki fyysisessä muodossa olevat tiedot kuten asiakirjat ja elektroninen media kuten DVD- ja kovalevyt, joissa on kortinhaltijoiden tietoja.

4.11 Valvo tarkasti kortinhaltijoiden tietoja sisältäviä tallennusvälineitä sekä niiden säilytystä ja käyttöä.

4.11.1 Merkitse tallennusvälineisiin, että ne sisältävät luottamuksellista tietoa.

4.11.2 Lähetä tallennusväline sen vastaanottajalle joko luotettavalla kuriirilla tai sellaista siirtotapaa käyttäen, jota on helppo seurata.

4.12 Varmista, että yrityksen johto hyväksyy kaikkien sellaisten tallennusvälineiden käytön, jotka siirretään pois suojatulta alueelta ja erityisesti, jos tallennusvälineitä jaetaan yksittäisille ihmisille.

4.13 Valvo huolellisesti kaikkien kortinhaltijoiden tietoja sisältävien tallennusvälineiden säilytystä ja niiden käyttöä.

4.13.1 Pidä yllä varaston lokia kaikesta tiedosta ja tallenna uusi tieto varastoon vähintään kerran vuodessa.

5 TASO

Kuudennessa tasossa keskitytään palomuurin määritysstandardeihin sekä pyritään kehittämään turvallisia järjestelmiä ja sovelluksia, jotka tuodaan työntekijöiden arkirutiineihin. Heille tulee lisäksi luoda dokumentoidut tietoturvakäytännöt, joita noudattamalla tietomurtoja ei pääse tapahtumaan inhimillisen toiminnan seurauksena. Tietoturvakäytäntö tulee koskea myös alihankkijoita ja heidän tulee sitoutua siihen yhtä tarkasti kuin yrityksen omien työntekijöiden, koska muuten tietoturvataso laskee. Yritykset voivat solmia kirjallisen sopimuksen, joka velvoittaa heitä toimimaan sovittujen käytäntöjen mukaan. Tämän avulla he voivat varmistua alihankkijoidensa toiminnasta.

Suojaa kortinhaltijatiedot asentamalla palomuuriohjelma ja ylläpitämällä sitä

5.1 Luo palomuurin määritysstandardi, joka on tarkoin määritelty prosessi kaikkien ulkoisten verkkoyhteyksien ja palomuurin tehtävien muutosten hyväksymiseen ja testaamiseen.

5.2 Palomuuriin tulee luoda ryhmien, roolien ja vastuiden kuvaus verkon osien loogisen hallinnan mahdollistamiseksi.

5.3 Palomuurin määritysstandardi tulee tarkastaa ja päivittää vähintään puolen vuoden välein.

Kehitä turvallisia järjestelmiä ja sovelluksia sekä ylläpidä niitä

5.4 Muutoksenhallintakäytäntöjen seuraaminen järjestelmiin ja ohjelmistoihin tehtävissä muutoksissa. Näihin käytäntöihin tulee sisältyä seuraavat pykälät:

5.4.1 Muutosten vaikutusten dokumentointi

5.4.2 Yrityksen johdon allekirjoitus soveltuvin osin

5.4.3 Toiminnan testaaminen

5.4.4 Muutosten kumoamiskäytännöt

Seuraa ja valvo kaikkea verkkoresurssien ja kortinhaltijoiden tietojen käyttöä

5.5 Suojaa jäljitystiedot siten, että niitä ei voi muuttaa sekä myös seuraavien asioiden varmistaminen:

5.5.1 Jäljitystietoja voivat tarkastella vain ne henkilöt, jotka tarvitsevat niitä tietoja työssään.

5.5.2 Suojaa jäljitystiedot luvattomalta muokkaukselta

5.5.3 Tee jäljitystiedostoista varmuuskopiot säännöllisesti keskitettyyn lokitiedostopalvelimeen tai sellaiseen muotoon, jossa lokitiedostoja on vaikea muuttaa.

5.5.4 Kopio langattomia verkkoja koskevat lokitiedostot lokipalvelimeen, joka on yrityksen verkon sisällä.

5.5.5 Käytä tiedostojen eheyden ja muutosten valvontaan tarkoitettua ohjelmistoa varmistaaksesi, jotta aiemmin luotuja lokitiedostoja ei pysty muuttamaan ilman erillistä varoitusta.

Testaa tietoturvajärjestelmät ja –prosessit säännöllisesti

5.6 Testaa, että langattomien verkkojen yhteydet toimivat käyttäen langatonta analysaattoria ja etsimällä kaikkia mahdollisia laitteita verkosta vähintään neljä kertaa vuodessa.

5.7 Testaa verkkoinfrastruktuurin ja käytössä olevien sovellusten alttius murtautumiselle ainakin kerran vuodessa, mutta jos verkossa tapahtuu muutoksia tai siihen lisätään laitteita, niin useammin. Kyseisiin testeihin tulee kuulua seuraavat asiat:

5.7.1 Verkkokerroksen murtautumistesti

5.7.2 Sovelluskerroksen murtautumistesti

Luo työntekijöitä ja alihankkijoita koskeva tietoturvakäytäntö

5.8 Luo ja ylläpidä tietoturvakäytäntö, joka tulee julkaista kaikkien yrityksen työntekijöiden kesken ja vakuuttua, että he ymmärtävät sen. Sen tulee sisältää seuraavat asiat:

5.8.1 Kaikki noudattavat PCI-standardin vaatimuksia

5.8.2 Sisältää vuosittaisen prosessin, jossa määritetään yrityksen uhat, haavoittuvuudet ja huolellisen riskianalyysin tulokset.

5.8.3 Vuosittain tehtävä tarkistus tietoturvakäytännön osalta ja sen muutoksista toimintaympäristön muuttuessa.

5.9 Laadi päivittäinen tietoturvakäytäntö. Sen tarkoituksena on luoda käytännöt käyttäjätilien ylläpitoon ja lokitiedostojen tarkistamiseen.

5.10 Laadi käytännöt työntekijöiden käyttämille kriittisille laitteille, kuten modeemeille ja langattomille päätelaitteille. Käytännöissä on tultava selville oikeaoppiset tavat käyttää kyseisiä laitteita, ja ne tulee esitellä niin työntekijöille kuin alihankkijoillekin. Käytännön toimenpiteiden tulee sisältää seuraavat asiat:

5.10.1 Yrityksen johdon nimenomainen hyväksyntä.

5.10.2 Teknologian käytön todentaminen.

5.10.3 Luettelo kaikista laitteisto ja henkilöistä, joilla on niihin käyttöoikeus.

5.10.4 Laitteiden omistajan, käyttötarkoituksen sekä merkintä laitteeseen.

5.10.5 Laitteiden käyttötarkoitukset.

5.10.6 Laitteiden sallitut sijainnit yrityksen verkossa.

5.10.7 Luettelo yrityksen hyväksymistä tuotteista.

5.10.8 Automaattinen yhteyden sammuttaminen, kun istunnot ovat olleet poissa käytöstä tietyn ajan.

5.10.9 Yhteyden muodostaminen verkon kautta alihankkijoihin vain silloin, kun he niitä tarvitsevat ja välitön sulkeminen, kun istunto päättyy.

5.10.10 Kun käsitellään kortinhaltijoiden tietoja etäyhteyden kautta kopioiminen ja liittäminen kovalevylle on kiellettyä ja tulostusmahdollisuudet tulee myös poistaa.

5.11 Varmista, että tietoturvakäytäntö selittää yskäselitteisesti työntekijöiden ja alihankkijoiden vastuut tietoturvasta.

5.12 Nimeä yksittäinen työntekijä tai ryhmä, jonka tulee varmistaa seuraavat tietoturvavastuut:

5.12.1 Tietoturvakäytäntöjen ja –prosessien luominen, dokumentointi sekä jakelu.

5.12.2 Tietoturvavaroitusten ja -tiedotteiden seuraaminen ja analysointi sekä tietojen välittäminen eteenpäin oikeille henkilöille.

5.12.3 Tietoturvarikkomuksiin reagoimista ja niistä raportoimista koskevien käytäntöjen luominen, dokumentoiminen ja jakelu, jotta kaikkiin tilanteisiin pystytään vastaamaan nopeasti ja tehokkaasti.

5.12.4 Käyttäjätilien hallinnointi, mukaan lukien niiden lisäykset, poistot ja muutokset.

5.12.5 Tarkkaile ja valvo pääsyä tietokantaan

5.13 Varmista, että kaikki työntekijät ovat tietoisia kortinhaltijoiden tietojen tietoturvan tärkeydestä ottamalla käyttöön tietoturvatietousohjelma.

5.13.1 Kouluta uusia työntekijöitä ennen töiden aloittamista ja vanhoja vähintään vuosittain.

5.13.2 Vaadi työntekijöiltä kirjallinen vakuutus siitä, että he ovat tutustuneet yrityksen tietoturvakäytäntöihin ja -prosesseihin sekä ymmärtäneet ne.

5.14 Minimoi sisäisten hyökkäysten riskit tarkistamalla mahdollisten uusien työntekijöiden tausta.

5.15 Laadi rikkomuksiin reagoimista koskeva suunnitelma. Järjestelmiin kohdistuvien rikkomusten tapahtuessa yrityksen on oltava valmis reagoimaan välittömästi. Sen tulee sisältää seuraavat asiat:

5.15.1 Eri osapuolten roolit ja vastuut sekä kommunikointi ja yhteydenotto-käytännöt.

5.15.2 Tarkat reagointikäytännöt erilaisten rikkomusten kohdilta.

5.15.3 Liiketoiminnan toipumista ja jatkamista koskevat käytännöt.

5.15.4 Tiedon varmuuskopiointikäytännöt

5.15.5 Lainmukaiset analyysit kompromissien tiedottamisesta.

5.15.6 Kriittisten komponenttien vakuutus/ korvaus.

5.16 Testaa suunnitelma vähintään vuosittain.

5.17 Määritä nimetyt henkilöt, jotka ovat valmiina vastaamaan hälytyksiin ympäri vuorokauden.

5.18 Tarjoa koulutusta niille henkilöille, jotka vastaavat tietoturvarikkomuksiin reagoinnista.

5.19 Sisällytä suunnitelmaan järjestelmiin tunkeutumisen havaitsemiseen, tunkeutumisen estämiseen ja tiedostojen eheyden tarkistamiseen tarkoitetuista järjestelmistä tulevat varoitukset.

5.20 Sisällytä suunnitelmaan prosessi, jonka avulla suunnitelmaa voidaan muokata ja kehittää kokemuksen myötä ja alan kehityksen mukaan. (PCI Council Priorized approach for DSS 1.2, [viitattu 16.10.2009].)

Palveluntarjoajien PCI-standardi vaatimukset

1. Turvaa seuraavat kohdat:

1.1 Varmista, että jokaisella osapuolella on yhteys vain omaan kortinhaltijatietoympäristöön.

1.2 Rajoita kunkin osapuolen pääsy vain ainoastaan sitä koskevaan kortinhaltijatieto ympäristöön.

1.3 Varmista, että jäljitysketjut ja lokikirjaus ovat voimassa, ja että ne ovat yksilöllisiä kunkin osapuolen kortinhaltijatietoympäristön kohdalla.

1.4 Luo prosessit, joiden avulla oikeudellinen tutkinta voidaan suorittaa ripeästi, jos hosting palveluita käyttävien osapuolten tietoturva murtuu. (PCI Council, Priorized approach for DSS 1.2, [viitattu 19.10.2009].)

Vaihtoehtoiset suojausmenetelmät

Vaihtoehtoisia suojaustapoja voidaan käyttää, jos yritys ei pysty täyttämään teknisiä suojausmekanismeja, joita PCI-standardi vaatii. Tätä vaihtoehtoa voidaan kuitenkin soveltaa vain, jos organisaatio on vähentänyt asiaan liittyviä riskejä huomattavasti, mutta ei silti pysty täyttämään teknisiä ehtoja. Vaihtoehtoisten suojausmenetelmien tehokkuus riippuu monista tekijöistä: ympäristöstä (missä sitä käytetään), muista turvajärjestelmistä sekä turva-asetuksista. Yritysten tulee ymmärtää, että vaihtoehtoisia suojausmenetelmiä ei voida käyttää kaikissa toimintaympäristöissä, ja ne tulee arvioida perusteellisesti käyttöönoton jälkeen, jotta voidaan varmistua niiden tehokkuudesta. (PCI Council, PCI-standardi 1.1, [viitattu 20.10.2009].)

Seuraavassa ohjeessa tutustutaan vaihtoehtoisiin suojausmenetelmiin tapauksissa, joissa yritykset eivät pysty tekemään kortinhaltijatiedoista lukukelvottomia PCI-standardi kohdan 5.2 mukaisesti.

Vaihtoehtoiset suojausmenetelmät standardin 5.2 vaatimukselle

Vain yritykset, jotka ovat tehneet perusteellisen riskianalyysin sekä, joilla on aitoja teknisiä tai dokumentoituja liiketoiminnallisia rajoitteita, voivat käyttää vaihtoehtoisia suojausmenetelmiä. Yritykset, jotka miettivät vaihtoehtoisten suojausmenetelmien käyttöä, tulee olla tietoisia mahdollisista tietoturvariskeistä, jotka syntyvät lukukelpoisten kortinhaltijatietojen säilyttämisestä. Mahdollisten suojamenetelmien on tarjottava lisäsuojaa, joka vähentää riskiä lukukelpoisten kortinhaltija tietojen pääsystä vääriin käsiin. Vaihtoehtoisena suojamenetelmänä voidaan käyttää laitetta tai niiden yhdistelmää, sovelluksia tai suojajärjestelmiä, joiden tulee täyttää seuraavat ehdot:

1. Tarjottava ylimääräistä segmentaatiota tai abstraktiota esimerkiksi verkkokerroksissa.

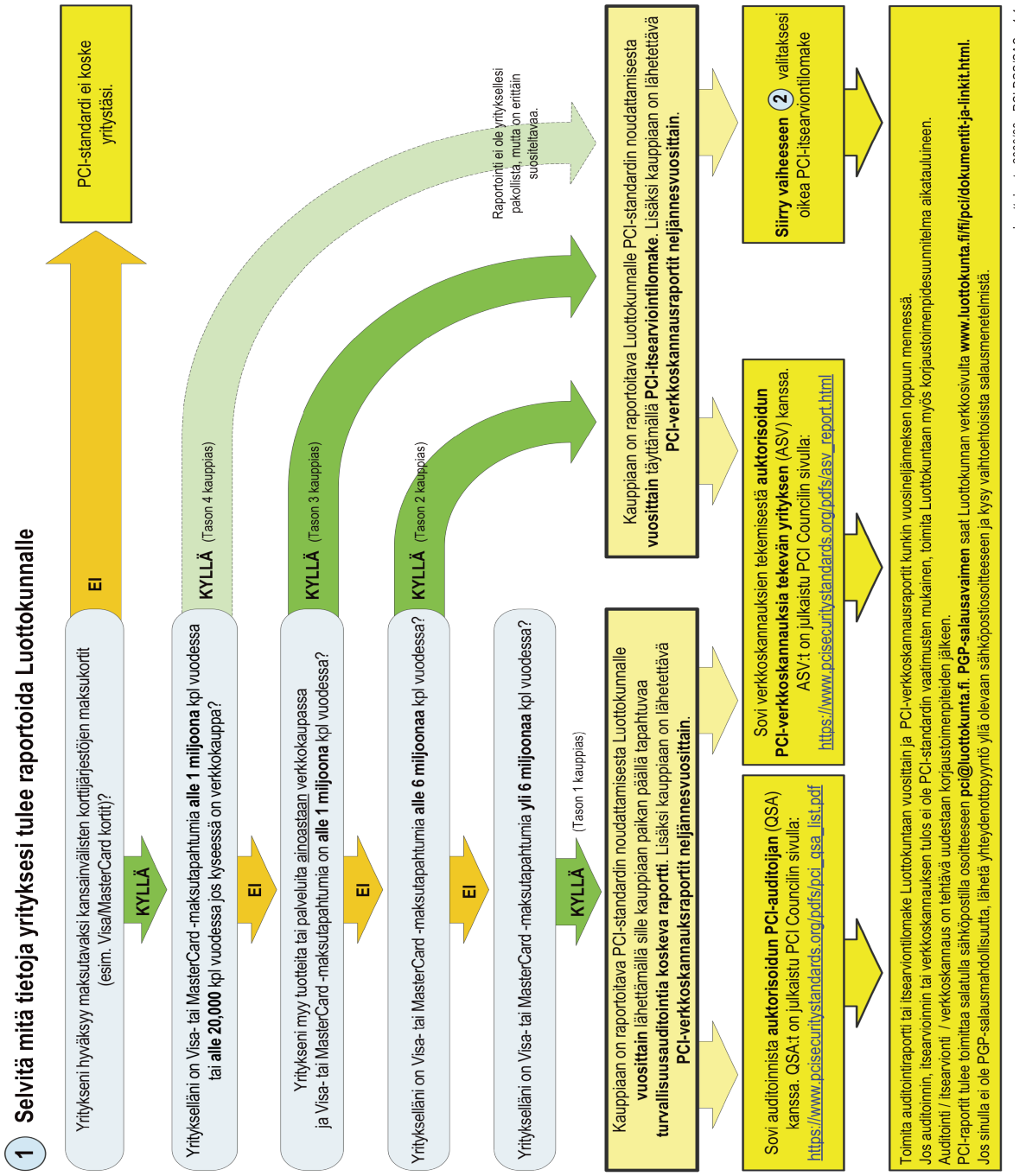
2. Tarjottava mahdollisuus rajoittaa pääsyä kortinhaltijoiden tietoihin tai tietokantoihin seuraavien kriteerien perusteella:
   - IP-osoite/ Mac-osoite
   - Sovellus/ Palvelu
   - Käyttäjätilit/ Ryhmät
   - Tietotyyppi

3. Rajoittaa loogista pääsyä tietokantaan

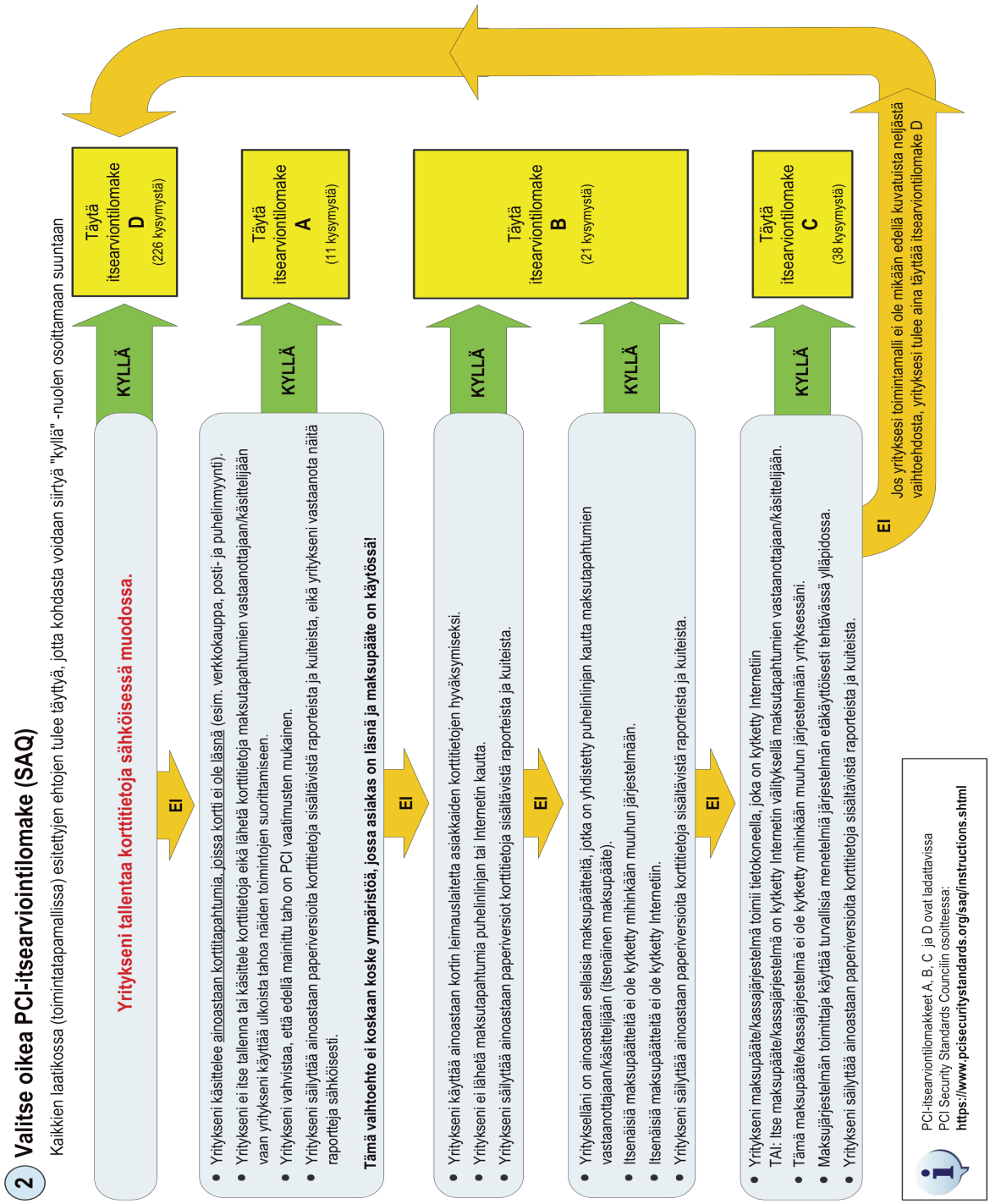
4. Estää ja havaita sovelluksiin ja tietokantoihin kohdistuvat hyökkäykset (PCI Council, PCI-standardi 1.1, [viitattu 20.10.2009].)

LIITE 2

Yritysten raportointi velvollisuudet



(Luottokunta. Kauppiaan raportointivelvollisuus PCI-tietoturvastandardin noudattamisesta [viitattu 20.8.2009].)



(Luottokunta. Kauppiaan raportointivelvollisuus PCI-tietoturvastandardin noudattamisesta [viitattu 20.8.2009].)