Opinnäytetyö (AMK)

Tietojenkäsittelyn koulutusohjelma

Yrityksen tietojärjestelmät

2015

Tomi Kiiski

VERKKOKAUPPA PCI DSS - STANDARDIN MUKAISEKSI

– Case Scandinavian Outdoor

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittelyn koulutusohjelma | Yrityksen tietojärjestelmät

2015 | Sivumäärä 33

Tuomo Helo

Tomi Kiiski

VERKKOKAUPPA PCI DSS -STANDARDIN MUKAISEKSI – CASE SCANDINAVIAN OUTDOOR

Tämän opinnäytetyön tavoitteena on selvittää, mitä toimia verkkokaupalta vaaditaan PCI DSS -standardin mukaisuuteen sekä mikä PCI DSS -standardi on ja mitä se sisältää. Työn toimeksiantaja on Scandinavian Outdoor Oy. Toimeksiantajan edellinen PCI DSS -auditointi on suoritettu standardin vanhalla versiolla ja standardista on nyt uusi versio.

Työn teoriaosa käsittelee yleisesti PCI DSS -standardia, sen sisältöä sekä vaatimuksia. Työn tärkeimpänä lähteenä on käytetty PCI SSC:n julkaisemaa PCI DSS -standardin 3.1-versiota. Empiirisessä osuudessa selvitetään teorianosan ohjaamana, miten toimeksiantajan verkkokaupat saadaan standardin mukaisiksi.

Lopputuloksena toimeksiantaja sai selkeän kuvauksen itse standardista ja sen sisällöstä sekä kuvauksen toimenpiteistä mitä standardin noudattaminen vaatii.

ASIASANAT:

PCI DSS, tietoturva, verkkokauppa, maksukortit

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Information Systems

2015 | Total number of pages 33

Tuomo Helo

Tomi Kiiski

PCI DSS COMPLIANCE FOR E-COMMERCE – CASE SCANDINAVIAN OUTDOOR

The aim of this thesis was to define how e-commerce can comply with Payment Card Industry Data Security Standard (PCI DSS) and research what PCI DSS is and its requirements for the client of this thesis, Scandinavian Outdoor. The client had complied with standard's older version but now needed to update to the latest version, namely PCI DSS version 3.1.

The theoretical framework of this thesis introduces PCI DSS in general and discusses what it requires from a company and its employers. The most important source is PCI DSS version 3.1. The empirical part explains how Scandinavian Outdoor's e-commerce can comply with PCI DSS.

As a result of this thesis, the client received a clear description of the standard and the actions needed in order to comply with PCI DSS.

KEYWORDS:

PCI DSS, information security, e-commerce, payment cards

SISÄLTÖ

KUVAT

TAULUKOT

1 JOHDANTO

PCI DSS on tietoturvastandardi, joka määrittelee maksukorttiliikenteelle vähimmäistietoturvatason. Standardi on pakollinen kaikille tahoille, jotka käsittelevät, tallentavat tai välittävät korttitietoja. Standardi kehittyy jatkuvasti ja työtä kirjoitettaessa uusin versio on 3.1. Digitalisoituvassa maailmassa uusia tietoturvauhkia löydetään päivittäin, ja niitä vastaan pitää pystyä puolustautumaan.

Työn toimeksiantaja Scandinavian Outdoor myy välineitä, varusteita ja vaatteita kaikenlaiseen retkeilyyn, urheiluun sekä ulkoiluun. Yrityksellä on useita kivijalkamyymälöitä sekä neljä verkkokauppaa. Suoritin työnharjoittelun Scandinavian Outdoorissa keväällä 2015. Harjoittelun aikana tuli puuttuva opinnäytetyö puheeksi ja sitä kautta tarjoutui tilaisuus kyseiseen aiheeseen. PCI DSS -standardi ei ole minulle entuudestaan tuttu käsite.

Tämän opinnäytetyön tavoitteena on selvittää miten Scandinavian Outdoorin verkkokaupat saadaan PCI DSS -standardin mukaisiksi. Työn teoriaosuuden tarkoitus on selvittää, mikä PCI DSS on sekä mitä se sisältää. PCI DSS -standardin ollessa kokonaisuudessaan hyvin laaja, on työ rajattu kohdistumaan erityisesti verkkokaupan näkökulmaan. Tietoturva on aina ajankohtainen aihe digitalisoituvassa maailmassa ja siksi mielenkiintoinen.

Opinnäytetyön lähestymistapa on tapaustutkimus, jossa vastausta tutkintakysymykseen etsitään yksittäisen tapauksen avulla (Aaltio 2014). Työssä käytetään konstruktiivista tutkimusotetta, joka selvittää tutkimuskysymyksiä ratkaisemalla reaalimaailman ongelmia. Konstruktiivinen tutkimus on yksi tapa suorittaa tapaustutkimus. Tutkimuksen pohjana on teoreettinen sisältö ja soveltavassa osuudessa lopputulosta verrataan teoriaan. (Lukka 2014.)

Luvussa 2 käsitellään yleisesti PCI-standardeja ja luvussa 3 tarkastellaan tarkemmin PCI DSS -standardia ja sen eri vaatimusluokkia. Luku 4 sisältää Scandinavian Outdoorin tämän hetkisen tilanteen ja kuvauksen. Luku 5 sisältää selvityksen miten toimeksiantajan verkkokaupat saadaan standardin mukaisiksi. Lopuksi on kokonaisuuden yhteenveto.

Tärkeimpänä lähteenä käytän PCI SSC:n internet-sivuja sekä itse PCI DSS -standardia. Muut lähteet ovat lähinnä internet-lähteitä käsiteltävästä aiheesta.

2 PCI-STANDARDIT

PCI SSC eli Payment Card Industry Security Standards Council on American Expressin, Discover Financial Servicesin, JCB Internationalin, MasterCardin ja Visan vuonna 2006 perustama maailmanlaajuinen riippumaton toimielin, joka vastaa luottokorttimaksujen tietoturvastandardien kehittämisestä, ylläpidosta sekä kouluttamisesta (PCI Security Standard Council 2015a).

PCI-lyhennettä käytetään yleisesti kuvaamaan korttimaksujen tietoturvaa. Useimmat PCI-standardit määrittelevät mitä tulee suojata, mutta eivät välttämättä puutu siihen, miten tai millä teknologialla se tulee tehdä. Tämä ei kuitenkaan tarkoita, että teknologiaa ei olisi. Sitä ei vain ole määritelty ja standardisoitu riittävästi. (Gomzin 2014, 55).

2.1 PCI-standardien vertailu

PCI-standardit jaetaan neljään eri standardiin niiden tarkoitusten mukaan, kuten taulukosta 1 selviää. Ehkä tunnetuin näistä on Payment Card Industry Data Security Standard eli PCI DSS -standardi, joka kertoo kauppiaille sekä palveluntarjoajille, miten arkaluontoisia korttitietoja tulee käsitellä ja suojata. Payment Application Data Security Standard eli PA-DSS -standardi antaa maksusovellusten kehittäjille ohjeet, miten heidän tulisi kehittää ohjelmistojaan PCI DSS -standardin mukaisiksi. Pin Transaction Security eli PTS-standardin tehtävä on antaa maksukorttilaitteiden valmistajille ohjeet niiden vähimmäistietoturvavaatimuksista. Uusimpana on Point-to-Point Encryption eli P2Pe -standardi, joka yhdistää kaikki aiemmin mainitut standardit. (Gomzin 2014, 57.)

Taulukko 1. PCI-standardien vertailu (Gomzin 2014, 58).

PCI-standardi	**Kohde**	**Missä käytetään?**	**Kuka käyttää?**
PCI DSS	Ympäristö	Maksuliikennettä käsittelevät ympäristöt	Kauppiaat, palvelun-tarjoajat
PA DSS	Ohjelmistot	Maksuliikenne ohjelmistot	Ohjelmistotoimittajat
PTS	Laitteet	Laitteiden tietoturva-moduulit	Laitteistovalmistajat
P2PE	Ympäristö, ohjelmistot sekä laitteet	P2PE ratkaisut sekä sovellukset	P2PE palveluntarjoajat sekä ohjelmisto-toimittajat

2.2 Miksi PCI-standardeja tulisi noudattaa?

PCI-standardin mukainen järjestelmä tarkoittaa asiakkaalle turvallista järjestelmää ja näin ollen asiakkaan ja kaupan välille syntyy luottamus. Luottamus useimmiten tarkoittaa kaupankäyntiä. Tyytyväiset asiakkaat tulevat todennäköisesti uudelleen ja suosittelevat paikkaa muille. Standardienmukaisuus kasvattaa luottamusta myös yrityskumppanien, kuten tavarantoimittajien sekä maksuja käsittelevien tahojen keskuudessa. Prosessi ennaltaehkäisee tietovuotoja ja maksukorttien väärinkäyttöä. Seuraamalla PCI-standardeja on mahdollista saada hyvä pohja yrityksen tietoturvakäytännöille sekä löytää keinoja IT-infrastruktuurin kehittämiseen ja tehostamiseen. (PCI Security Standard Council 2015b.) Mikäli korttimaksaminen vaarantuu ja standardia ei ole noudatettu, voi kauppias joutua maksamaan sanktioita sekä tapauksesta seuranneet kulut (Nets 2015a).

2.3 PCI DSS -standardi

PCI DSS -standardin noudattaminen on pakollista kaikille yrityksille ja tahoille, jotka käsittelevät, tallentavat tai välittävät kansainvälisten maksukorttien kortti-

tietoja. Standardi määrittelee minimitietoturvatason kaikelle korttimaksamiselle. Standardin tavoitteena on suojata korttitiedot kaikissa tilanteissa ja näin ollen turvata liiketoiminnan turvallisuus, maine sekä jatkuvuus. PCI DSS -standardin noudattaminen tekee korttimaksamisesta turvallisempaa niin kauppiaalle kuin asiakkaallekin. Kauppiaan tulee noudattaa standardia sen vaatimalla tavalla. Kauppias myös vastaa siitä, että kaikki sopimuskumppanit, jotka käsittelevät, välittävät tai tallentavat korttitietoja tai osallistuvat korttitietoja sisältävien järjestelmien ylläpitoon, noudattavat PCI DSS -standardia. (Nets 2015b.)

Visa ja MasterCard raportoivat 1988-1998 välisenä aikana yhteensä 750 miljoonan dollarin arvosta maksukorttipetoksia. Vuosituhannen vaihteessa internetin yleistyessä alkoivat myös internetin välityksellä tehdyt maksukorttipetokset yleistyä. CyberSourcen mukaan vuonna 2000 tehtiin maksukorttipetoksia 1,5 miljardin dollarin edestä pelkästään internetin välityksellä. Näiden tapahtumien seurauksena luottokorttiyhtiöt alkoivat tehdä yhteistyötä, jotta luottokorttipetokset saataisiin aisoihin. PCI DSS -standardin ensimmäinen versio julkaistiin joulukuussa 2004. (SearchSecurity 2013.)

Uusin PCI DSS -standardin versio 3.1 julkaistiin 15.4.2015 ja pitää ottaa käyttöön kokonaisuudessaan 30.6.2016 mennessä (Heinonen 2015). Näiden päivämäärien välissä olevana siirtymäaikana on mahdollista käyttää vielä standardin vanhempaa versiota.

PCI SSC ei ylläpidä minkäänlaista listaa yrityksistä, jotka noudattavat PCI DSS -standardia, vaan yritykset ovat itse vastuussa standardin noudattamisesta. PCI DSS on itse asiassa kauppiaan ja palveluntarjoajan välinen sopimuksellinen asia. Standardia tulee siis noudattaa, mikäli korttitietoja käsitellään tavalla tai toisella. Yrityksen tulee itse noudattaa standardia ja varmistaa, että yrityksen käyttämät palveluntarjoajat noudattavat sitä. (Wright 2011, 33-34.)

2.4 Auditointi

Kaikkien korttitietoja käsittelevien, tallentavien tai välittävien tahojen tulee noudattaa PCI DSS -standardia. Standardin vaatimukset kuitenkin vaihtelevat riip-

puen yrityksen koosta, tavasta vastaanottaa korttitietoja ja vuosittaisista käsiteltyjen korttitietojen määrästä. Vaikka yritys ulkoistaisi maksutoiminnot PCI DSS -standardia noudattavalle kolmannelle osapuolelle, ei se tee yrityksestä automaattisesti standardinmukaista. (Wright 2011, 24, 34.)

PCI-standardien auditoinnin voi suorittaa joko itsenäisesti tai PCI-auditointeja tarjoavan tahon kautta. Järjestelmän saattaminen PCI-standardin mukaiseksi on jatkuva, ei kertaluontoinen, prosessi. QSA eli Qualified Security Assessors ovat PCI SSC:n valtuuttamia asiantuntijoita, jotka auttavat PCI-auditoinneissa. SAQ eli Self-Assessment Questionnaire on lomake, jolla voidaan suorittaa PCI-auditointi itsenäisesti. SAQ -lomakkeita on erilaisia eri käyttötarkoituksiin. Lomakkeiden käyttö määritellään sen mukaan, miten korttimaksuja vastaanotetaan ja korttitietoja käsitellään yrityksessä. Mikäli korttimaksuja käsitellään kolmannen osapuolen toimesta, on lomake huomattavasti suppeampi kuin jos korttitietoja käsitellään ja tallennetaan omilla palvelimilla. (PCI Security Standard Council 2015c, 5, 10, 27, 32.) Tarkemmat auditoinnin kriteerit tulee tarkastaa omalta maksunvälittäjältä (Heikkinen 2014). Esimerkiksi Nets määrittelee, että mikäli vuodessa maksutapahtumia on enemmän kuin miljoona, tulee auditointi suorittaa PCI-auditointeja tarjoavan tahon toimesta, muutoin auditoinnin voi suorittaa itsenäisesti käyttäen SAQ -lomakkeita (Nets 2015a).

Verkkokauppoihin voidaan soveltaa kolmea eri SAQ-lomaketta, SAQ A, SAQ A-EP ja SAQ D. SAQ A -lomaketta käytetään, kun verkkokauppaa ylläpidetään kokonaisuudessaan PCI-auditoidun kolmannen osapuolen toimesta tai kun verkkokauppa käyttää iFrame-elementtiä tai suoraa linkkiä maksusivun näyttämiseen. Maksusivun elementit tulevat ainoastaan PCI-auditoidun kolmannen osapuolen toimesta. SAQ A-EP -lomaketta sovelletaan silloin, kun käytetään iFrame-elementtiä tai suoraa linkkiä maksusivun näyttämiseen, mutta osa sivun sisällöstä, kuten CSS-tyylimäärittelyt tulevat kauppiaan järjestelmästä. SAQ A-EP -lomaketta käytetään myös, mikäli itse verkkokaupassa luodaan maksulomake, joka käyttää DirectPost-menetelmää tietojen siirtämiseen. SAQ D -lomaketta tulee käyttää, kun verkkokauppa ei täytä SAQ A tai SAQ A-EP -

lomakkeiden määrityksiä tai verkkokauppa tallentaa korttitietoja tai maksusivu on kokonaisuudessaan luotu kauppiaan toimesta. (Thomas 2014.)

Eri lomakkeiden merkitys vaadittavan työn ja kustannusten määrässä on suuri. Pienimmällä työllä ja kustannuksilla pääsee SAQ A -lomakkeella. Lomakkeessa on noin 15 sivua, jotka sisältävät 14 kysymystä liittyen itse standardiin. Lisäksi A-lomake ei vaadi säännöllisiä verkkoskannauksia tai penetraatiotestauksia. SAQ A-EP -lomake on työmäärältään jo huomattavasti suurempi, sivumäärä kasvaa jo noin neljäänkymmeneen, ja kysymyksiä itse standardiin liittyen on jo lähes 140. Lisäksi verkkoskannauksia ja penetraatiotestausta tulee tehdä säännöllisesti. SAQ D-lomake on kaikista lomakkeista laajin. Se sisältää noin 330 kohtaa, jotka käyvät jo koko standardin kaikki kohdat läpi sekä vaatii säännöllisesti verkkoskannauksia ja penetraatiotestejä. (Security Metrics 2015.)

3 PCI DSS -STANDARDIN VAATIMUSLUOKAT

PCI DSS -standardi määrittelee kaksitoista vaatimusluokkaa, jotka on jaoteltu kuudeksi kokonaisuudeksi. Kokonaisuudet ovat: turvallinen verkko, korttitietojen suojaaminen, haavoittuvuuksilta suojautuminen, käyttäjien hallinta, verkon valvonta ja tietoturvakäytänteet. (PCI 2015, 5.) Kokonaisuudet ja niiden vaatimusluokat on listattuna taulukossa 2. Tässä luvussa käsitellään PCI DSS -standardin viimeisintä 3.1 versiota.

Taulukko 2. PCI DSS -standardin vaatimusluokat. (PCI 2015, 5; Nets 2015b.)

Kokonaisuus	Vaatimusluokka
Turvallinen verkko	Suojaa tiedot asentamalla palomuuriratkaisu ja ylläpitämällä sitä
	Älä käytä ohjelmistotoimittajan määrittämiä oletussalasanoja tai muita oletusasetuksia
Korttitietojen suojaaminen	Suojaa tallennetut korttitiedot
	Siirrä korttitiedot ja muut luottamukselliset tiedot julkisissa tietoverkoissa salattuina
Haavoittuvuuksilta suojautuminen	Käytä virustorjuntaohjelmistoa ja päivitä se säännöllisesti
	Kehitä turvallisia järjestelmiä ja sovelluksia sekä ylläpidä niitä
Käyttäjien hallinta	Rajoita pääsy tietoihin koskemaan vain niitä, jotka tarvitsen niitä liiketoiminnallisiin tarkoituksiin
	Luo jokaiselle tietojärjestelmän käyttäjälle yksilöllinen käyttäjätunnus
	Rajoita fyysinen pääsy kortinhaltijoiden tietoihin
Verkon valvonta	Seuraa ja valvo kaikkea verkkoresurssien ja kortinhaltijoiden tietojen käyttöä
	Testaa tietoturvajärjestelmät ja -prosessit säännöllisesti
Tietoturvakäytänteet	Luo työntekijöitä ja alihankkijoita koskeva tietoturvakäytäntö

3.1 Turvallinen verkko

Palomuurit ja reitittimet ovat avainasemassa sekä sisään että ulos menevän liikenteen kontrolloimisessa. Standardin mukaan verkon tulee olla suojattu palomuurilla, jotta kaikki luvaton liikenne voidaan estää. Palomuuriratkaisua tulee ylläpitää ja päivittää säännöllisesti, jotta se olisi ajantasainen. Organisaatiolla tulee olla virallinen menettelytapa verkkoyhteyksien hyväksymisille ja testaamiselle sekä kaikille muutoksille palomuureissa ja reitittimissä. Kaikki muutokset verkkoyhteyksissä, palomuureissa ja reitittimissä tulee hyväksyttää, testata ja dokumentoida. (PCI 2015, 19.)

On tärkeää ylläpitää ajantasaista kaaviota kaikista verkon laitteista, yhteyksistä ja konfiguroinneista. Ilman ajantasaista karttaa saattaa jokin laite tai yhteys jäädä huomiotta, ja näin ollen järjestelmään tulee selvä haavoittuvuus. Mikäli korttitietoja tallennetaan, prosessoidaan tai siirretään verkossa, tulee niiden liikkeet ilmetä kaaviossa. (PCI 2015, 20.)

Standardi määrittelee, että palomuuria tulee käyttää kaikissa verkkoyhteyksissä internetin ja DMZ:n välissä sekä DMZ:n ja sisäisen verkon välissä. Näin pystytään seuraamaan ja rajoittamaan pääsyä sekä minimoimaan haitallisten yhteyksien luonti suojattoman yhteyden kautta. Standardin mukaan sekä saapuvaa että lähtevää liikennettä korttitietoihin tulee rajoittaa. Oikeuksia ei tule antaa kuin niitä tarvitseville. Liikenteen rajoittamiseen tulee käyttää niin palomuuria kuin reititystä. Reitittimien konfigurointien tulee pysyä muuttumattomina laitteiden uudelleenkäynnistyksen jälkeen. Standardin mukaan palomuuri tulee määritellä myös langattomille verkoille ja kaikki langaton liikenne korttitietoihin tulee estää, ellei se ole tarpeellista kaupankäynnin kannalta. (PCI 2015, 20-23.)

Standardin mukaan verkon eri osien ylläpidolle tulee määritellä vastuuhenkilö. Näin voidaan varmistua siitä, että jokainen verkon osa pysyy ajantasaisena. Käyttämättömät ja suojaamattomat palvelut, protokollat sekä portit ovat tietoturvan kannalta uhka. Siksi on hyvä dokumentoida selkeästi kaikki käytetyt protokollat, portit ja palvelut sekä niiden käyttötarkoitus. Mikäli jokin näistä ei ole liiketoiminnan kannalta välttämätön, tulee se ottaa pois käytöstä tai poistaa koko-

naan. Myös palomuurin ja reitittimien konfigurointeja tulee tarkistaa säännöllisesti. Tarkistuksessa tulee katsoa läpi kaikki tarpeettomat, vanhat ja ei käytetyt säännöt ja päivittää ne ajan tasalle. Nämä toimenpiteet tulee suorittaa 6 kuukauden välein. (PCI 2015, 21-22.)

Standardin mukaan kaikkiin työntekijöiden käyttämiin kannettaviin tietokoneisiin ja muihin mobiililaitteisiin, jotka ovat yhteydessä internetiin yrityksen verkon ulkopuolella, tulee asentaa ohjelmistopalomuuri. Palomuuri on oltava aina päällä ja toiminnassa. Henkilökohtaisen palomuurin käyttö suojaa laitteita Internetistä tulevilta hyökkäyksiltä. (PCI 2015, 27.)

Gomzin kuitenkin muistuttaa miettimään normaalia myymälää, jossa kassakone ja maksupääte ovat esillä myymälässä. Nämä laitteet ovat yrityksen sisäverkossa, ja periaatteessa kuka tahansa pääsee käsiksi niihin ja sitä kautta verkkoon sekä mahdollisesti korttitietoihin. Hän myös kehottaa pohtimaan, onko yrityksillä resursseja asentaa palomuuriratkaisuja jokaiseen myymälään. (Gomzin 2014, 70.)

Oletusasetukset sekä valmiit käyttäjätunnukset ja salasanat tekevät hakkereiden työn helpoksi. Laitevalmistajat julkaisevat kaikki nämä tiedot sisältävät ohjekirjat sivuillaan ja näin ollen kaikilla on mahdollisuus näitä lukea. On siis tärkeää muuttaa laitteiden ja palveluiden oletusasetukset, käyttäjätunnukset ja salasanat, jotta ulkopuoliset eivät pääse niihin käsiksi. Käyttämättömät käyttäjätilit tulee poistaa käytöstä. Näistä toimista on hyvä luoda käytäntö, jota sovelletaan kaikille laitteille, ennen kuin ne liitetään verkkoon. (PCI 2015, 28-35.)

Gomzin pitää tätä vaatimusta itsestään selvyytenä alan ihmisille ja ihmettelee, miksi siitä on tehty oma vaatimuksensa. Jos mietitään henkilöä, joka konfiguroi palomuureja tai monitoroi verkon liikennettä, kuten muissa vaatimuksissa vaaditaan, pitäisi oletussalasanojen ja -asetusten käytön vaarat olla tiedossa. (Gomzin 2014.)

3.2 Korttitietojen suojaaminen

Korttitietoja ei tule tallentaa, ellei niille ole todellista tarvetta. Mikäli niitä tallennetaan, tulee ne salata ja suojata asianmukaisesti. Taulukkoon 3 on koottu korttitietojen tallennusta koskevat määräykset. Korttitietoihin tulee määritellä sellaiset oikeudet, että niihin pääsevät käsiksi ainoastaan sellaiset henkilöt, jotka niitä tarvitsevat työssään tai omaavat muuten laillisen oikeuden niihin. Mitään todentamistietoja, kuten PIN-koodia, magneettiviivan tai sirun tietoja tai kortin turvanumeroa, ei tule tallentaa missään olosuhteissa. Kyseiset tiedot tulee poistaa heti todentamisen jälkeen. Korttinumero, kortinhaltijan nimi sekä kortin voimassaoloaika ovat tietoja, jotka saa tarvittaessa tallentaa. Korttinumero tulee olla tallennettuna muodossa, jota ei voi lukea. Kun korttinumeroa tarvitaan esimerkiksi kuittiin, siitä saa näkyä enintään kuusi ensimmäistä ja neljä viimeistä numeroa. (PCI 2015, 36-45.)

Taulukko 3. Korttitietojen tallentamisen määräykset. (PCI 2015, 8.)

Tallennettava tieto		Saa tallentaa	Suojattava
Kortinhaltijatiedot	Korttinumero	Kyllä	Kyllä
	Kortinhaltijan nimi	Kyllä	Ei
	Palvelukoodi	Kyllä	Ei
	Voimassaoloaika	Kyllä	Ei
Arkaluontoiset tunnistetiedot	Magneettijuovan ja sirun tiedot	Ei	-
	Kortin turvanumero	Ei	-
	PIN	Ei	-

Korttitietojen suojaamisessa vaikein osuus on tietää, missä tarkalleen tieto kulkee missäkin vaiheessa sen elinkaarta. Mikäli ei tiedä, missä se sijaitsee, on sitä mahdotonta suojata. On tärkeää tietää, missä kaikissa laitteissa tai muissa

paikoissa korttitietoja siirretään tai säilytetään, koska korttitietojen tulee olla aina salatussa muodossa. (Norris 2007.)

Herkät tiedot tulee salata, kun niitä siirretään julkisissa verkoissa. Erityisesti väärin konfiguroidut langattomat verkot sekä salaus- ja todennusprotokollien haavoittuvuudet ovat paikkoja, joista hakkerit voivat päästä käsiksi siirrettäviin korttitietoihin. (PCI 2015, 46.)

Standardin mukaan korttitietojen turvalliseen siirtoon vaaditaan luotettavien avaimien ja sertifikaattien käyttö, turvallisen protokollan käyttö sekä kunnollisen salaustekniikan käyttö korttitietojen salauksessa. Joissain protokollissa, kuten SSL sekä SSH:n ja TLS:n vanhemmissa versioissa, on havaittu haavoittuvuuksia, minkä vuoksi niitä tulisi välttää. Sen sijaan nykyisin hyviä esimerkkejä ovat uusimmat versiot TLS-, SSH- ja IPSEC-protokollista. Kun internet-selaimessa välitetään arkaluontoista tietoa, tulee osoitteen alussa olla HTTPS, joka tarkoittaa, että yhteys on suojattu käyttämällä TLS-protokollaa. (PCI 2015, 46-47.)

Standardi määrittelee, että langattomat verkot tulee suojata käyttäen viimeisintä tekniikkaa, joka tällä hetkellä on WPA2 tietoturvastandardi. Vanhoja tekniikoita, kuten WEP ja SSL, ei tule käyttää. Korttitietoja, kuten korttinumeroa, ei tule lähettää selkokielisenä yleisillä henkilökohtaisilla viestintätavoilla, kuten sähköpostilla, tekstiviestinä tai pikaviestimillä. Mikäli tietoja kuitenkin on tarpeellista lähettää näillä tavoilla, tulee ne suojata asianmukaisesti. (PCI 2015, 48.)

Gomzin muistuttaa, että tänä päivänä kaikki liikenne tulisi olla suojattua, oli liikenne sitten langatonta, langallista, internetin kautta kulkevaa tai vain johtoa pitkin laitteesta toiseen kulkevaa. (Gomzin 2014. 71)

3.3 Haavoittuvuuksilta suojautuminen

Erilaiset haittaohjelmat, kuten virukset, madot, vakoiluohjelmat, mainosohjelmat sekä troijalaiset, leviävät internetin ja muun tekniikan välityksellä helposti. Niitä saattaa liikkua esimerkiksi sähköpostin, muistitikkujen tai internetsivustojen kautta. Kaikkiin käyttöjärjestelmiin, joissa esiintyy yleisesti haittaohjelmia, tulee

asentaa virustorjuntaohjelmisto. Käyttöjärjestelmät, joissa haittaohjelmia ei yleisesti esiinny, tulee tarkastaa säännöllisesti ja arvioida niiden tilanne virustorjuntaohjelmiston osalta uudelleen. (PCI 2015, 49-50.)

Virustorjuntaohjelmiston pitää pystyä havaitsemaan, poistamaan ja suojaamaan kaikenlaisilta tunnetuilta haittaohjelmilta. Ohjelmistot tulee pitää ajantasaisina uusimmilla ohjelmistopäivityksillä sekä virustunnisteilla. Virustarkistukset tulee suorittaa säännöllisesti. Ohjelmistoa ei pidä pystyä ottamaan pois päältä tai muuttamaan sen asetuksia ilman järjestelmävalvojan oikeuksia. Virustorjuntakäytänteet tulee olla dokumentoituna ja käytössä. Standardin mukaan henkilöstö tulee kouluttaa noudattamaan kyseisiä käytänteitä. (PCI 201550-51.)

Gomzin kirjoittaa, että kaikilla kassalaitteilla tulee olla virustorjuntaohjelmisto asennettuna, niin kuin kaikissa laitteissa, jotka ovat yhteydessä internetiin. Hän kuitenkin miettii, että onko oikein luottaa ohjelmistojen valmistajiin korttitietojen suojaamisessa. Eri virustorjuntaohjelmistot saattavat havaita eri haittaohjelmia eivätkä ohjelmistojen kehittäjät välttämättä ole tietoisia siitä, että heidän ohjelmansa ovat osittain vastuussa korttitietojen suojaamisesta. (Gomzin 2014, 71-72.)

Hakkerit käyttävät eri järjestelmien tietoturva-aukkoja päästäkseen järjestelmiin käsiksi. Näitä haavoittuvuuksia ohjelmisto- ja laitteistovalmistajat paikkailevat usein tietoturvapäivityksillä. Järjestelmiin tulee asentaa kaikki asianmukaiset päivitykset tietoturvauhkia vastaan kuukauden kuluessa niiden julkaisusta. (PCI 2015, 52.)

Gomzinin mukaan päivitysten asentaminen toimii hyvin, kun ohjelmistossa on automaattinen ja huomaamaton päivitystoiminto. Monet maksuohjelmistoja kehittävät ohjelmistotoimittajat eivät kuitenkaan vielä käytä niin automatisoituja ohjelmistoratkaisuja, ja näin ohjelmistojen päivittäminen vaatii ihmisen työtä. Tällainen järjestely on Gomzinin mielestä tehoton. (Gomzin 2014, 71.)

Sovelluksia tulee kehittää PCI DSS:n ja muiden alan standardien mukaisesti sekä ottamalla yleinen tietoturva huomioon koko sovelluksen eliniän. Sovelluksista tulee poistaa kaikki kehitys- ja testiympäristöissä käytetyt tilit, käyttäjätun-

nukset sekä salasanat ennen sovelluksen julkaisua. Nämä tiedot väärissä käsissä saattavat helpottaa murtautumista ohjelmistoon ja sitä kautta korttitietoihin. Kaikki koodimuutokset sovelluksissa tulee käydä läpi ennen julkaisua. Läpikäynnin tulee suorittaa joku muu asiantunteva taho kuin koodin kirjoittanut henkilö. Tällä menetelmällä pystytään havaitsemaan mahdolliset haavoittuvuudet ja virheet koodissa. Kaikki löydetyt virheet tulee korjata ja hyväksyttää ennen julkaisua. (PCI 2015, 53-55.)

Ohjelmistojen muutostenhallinnassa prosessien ja menetelmien tulee olla seuraavanlaiset:

- Kehitys- ja testausympäristö pitää olla erillinen kokonaisuus tuotantoympäristöstä. Ympäristöissä tulee olla pääsynhallinta käytössä.
- Pääsy tuotantoympäristöön ja korttitietoihin vain tietyille henkilöille.
- Tuotantoympäristössä olevaa dataa, esim. korttinumeroita, ei tule käyttää kehitys- ja testausympäristöissä.
- Kehitys- ja testausympäristössä käytetty data tulee poistaa ennen tuotantoon siirtämistä.
- Muutosten dokumentoinnin tulee sisältää tiedot muutoksen vaikutuksesta, muutoksen hyväksyjästä, testauksesta sekä peruutusmenetelmästä. (PCI 2015, 55-57.)

Sovelluskehityksessä tulee huomioida yleiset ohjelmoinnin tietoturvaan liittyvät asiat, kuten koodi-injektiot, puskurin ylivuotovirheet, arkaluontoisen tiedon salaus ja cross site scripting. Henkilöstön tulee olla tietoinen ohjelmistojen tietoturvasta ja kouluttautua tarvittaessa. (PCI 2015, 58-62.)

3.4 Käyttäjien hallinta

Standardin mukaan kriittisiin tietoihin tulee määritellä pääsy vain niille, jotka tarvitsevat tietoja työssään. Mitä vähemmän oikeuksia on jaettu, sitä varmemmin tiedot ovat suojassa ja väärinkäytöksiltä vältytään. Oikeudet tulee määritellä työtehtävien mukaisesti ryhmiin ja antaa vain ne tiedot sekä järjestelmät käyt-

töön, joita työn tekeminen vaatii. Näin työntekijälle voidaan antaa työn tekemiseen vaadittavat oikeudet. Oikeuksien myöntäjät sekä itse oikeudet tulee dokumentoida. Lähtökohta kaikkiin korttitietoja koskeviin oikeuksiin on, että oikeudet ovat estettyjä, mikäli niitä ei ole erikseen annettu. (PCI 2015, 64-66.)

Vaikka standardia noudatetaan täysin, ei sillä saavuteta täydellistä suojaa. Korttitiedot näkyvät jossain kohtaa järjestelmää selkokielisenä. Joillakin käyttäjillä, kuten järjestelmänvalvojilla tai muilla pääkäyttäjillä, on aina oltava oikeudet arkaluontoiseen tietoon. Näiden henkilöiden työnkuvaan saattaa liittyä vikojen etsimistä tai järjestelmän ylläpitoa. Nämä käyttäjät eivät välttämättä ole niitä väärinkäyttäjiä, vaan heidän tilinsä voidaan kaapata ja näin väärinkäyttää. (Gomzin 2014, 72-73.)

Standardi määrittelee, että kaikille käyttäjille tulee luoda henkilökohtainen tili, jolla he voivat kirjautua järjestelmiin. Näin pystytään seuraamaan toimintaa sekä selvittämään tarvittaessa väärinkäytöksiä. Käyttäjätilien lisäämistä, poistamista ja muokkaamista tulee valvoa. Kun työntekijä lähtee yrityksestä, tulee käyttäjätilin oikeudet perua mahdollisimman pian. Käyttäjätilit, joita ei käytetä vähintään 90 päivän välein, tulee jäädyttää tai poistaa kokonaan. Standardin mukaan etäyhteyksille tulee määritellä sallitut kellonajat ja yhteyksiä tulee valvoa. Mikäli virheellisiä kirjautumisyrityksiä tulee samalla tilille peräkkäin enintään kuusi kappaletta, tulee kyseinen tili lukita. Näin voidaan välttyä käyttäjätileihin murtautumisilta. Kyseisen tapahtuman seurauksena lukitun tilin tulee olla lukittuna vähintään 30 minuuttia tai lukituksen voi avata järjestelmänvalvoja. Mikäli istunto on ollut enintään 15 minuuttia toimeton, tulee käyttäjältä vaatia uudelleen kirjautuminen. (PCI 2015, 67-69.)

Kun salasanoja tallennetaan tai siirretään verkossa, tulee ne salata asianmukaisesti. Käyttäjän pyytäessä kirjautumistietojen muutoksia, esim. salasanan nollausta sähköpostitse, puhelimitse tai muulla kasvottomalla tavalla, tulee käyttäjän identiteetti varmistaa ennen kun kirjautumistietoja muutetaan. Salasanojen tulee olla vähintään seitsemän merkkiä pitkiä ja sisältää sekä kirjaimia että numeroita. Standardin mukaan käyttäjien tulee vaihtaa salasana vähintään 90 päivän välein. Salasana ei voi olla sama kuin neljänä viime kertana on käytetty.

Käyttäjän tulee vaihtaa salasana ensimmäisen kirjautumisen yhteydessä. Sisäverkon ulkopuolelta tulevilta etäyhteyksiltä tulee vaatia kaksivaiheinen kirjautuminen. Työntekijöille tulee tarjota tietoa ja ohjeistusta salasanoista ja niiden tärkeydestä liittyen tietoturvaan. Näin työntekijät todennäköisemmin noudattavat annettuja ohjeita ja määräyksiä koskien tietoturvaa. (PCI 2015, 70-75.)

Gomzin pitää vaatimusta hyödyllisenä lähinnä tietomurtojen selvittämisessä, ei tietojen suojaamisessa. Kuitenkin kaksi kohtaa hän nostaa esiin tärkeinä korttitietojen suojaamisessa. Hänen mukaansa tärkeimmät kohdat ovat kaksivaiheinen kirjautuminen ulkopuolisista verkoista sekä salasanojen asianmukainen suojaaminen niitä tallennettaessa tai siirrettäessä. (Gomzin 2014, 73.)

Standardin mukaan kaikki laitteet ja järjestelmät, jotka liittyvät korttitietoja sisältävään verkkoon, tulee sijoittaa paikkaan, jossa on mahdollista valvoa ja rajoittaa fyysistä pääsyä. Paikka voi olla lukittava tila, jonne pääsevät vain tietyt henkilöt esimerkiksi kulkukortilla tai avaimella. Tiloissa tulee käyttää tiukkaa kulunvalvontaa, joko videovalvonnalla tai muulla kulunvalvontamekanismilla. Kulunvalvonta tulee määritellä siten, että vierailijat ovat helposti tunnistettavissa, esimerkiksi kulunvalvontakortilla. Työntekijöillä ja vierailijoilla tulee olla erilaiset oikeudet liikkumiseen ja siksi heidät pitää tunnistaa toisistaan. Kun vierailija lähtee, tulee heidän kulkulupansa perua. Työntekijöille tulee määrittää kulkuoikeudet työnkuvan mukaan. Työntekijää ei tule päästää alueille, joita hän ei työssään tarvitse. Mikäli työntekijä esimerkiksi irtisanoutuu, tulee hänen kulkulupansa perua mahdollisimman pian. (PCI 2015, 76-84.)

Standardin mukaan kaikki sähköiset ja paperiset korttitietoja sisältävät mediat tulee suojata asianmukaisesti, kun niitä varastoidaan tai siirretään. Mikäli jotain mediaa ei enää tarvita liiketoiminnallista tai lainmukaisista syistä, tulee se tuhota lukukelvottomaksi. (PCI 2015, 80-81.)

Vaatimus on realistinen ja asianmukainen palveluntarjoajille, joiden laitteet ovat datakeskuksissa, palvelinsaleissa tai muissa vastaavissa paikoissa. Vaatimuksen mukaan tiloissa tulee käyttää tiukkaa kulunvalvontaa esimerkiksi kulunval-

vontakorteilla, joka ei ole kovin realistinen toimenpide myymälöissä. (Gomzin 2014, 73.)

Verizonin mukaan yritykset usein keskittyvät suojautumaan hakkeroinneilta, viruksilta ja muita elektronisilta hyökkäyksiltä ja saattavat jättää fyysisen suojaamisen huomiotta. Tulee muistaa, että mikäli tunkeutuja pääsee fyysisesti käsiksi johonkin laitteeseen, on tietojen väärä käyttö paljon helpompaa ja nopeampaa. (Verizon 2015, 55.)

3.5 Verkon valvonta

Lokien ylläpitäminen sekä käyttäjien toimintojen seuraaminen auttavat ennalta ehkäisemään, havaitsemaan ja minimoimaan tietomurtoja. Lokien pitäminen kaikissa ympäristöissä auttaa myös tietomurtojen ja muiden virheiden etsinnässä. Ilman lokeja olisi lähes mahdotonta selvittää kuka on tehnyt ja mitä. (PCI 2015, 85.)

Kaikilla järjestelmien käyttäjillä tulee olla oma tili kirjautumiseen ja tilien toimia tulee seurata. Lokeihin tulee kerätä tietoa kaikesta epäilyttävästä ja poikkeavasta. Lokien tulee kerätä tietoja käyttäjien yhteyksistä korttitietoihin tai käyttäjätileihin, kirjautumiseen liittyvistä epäkohdista sekä lokeihin tehtävistä muutoksista. Yksittäisen lokin tulee sisältää tietoja käyttäjän tunnistautumisesta, tapahtuneesta asiasta, päivämäärästä ja ajasta, tapahtuman onnistumisesta, paikasta sekä tiedot datasta, komponentista tai resurssista, jota tapahtuma koskee. (PCI 2015, 85-88.)

Pääsy lokeihin tulee olla vain henkilöillä, jotka tarvitsevat niitä työssään. Lokeja ei tule näyttää henkilöille, jotka eivät tarvitse kyseistä tietoa. Lokitiedostot tulee suojata asianmukaisesti, jotta ulkopuoliset eivät pääse muokkaamaan tai tarkastelemaan niitä. Lokitiedostoja tulee säilyttää ainakin 12 kuukautta ennen niiden poistamista sekä niistä tulee olla varmuuskopiot. Lokitietoja tulee tarkkailla päivittäin ja tarkastaa erityisesti tärkeimpien järjestelmien hälytykset ja huomautukset. (PCI 2015, 88-91.)

Verizon pitää vaatimusta tärkeänä ongelmien havaitsemisessa ja niiden selvittämisessä. Asianmukaisten lokien avulla voidaan esimerkiksi selvittää mitä tietoja tietomurron yhteydessä on tehty tai viety. (Verizon 2015, 58.)

Haavoittuvuuksia ja tietoturva-aukkoja löydetään jatkuvasti ohjelmistoista sekä laitteistoista. Tämän vuoksi järjestelmää ja sen osia tulee testata säännöllisesti. Näin varmistutaan hyvästä tietoturvatasosta, vaikka maailma ympärillämme muuttuukin. (PCI 2015, 92.)

Tietomurtoja tapahtuu usein langattomien verkkojen kautta. Siksi on tärkeää tarkastaa langattomien verkkojen laitteet säännöllisesti, ettei verkkoon ole esimerkiksi liitetty ulkopuolisia tukiasemia tai muita laitteita, joiden kautta ulkopuolinen voisi päästä yrityksen verkkoon. Sisä- ja ulkoverkkoihin on suoritettava haavoittuvuustarkastukset vähintään kolmen kuukauden välein sekä silloin, kun verkkoihin tehdään merkittäviä muutoksia. Tarkastuksissa löydetyt epäkohdat tulee korjata mahdollisimman pian. Tarkastus tulee suorittaa uudelleen niin kauan kunnes epäkohtia ei enää löydy. (PCI 2015, 92-95.)

Standardin mukaan järjestelmän tulee havainnoida epäilyttävää korttitietoihin kohdistuvaa liikennettä ja poikkeavia tapahtumia, jotta kaikki tunkeutumisyritykset voidaan havainnoida ja estää. Myös muutosten havainnointijärjestelmä tulisi olla käytössä. Sen tehtävä on hälyttää henkilökunnalle, kun tapahtuu luvattomia muutoksia kriittisiin järjestelmä-, konfigurointi- tai sisältötiedostoihin. (PCI 2015, 99.)

3.6 Tietoturvakäytänteet

Standardin mukaan yrityksellä tulee olla tietoturvakäytänteet. Käytänteet tulee tarkistaa vuoden välein ja päivittää niitä kun järjestelmässä tai ympäristössä tapahtuu muutoksia. Riskien arviointiprosessi tulee tehdä kerran vuodessa ja aina kun järjestelmässä tai ympäristössä tapahtuu merkittäviä muutoksia. Prosessin tulee tunnistaa kriittiset vaarat, uhat ja haavoittuvuudet, ja lopputuloksena prosessista tulee virallinen dokumentti. Standardin mukaan yrityksellä tulee olla käytänteet ja menettelytavat etäyhteyksille, langattomille verkoille, ulkoisille

medioille, sähköpostille, kannettaville laitteille sekä internetin käytölle. (PCI 2015, 100.)

Tietoturvapolitiikan ja menettelytapojen tulee selkeästi määritellä tietoturvan vastuut koko henkilöstölle. Yrityksellä tulee olla erillinen henkilö tai ryhmä, jonka tehtävänä on luoda ja ylläpitää tietoturvakäytänteitä ja menettelytapoja, analysoida tietoturvahälytyksiä ja informaatiota, hallinnoida käyttäjätilejä sekä kontrolloida kaikkea pääsyä korttitietoihin. Standardin mukaan yrityksellä tulee olla virallinen tietoturvaohjelma tai koulutus, jonka tehtävä on antaa kaikille työntekijöille tietoa tietoturvan tärkeydestä erityisesti koskien korttitietoja. (PCI 2015, 101-103.)

Standardin mukaan käytetyistä palveluntarjoajista, jotka pääsevät käsiksi korttitietoihin tai voivat muuten vaikuttaa niiden turvallisuuteen, tulee pitää listaa. Yrityksen ja palveluntarjoajan sopimuksista tulee ilmetä, että kaikki ovat omalta osaltaan vastuussa korttitietojen tietoturvasta. Yrityksen tulee huolehtia, että jokainen käytetty palveluntarjoaja seuraa PCI DSS -standardia. (PCI 2015, 105-107.)

Standardin mukaan yrityksellä tulee olla käytänteet, joita noudatetaan jos tapahtuu tietomurto. Käytänteet tulee testata vähintään vuosittain ja päivittää säännöllisesti. Yrityksen tulee määritellä, että tietyt henkilöt ovat valmiudessa ympäri vuorokauden hälytyksien sattuessa. Henkilökunta tulee kouluttaa toimimaan tietomurtotilanteissa. (PCI 2015, 103-109.)

Verizonin mukaan teknologia voi suojata yritystä ja ylläpitää tietoturvaa vain tiettyyn pisteeseen asti. Tietoturvan heikko lenkki on usein käyttäjä. Mikäli käyttäjät eivät tiedä, miten toimia tai mitä heiltä odotetaan, he voivat laittaa korttitiedot vaaraan. Sen takia on tärkeää ylläpitää ajantasaista ja virallista tietoturvakäytäntöä, josta selviää kuka on vastuussa mistäkin ja mitä heiltä odotetaan. (Verizon 2015, 67.)

4 CASE SCANDINAVIAN OUTDOOR

Scandinavian Outdoor myy välineitä, varusteita ja vaatteita kaikenlaiseen retkeilyyn, urheiluun sekä ulkoiluun. Yrityksellä on useita kivijalkamyymälöitä sekä neljä verkkokauppaa. Scandinavian Outdoor on perustettu 1970 ja yritys työllistää tällä hetkellä noin 100 työntekijää. Liikevaihto tilikaudella 2014-2015 oli noin 18 miljoonaa euroa.

Opinnäytetyön tavoitteena on selvittää mitä vaaditaan, jotta kaikki neljä verkkokauppaa saadaan PCI DSS -standardin mukaisiksi. Scandinavian Outdoor on suorittanut aiemmin PCI DSS -auditoinnin standardin vanhalla versiolla. Vanha versio ei ole enää voimassa, vaan sen päivittäminen on ollut pakollista viimeistään 1. tammikuuta 2015 (Valladares 2013). Nyt on tarkoitus päivittää versioon 3.1.

Scandinavian Outdoorilla on neljä verkkokauppaa, scandinavianoutdoor.fi, ulkoilukappa.com, outdooroutlet.fi sekä retkiaitta.fi. Scandinavian Outdoor on ulkoistanut verkkokauppojen maksutoiminnot kolmannen osapuolen maksunvälittäjälle, eikä itse tallenna, välitä tai käsittele korttimaksuja. Tällä hetkellä retkiaitta.fi on ulkopuolisen verkkokauppaohjelmiston alaisena ja maksut kulkevat kolmannen osapuolen maksuvälittäjän kautta. Muut kolme verkkokauppaa ovat oman verkkokauppaohjelmiston alaisena, ja niitä kehitetään yrityksessä itsenäisesti. Myös näissä verkkokaupoissa maksut kulkevat kolmannen osapuolen maksunvälittäjän kautta. Maksunvälittäjä on tosin eri kuin retkiaitta.fi:ssä, mutta toiminta on samanlaista.

5 PCI DSS -STANDARDIN MUKAINEN VERKKOKAUPPA

PCI DSS -standardin noudattaminen on pakollista kaikille tahoille, jotka vastaanottavat korttimaksuja tai tallentavat, välittävät tai käsittelevät korttitietoja (Nets 2015b). Näin ollen jokainen verkkokauppa, jossa voi käyttää maksukorttia maksamiseen, on velvollinen noudattamaan standardia. Verkkokauppa voi kuitenkin supistaa omaa osuuttaan standardin noudattamisessa ulkoistamalla maksuprosessin kolmannen osapuolen maksunvälittäjälle. Tällöin verkkokauppiaan tulee kuitenkin varmistaa, että käytetty palveluntarjoaja noudattaa PCI DSS -standardia (Wright 2011, 33-34).

Standardi saattaa vaikuttaa ensisilmäyksellä monimutkaiselta ja onkin sitä mikäli korttitietoja käsitellään, välitetään tai tallennetaan itse. Verkkokaupan ulkoistaessa maksupalvelut kolmannen osapuolen hoidettavaksi helpottuvat PCI DSS -standardin vaatimukset verkkokaupan osalta huomattavasti.

Standardinmukaisuuden voi tarkastuttaa käytännössä kahdella eri tavalla, ulkopuolisen PCI-auditointeja tarjoavan kolmannen osapuolen toimesta tai täyttämällä asianmukaisen SAQ-lomakkeen. QSA:n avulla auditointi voidaan suorittaa minkäkokoiselle yritykselle tahansa riippumatta siitä, miten maksuja tai korttitietoja vastaanotetaan. QSA:n tehtävänä on joko auttaa auditoinnissa tai suorittaa se yrityksen puolesta. (PCI Security Standard Council 2015c, 10.) Itsenäisen auditoinnin SAQ-lomakkeen avulla voi suorittaa, mikäli korttimaksuja vastaanotetaan vuodessa alle miljoona (Nets 2015a). Tarkemmat auditoinnin vaatimukset tulee kuitenkin tarkastaa omalta maksupalveluntarjoajalta (Heikkinen 2014). Esimerkiksi raportointi standardin noudattamisesta saattaa olla erilainen eri palveluntarjoajilla.

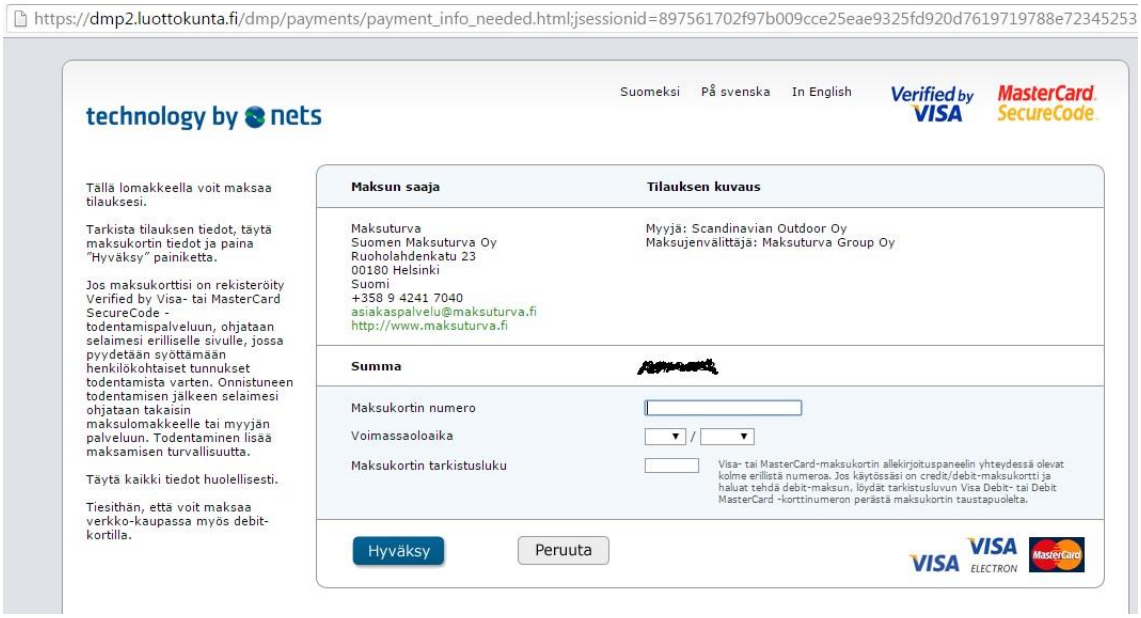
Standardin 12 vaatimusluokkaa antavat hyvän lähtökohdan ja paljon mietittävää tietoturvakäytännöille ja -ohjeistuksille mille tahansa yritykselle. Tulee kuitenkin muistaa, että vaikka noudattaisi standardin jokaista kohtaa, ei se tee tietoturvasta pettämätöntä. Standardi antaa vain vähimmäisvaatimukset tietoturvalle kortti-

tietoja käsiteltäessä. Maailma myös muuttuu koko ajan ja uusia tietoturvauhkia sekä -aukkoja löydetään jatkuvasti.

5.1 Laajuuden selvittäminen

Yrityksen PCI DSS -standardin mukaisuuden saavuttamiseksi ensimmäinen askel on selvittää, miten, missä ja kuinka paljon korttimaksuja tai tietoja yrityksessä vastaanotetaan. Scandinavian Outdoorin tapauksessa korttimaksuja vastaanotetaan vuodessa alle miljoona ja maksut vastaanotetaan kolmannen osapuolen maksunvälittäjän toimesta. Tämän vuoksi PCI DSS -auditointiin voidaan käyttää itse täytettyä SAQ-lomaketta tai vaihtoehtoisesti ulkopuolista PCI-auditointeja tarjoavaa tahoa.

Oikean SAQ-lomakkeen valitsemiseksi tulee selvittää miten korttimaksut vastaanotetaan ja vielä tarkemmin, että miten ja kenen toimesta maksusivu luodaan. Scandinavian Outdoorin tapauksessa korttitiedot syötetään maksusivulle, joka tulee kokonaisuudessaan kolmannen osapuolen toimesta, kuten kuvasta 1 selviää. Tämän takia oikea lomake on SAQ A.



Kuva 1. Maksusivu.

5.2 SAQ A -lomake

Ennen kuin lomakkeelta löytyy mitään täytettävää, sieltä selviää minkälainen kauppiaan maksukanavan tulee olla. Lomake velvoittaa yritystä tarkastamaan seuraavat asiat:

- Yritys vastaanottaa ainoastaan verkkokauppamaksuja.
- Yritys on ulkoistanut kaikki korttitietojen tallentamisen, siirtämisen ja välittämisen PCI DSS -standardia noudattavalle kolmannen osapuolen palveluntarjoajalle.
- Yritys ei tallenna, siirrä tai välitä korttitietoja sähköisesti järjestelmissään tai toimitiloissaan, vaan on ulkoistanut toiminnot PCI DSS -standardia noudattaville toimijoille.
- Yritys varmistaa, että kaikki palveluntarjoajat, jotka käsittelevät korttitietoja noudattavat PCI DSS -standardia.
- Yritys säilyttää ainoastaan paperiraportteja tai kuitteja korttitiedoista ja näitä tietoja ei vastaanoteta sähköisesti.
- Yritys varmistaa, että kaikki maksusivun elementit tulevat PCI DSS -standardia noudattavalta palveluntarjoajalta. (PCI Security Standard Council 2015d, iii, 3.)

Mikäli yritys ei täytä näitä kriteereitä, ei kyseistä SAQ-lomaketta voi käyttää. Tällöin kannattaa selvittää uudelleen, mikä lomake yritykselle olisi oikea. Lisäksi lomake antaa ohjeet SAQ mekanismin käyttöön sekä yksityiskohtaiset ohjeet itse lomakkeen täyttämiseen (PCI Security Standard Council 2015d, iii-v).

Täytettävät kohdat alkavat yrityksen ja mahdollisen QSA:n perustiedoilla kuten nimillä, osoitteilla ja puhelinnumeroilla. Vielä ennen varsinaisia korttitietoja koskevia kysymyksiä, tulee lomakkeelle selventää yrityksen toimintaa korttitietoihin liittyen. Nämä kohdat sisältävät kysymyksiä mm. käytetyistä maksunvälittäjistä, maksusovelluksista sekä tavoista vastaanottaa maksuja. (PCI Security Standard Council 2015d, 1-3.)

Lomakkeen varsinaisissa korttitietoihin kohdistuvissa kysymyksissä selvitetään muutamia kohtia standardin vaatimuksista yhdeksän ja kaksitoista. Lomakkeen avulla varmistetaan, että mikäli yritys vastaanottaa maksuvälittäjältä paperisia kuitteja tai raportteja, jotka sisältävät korttitietoja, tulee näitä dokumentteja käsitellä standardin vaatimalla tavalla sekä mikäli dokumentteja ei enää tarvita tulee ne tuhota asianmukaisesti. Lisäksi varmistetaan, että yritys ylläpitää listaa palveluntarjoajista, jotka liittyvät korttitietoihin sekä palveluntarjoajat ovat tietoisia PCI DSS -standardista ja noudattavat tätä. Yrityksen tulee siis varmistua, että käytetyt palveluntarjoajat noudattavat PCI DSS -standardia ja he ovat tietoisia vastuustaan korttitietojen tietoturvassa. Lomakkeella on muutama liite, joita pitää täyttää riippuen aiemmin annetuista vastauksista. Liitteiden avulla täydennetään vastauksia tarpeen mukaan. (PCI Security Standard Council 2015d, 4-10.)

Lopuksi lomakkeella on yhteenveto täytetyistä tiedoista sekä allekirjoitukset asiaankuuluvilta henkilöiltä. Yhteenvedossa tarkastetaan, että täyttääkö yritys standardin vaatimat kohdat eli noudattaako yritys standardia vai tarvitaanko muita toimenpiteitä sen noudattamiseen. Tämä tarkastus tehdään rasti ruutuun menetelmällä. Näin tarkastetaan, että kaikki tarpeelliset kohdat on täytetty ja läpäisty. (PCI Security Standard Council 2015, 11-12.)

Kun lomake on täytetty ja yritys todettu standardinmukaiseksi, tulee lomake toimittaa maksunvälittäjälle tai muulle taholle, joka vaatii noudattamaan standardia. Mikäli mikään taho ei vaadi raportointia standardin noudattamisesta, riittää pelkkä SAQ-lomakkeen täyttäminen (PCI Security Standard Council 2015d, iii.) Mikäli lopputuloksena todetaan, että yritys ei täytä lomakkeella esitettyjä standardin vaatimuksia, tulee yrityksen korjata puuttuvat virheet ja suorittaa prosessi uudelleen, kunnes yritys täyttää lomakkeella esitetyt standardin vaatimukset (PCI Security Standard Council 2015d, 11, 13).

5.3 Suositukset

Scandinavian Outdoorin tapauksessa PCI DSS -auditointi voidaan suorittaa itsenäisesti SAQ A -lomaketta käyttäen. Yrityksen tulee tarkastaa, että käytetyt

palveluntarjoajat noudattavat PCI DSS -standardia sekä selvittää tuleeko heidän raportoida omasta PCI DSS -standardin noudattamisesta jollekin palveluntarjoajalle.

PCI DSS -standardin auditointiprosessiin on hyvä määrittää vastuuhenkilö. Henkilön tehtävänä on selvittää auditoinnin laajuus ja täyttää tarvittavat lomakkeet sekä olla yhteydessä tarvittaessa palveluntarjoajiin. Vastuuhenkilön on oltava tietoinen järjestelmän muutoksista ja standardin uusista versioista, jotka vaikuttavat standardinmukaisuuteen.

Vaikka standardi ei vaadi yksinkertaisimmassa muodossaan itse verkkokaupan tietoturvalta mitään, tulee siihen kuitenkin kiinnittää huomiota. Jos maksusivulle siirtymiseen käytetään suoraa linkkiä tai iFrame-elementtiä, on tärkeää, että niissä oleviin linkkeihin ei pääse ulkopuolinen taho käsiksi. Jos ulkopuolinen pääsisi niihin käsiksi, olisi mahdollista muuttaa linkki virheelliseksi maksusivuksi ja tällöin korttitiedot olisivat vaarassa.

6 YHTEENVETO

PCI DSS -standardin vaatimukset verkkokaupalle riippuvat miten, missä ja kuinka paljon korttimaksuja vastaanotetaan. Scandinavian Outdoorin tapauksessa korttimaksut kulkevat PCI DSS -standardia noudattavan maksunvälittäjän kautta, maksusivu luodaan kokonaisuudessaan maksunvälittäjän kautta sekä maksutapahtumia vuodessa on alle miljoona. Scandinavian Outdoorin voi käyttää joko ulkopuolista PCI-auditoijaa tai käyttää SAQ A -lomaketta todetakseen verkkokauppojensa noudattavan PCI DSS -standardia.

PCI DSS antaa toimintaohjeet kaikille korttimaksuja käsitteleville toimijoille ja parantaa näin korttimaksujen tietoturvaa. Kaikkien toimijoiden kannalta oleellista on tietää missä ja miten korttitietoja käsitellään. Tärkeimpänä asiana on muistaa, ettei korttitietoja tule tallentaa ellei sille ole todellista tarvetta.

Opinnäytetyön tavoitteena oli selvittää, mikä PCI DSS -standardi on ja mitä se sisältää sekä selvittää miten toimeksiantajan verkkokaupat saadaan noudattamaan standardin uusinta versiota. Asetetut tavoitteet täytettiin ja toimeksiantaja saa työstä hyvän pohjan PCI DSS -standardin ymmärtämiseen ja sen ajantasalle saattamiseen. Vaikka työ onkin tehty yksittäisen tapauksen perusteella, voivat muut yritykset käyttää työtä selvittääkseen standardin vaatimukset omalle toiminnalleen.

PCI DSS -standardi ei ollut itselleni entuudestaan tuttu. En oikeastaan ollut kuullut koko standardista ennen kuin aihetta minulle ehdotettiin. Työn aikana opin itse standardista ja siihen liittyvistä asioista paljon ja koen, että työ on ollut hyvin opettavainen ja hyödyllinen itselleni. Kokonaisuudessaan standardi on hyvin laaja ja siksi työn rajaaminen ja keskittäminen verkkokaupan näkökulmaan oli hyvä päätös.

LÄHTEET

Aaltio, I. 2014. Case-tutkimus metodisena lähestymistapana. Viitattu 11.11.2015 https://metodix.wordpress.com/2014/05/19/aaltio-marjosola-casetutkimus/.

Gomzin, S. 2014. Hacking Point of Sale : Payment Application Secrets, Threats, and Solutions. Indianapolis, Indiana: John Wiley & Sons, Inc.

Heikkinen, S. 2014. Verkkokaupat PCI DSS -standardin kurimuksessa. Viitattu 5.11.2015 http://www.nixu.com/fi/blogi/2014-09/verkkokaupat-pci-dss-standardin-kurimuksessa.

Heinonen, P. 2015. Version 3.1 of the PCI DSS standard drives better encryption. Viitattu 2.12.2015. http://www.nixu.com/en/blog/2015-08/version-31-of-the-pci-dss-standard-drives-better-encryption.

Lukka, K. 2014. Konstruktiivinen tutkimusote. Viitattu 11.11.2015 https://metodix.wordpress.com/2014/05/19/lukka-konstruktiivinen-tutkimusote/.

Nets 2015a. Tuki - Usein kysyttyä - Turvallisuus. Viitattu 30.9.2015 http://www.nets.eu/fi-fi/tuki/usein-kysyttya/turvallisuus/Pages/default.aspx.

Nets 2015b. Tuotteet ja Palvelut - Korttimaksujen vastaanotto - Turvallisuus. Viitattu 30.9.2015 http://www.nets.eu/fi-fi/tuotteet-ja-palvelut/korttimaksujen-vastaanotto/ohjeita/Pages/Turvallisuus.aspx.

Norris, C. 2007. Guide to passing PCI's five toughest requirements. Viitattu 4.11.2015 http://searchsecurity.techtarget.com/tip/Guide-to-passing-PCIs-five-toughest-requirements.

PCI 2015. Payment Card Industry Data Security Standard. Requirements and Security Assessment Procedures. Version 3.1. Viitattu 11.11.2015 https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf.

PCI Security Standard Council 2015a. About Us. Viitattu 24.9.2015 https://www.pcisecuritystandards.org/organization_info/index.php.

PCI Security Standard Council 2015b. Why Comply?. Viitattu 30.9.2015 https://www.pcisecuritystandards.org/security_standards/why_comply.php.

PCI Security Standard Council 2015c. PCI DSS Quick reference guide. Viitattu 24.11.2015 https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf.

PCI Security Standard Council 2015d. Self-Assessment Questionnaire A and Attestation of Compliance. Viitattu 26.11.2015 https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1_SAQ_A_rev1-1.pdf.

SearchSecurity 2013. The history of the PCI DSS standard. Viitattu 23.10.2015. Security Metrics 2015. Ecommerce Guide to PCI DSS 3.0. Viitattu 11.11.2015 https://www.securitymetrics.com/static/resources/orange/Ecommerce_slide_show_v3.pdf.

Security Metrics 2015. Ecommerce Guide to PCI DSS 3.0. Viitattu 11.11.2015 https://www.securitymetrics.com/static/resources/orange/Ecommerce_slide_show_v3.pdf.

Thomas, T. 2014. SAQ A vs. A-EP: What E-Commerce Merchants, Service Providers Need to Know Now. Viitattu 5.11.2015 https://www.pcicomplianceguide.org/saq-a-vs-a-ep-what-e-commerce-merchants-service-providers-need-to-know-now/.

Valladares C. 2013. How PCI DSS v3.0 Will Affect Your Organization. Viitattu 6.11.2015 http://www.tripwire.com/state-of-security/regulatory-compliance/will-pci-dss-v3-0-affects-organization/.

Verizon 2015. PCI Compliance Report. Viitattu 18.11.2015 http://www.verizonenterprise.com/resources/report/rp_pci-report-2015_en_xg.pdf.

Wright S. 2011. PCI DSS: A Practical Guide to Implementing and Maintaining Compliance, third edition. Cambridgeshire: IT Governance Publishing.