LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Sosiaalisen median riskit yritysmaailmassa

Kilpinen, Joni

2015 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Sosiaalisen median riskit yritysmaailmassa

Kilpinen, Joni
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Maaliskuu, 2015

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Kilpinen, Joni

Sosiaalisen median riskit yritysmaailmassa

Vuosi 2015 Sivumäärä 65

Sosiaalisen median palveluista on kirjoitettu lukuisia kirjoja ja artikkeleita, joissa niitä ylistetään varsinkin yritysnäkökulmasta. Vaikka sosiaalinen media on muuttanut olennaisesti tapaa, jolla keskustella, mainostaa, etsiä ja jakaa tietoa, piilee sen palveluiden käytössä kuitenkin erilaisia uhkakuvia. Yritykset ja asiantuntijat pelkäävät sosiaalisen median avoimuuden aiheuttavan suuria tietoturvariskejä. Lisäksi asiantuntijat ovat varoitelleet sosiaalisessa mediassa olevista haittaohjelmista, joita liikkuu sen tuomissa sovelluksissa.

Tämän opinnäytetyön tarkoituksena on tutkia sosiaalisen median käyttöön liittyviä uhkia yritysmaailmassa. Opinnäytetyö vastaa kolmeen kysymykseen. Ensiksi opinnäytetyössä tutkitaan, minkälaisia riskejä sosiaalinen media saattaa tuoda yrityksille. Toiseksi tarkastellaan, miten yritykset ja sen työntekijät voivat suojautua sosiaalisen median riskeiltä. Kolmanneksi selvitetään, miksi riskejä pääsee syntymään sosiaalisessa mediassa.

Ensimmäisessä kysymyksessä tutkitaan kaikkia niitä tekijöitä, jotka voivat aiheuttaa yrityksille ei-toivottuja tuloksia sosiaalisessa mediassa. Tavoitteena on löytää keskeiset asiat, jotka nykypäivän yritysten pitäisi huomioida oman tietoturvansa kannalta. Vastaus toiseen ja kolmanteen kysymykseen haetaan käyttämällä hyväksi edellisen tutkimuskysymyksen vastauksia. Vastauksia käyttämällä tutkitaan syitä siihen, miksi riskejä pääsee syntymään nykypäivän yrityksissä.

Opinnäytetyö osoittaa, että sosiaalisessa mediassa on monenlaisia eri riskitekijöitä. Suurin syy, miksi riskejä syntyy sosiaalisessa mediassa, johtuu yritysten työntekijöistä. Suurimpia ongelmien aiheuttajia ovat ihmisten huolimattomuus ja tietämättömyys. Vastaukseksi toiseen tutkimuskysymykseen on, että sosiaalisen median käyttäjien kannattaa aina miettiä ennen kommenttien ja muun materiaalin lisäämistä sekä muistaa tietoturvan perussäännöt. Paras keino ennaltaehkäistä riskien syntyminen on selkeä ohjeistus työyhteisössä, henkilöstön koulutus ja turvallisuustietoisuuden lisääminen. Opinnäytetyössä käy ilmi, että sosiaalisessa mediassa syntyvien odottamattomien riskien suurimmat aiheuttajat ovat: ihmisten sosiaalisuuden tarve, suuri luottamus muihin ihmisiin ja keskittynyt rikollinen toiminta.

Sosiaalinen media, riskit, työelämä, Facebook, Twitter

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

Kilpinen, Joni

Social Media Risks in Business

Year 2015 Pages 65

Numerous books and articles have been written from the social media perspective. Most of the books are praising social media, especially from the business viewpoint. Although social media has substantially changed a way to discuss, advertise, search and share information, it also includes different kind of threats. Companies and experts fear that the transparency of social media might cause some major security risks. Experts have also warned about various social media malwares.

The purpose of this thesis is to conduct a research about social media risks in a corporate world. This thesis replies to the three research questions. Firstly, in this thesis it is studied what kind of risks social media might bring for businesses. Secondly, it is examined how businesses and employees can protect themselves from social media risks. Thirdly, it is inspected why social media risks are occurring in business world and what are the reasons behind it.

The first question is approached by analysing all the factors that could cause businesses to get undesirable results in social media. The goal is to find key issues which businesses should take into account to have better and safer network security. The answers for the second and third research questions are found by using the answers from the previous research question. The purpose is to find the main reasons why social media is causing so many different risks for businesses.

The conclusion of this thesis is that there is a wide range of risk factors in social media. The biggest reason why different kinds of risks are happening is people's carelessness and ignorance. The response to the second research question is that social media users should always think before adding some comments. It is also always good to remember the basic IT-security rules. The best ways to prevent risks from occurring are clear guidance in working community, personnel training and the increase of security awareness. The thesis shows that the main reasons why social media is creating unforeseen risks are: need to socialize, great confidence in other people and focused criminal activity.

Social media, risks, working life, Facebook, Twitter

Sisällys

1 Johdanto

Sosiaalisen median suosio on kasvanut räjähdysmäisesti erittäin lyhyessä ajassa. Samalla se on muuttanut ihmisten tapaa jakaa ja vastaanottaa eri muodoissa olevaa tietoa. Tiedonjakaminen ei olekaan koskaan ollut yhtä helppoa ja nopeaa, kun se on nykypäivän sosiaalisilla työkaluilla. Tämä saattaa aiheuttaa yrityksille monenlaisia ongelmia, joista osa on vältettävissä toimimalla sosiaalisessa mediassa harkiten ja ohjeistamalla omia työntekijöitä siitä, mitä asioita sosiaalisessa mediassa ei saa jakaa.

Monien yritysten johtajat ovatkin erittäin huolestuneita työntekijöidensä sosiaalisessa mediassa jakamista asioista. Samalla tietoturvallisuusasiantuntijat varoittavat sosiaalisen median riskeistä. Asiantuntijoiden mukaan sosiaalinen media mahdollistaa haittaohjelmien leviämisen laitteesta toiseen sekä yrityssalaisuuksien vuotamisen ulkopuolisille henkilöille. Tämän johdosta osa yritysjohtajista on kieltänyt sosiaalisen median käytön yritysten omista tietoverkoista.

Tämän opinnäytetyön tarkoitus on tarkastella sosiaalisen median tuomia riskejä ja selvittää, miksi erilaisia sosiaaliseen mediaan liittyviä ongelmia on päässyt käymään eri yrityksissä. Tutkimus on toteutettu käyttäen laadullisen tutkimuksen menetelmiä eli kvalitatiivista tutkimusta ja tutkimusstrategiaksi valittiin toimintatutkimus.

Opinnäytetyön päätavoitteena on löytää vastaukset seuraaviin tutkimuskysymyksiin:

- Minkälaisia riskejä sosiaalinen media saattaa tuoda yrityksille?
- Miten yritykset ja sen työntekijät voivat suojautua sosiaalisen median riskeiltä?
- Miksi riskejä pääsee syntymään yritysten ja työntekijöiden toimiessa sosiaalisessa mediassa?

Tämän opinnäytetyön pääpaino on Suomen käytetyimmissä sosiaalisen median palveluissa. Opinnäytetyön tarkastelun kohteena ovat: Facebook, Twitter, LinkedIn, YouTube ja keskustelufoorumit. Valinta perustui kävijämäärätutkimuksiin, joissa selvitettiin mitä sosiaalisen median palveluita Suomessa käytetään kaikkein eniten. Vaikka sosiaalinen media on todistetusti oiva työkalu lisäämään yritysten tuottavuutta, käydään tässä opinnäytetyössä pääasiassa läpi vain sen tuomia riskejä. Tämän opinnäytetyön tarkoitus ei ole perehdyttää lukijaa lainsäädäntöasioihin, muutamaa oleellista viittausta lukuun ottamatta.

Opinnäytetyö etenee johdatuskappaleen jälkeen seuraavasti. Kappaleessa kaksi kuvaillaan tutkimusmetodeita, joita tässä opinnäytetyössä käytettiin. Kolmannessa kappaleessa selvitetään tämän työn tärkeimmät tutkimuskäsitteet. Kappaleessa neljä avataan käsite ”sosiaalinen media” sekä kerrotaan, miten kaikki alkoi. Lisäksi kappaleessa kerrotaan lyhyesti suosituim-

mista sosiaalisen median palveluista. Kappale viisi vastaa kysymykseen, millaiset ovat yritysten ja työntekijöiden sananvapaussäädökset. Kappaleessa kuusi tutkitaan sosiaalisen median sääntelyyn liittyviä asioita. Kappaleessa seitsemän kerrotaan, minkälaisia ongelmia sosiaalinen media saattaa aiheuttaa työntekijöissä. Lisäksi kappaleeseen on kerätty käytännön ohjeita yrityksille, jotta toimiminen sosiaalisessa mediassa olisi mahdollisimman turvallista. Kahdeksannessa kappaleessa käydään läpi muutamalle yritykselle aiheutuneita ongelmia sosiaalisen median aikakaudella.

Yhdeksännessä kappaleessa vastataan kysymykseen, millaista rikollista toimintaa sosiaalisessa mediassa on ja mihin yritysten kannattaa varautua. Kappaleessa kymmenen käydään läpi tietoturvariskejä, joita yritysten on syytä ottaa huomioon sosiaalisen median kannalta. Kappaleessa yksitoista kerrotaan puolestaan, miten yritysten on mahdollista suojautua erilaisilta sosiaalisen median riskiltä. Kahdennessatoista kappaleessa on yhteenveto koko opinnäytetyöstä. Kappaleessa pohditaan asioita, jotka vaikuttivat opinnäytetyöaiheen valitsemiseen sekä sen työstämiseen. Kappaleessa annetaan myös suosituksia jatkotutkimusten aiheiksi.

2 Opinnäytetyön tutkimuksellinen viitekehys

Tutkiminen on valintojen ja päätösten tekoa aina siihen saakka, kun tutkielma on viimeistelty ja julkaistu. Ennen aineiston keruuta on tehtävä monenlaisia valintoja. Keskeisimmät valinnat ovat tutkimuksen kohde sekä aineistotyypin- ja tutkimuksellisen lähestymistavan valitseminen. Kaikkein syvimmät päätökset tehdään tieteenfilosofisella tasolla joko tiedostaen tai tiedostamatta. (Hirsjärvi, Remes & Sajavaara 2012, 123.)

Tutkimuksen tekijät useimmiten nojautuvat johonkin tiettyyn tutkimukselliseen lähestymistapaan kerta toisensa jälkeen. Erilaisia tutkimuksellisia lähestymistapoja on useita ja niiden muistaminen saattaa olla vaikeaa. Psykologisesti suuntautuneet tutkijat saattavat käyttää vain eksperimentaalista strategiaa ja sosiaalitieteilijät vain survey-aineiston tilastollisen käsittelyn tutkimustapaa. (Hirsjärvi ym. 2012, 132.)

2.1 Laadullinen tutkimus ja valintaan vaikuttavat haasteet

Tämän opinnäytetyön lähestymistavaksi valittiin laadullinen tutkimus eli kvalitatiivinen tutkimus. Se soveltuu hyvin tutkimuksen lähestymistavaksi, koska se on luonteeltaan kokonaisvaltaista tiedonhankintaa, ja aineisto kootaan todellisista tilanteista (Hirsijärvi ym. 2012, 164). Laadullisessa tutkimuksessa on tyypillistä kuvata merkityksiä eli esimerkiksi ongelmien syitä ja seuraamuksia (Saaranen-Kauppinen & Puusniekka).

Laadullinen tutkimus vastaa ensisijaisesti kysymyksiin miksi, millainen ja miten. Sitä käytetään helpottamaan asioiden ymmärtämistä esimerkiksi ihmisten, kuluttajien ja asiakkaiden näkökulmasta. Laadullinen tutkimusmenetelmä on erityisen hyödyllinen silloin kun tarvitaan tietoa asioista, joita ei tunneta tai tiedetä erityisen hyvin. (Inspirans.) Laadulliseen tutkimukseen kuuluu joukko mitä moninaisimpia tutkimuksen lajeja (Hirsijärvi ym. 2012, 162). Tutkimuslajien laajasta joukosta, valittiin tämän opinnäytetyön tutkimuslajiksi toimintatutkimus.

Laadullisen tutkimusmenetelmän tarkastelu aloitettiin tutkimalla siitä kertovaa lähdemateriaalia. Lähdemateriaalia vertailemalla ja tavoitteita sekä alustavia tutkimuskysymyksiä tarkastelemalla päädyttiin kolmeen mahdolliseen tutkimusmenetelmään. Nämä ovat: tapaustutkimus, toimintatutkimus ja konstruktiivinen tutkimus. Työtä voidaan lähestyä minkä tahansa edellä mainittujen tutkimusmenetelmiä käyttäen.

Mikäli työtä lähestytään tapaustutkimuksena, on kyse empiirisestä tutkimuksesta, jossa tutkitaan nykyajan ilmiötä todellisessa elämän tilanteessa käyttämällä useita eri tietolähteitä. Tutkimusstrategia valitaan silloin, kun halutaan kysyä kuinka- ja miksi-kysymyksiä nykyajan tapahtumista, joita tutkija itse ei voi kontrolloida. (Koskennurmi-Sivonen.)

Jos työtä puolestaan lähestytään toimintatutkimuksena, on kysymyksessä tutkimus, jossa etsitään ratkaisuja erilaisiin ongelmiin. Käytännössä toimintatutkimuksessa olennaista on ihmisten välinen vuorovaikutus. (Kuula.) Toimintatutkimuksella pyritään saattamaan yhteen teorian ja käytännön sekä tutkijat ja käytännön edustajat (Piippo 2013). Toimintatutkimus on aina myös tapaustutkimusta. Tämän takia sen empiirinen tieto on paikallista ja suorassa suhteessa toimintaan. (Linturi 2003.)

Konstruktiivinen tutkimus on metodologinen lähestymistapa, jota voidaan tarkastella yhtenä tapaustutkimuksen muotona ollen rinnastettavissa teoriaa havainnollistavaan case-tutkimukseen, teoriaa testaavaan case-tutkimukseen ja toimintatutkimukseen. Konstruktiivinen tutkimus on luonteeltaan ongelmakeskeistä, jossa tyypillisesti päämääränä on parantaa ja kontrolloida tosielämän tapahtumia. (Anttila 1998.)

2.2 Toimintatutkimus

Tässä opinnäytetyössä käytettiin toimintatutkimusta strategisesti hyväksi työn eri vaiheissa. Kirjallisuuskatsausta käyttämällä saatiin kuva tutkimusmenetelmistä sekä työn taustalla vaikuttavista teorioista. Aineistoanalyysiä käyttämällä tutkittiin Internetistä ja muista lähteistä kerättyä aineistoa sosiaalisesta mediasta ja sen riskeistä.

Toimintatutkimuksen avulla etsitään ratkaisuja erityyppisiin ongelmiin. Ongelmat voivat olla esimerkiksi yhteiskunnallisia, sosiaalisia, eettisiä tai ammatillisia. Toimintatutkimuksille on tyypillistä muun muassa käytännön suuntautuminen, ongelmakeskeisyys sekä tutkijan ja tutkittavien roolit aktiivisina toimijoina muutosprosesseissa. (Kuula.)

Toimintatutkimuksessa on olennaista tiedon ja ymmärryksen kumulatiivinen kasvu. Sen lähtökohta on useimmiten käytännön työelämän tilanne, joka koetaan jostakin syystä ongelmalliseksi. Kehittämistarpeet johtuvat usein ympäristön jatkuvasta muutoksesta. Yksikään organisaatio ei voi pitkään elää irrallaan ympäristöstä, vaan sen on vähintään mukauduttava ympäristömuutoksiin. Toimintatutkimus pyrkii vaikuttamaan käytännön toimintojen kehittymiseen, osallistujien toimintojensa ymmärtämiskyvyn kehittymiseen ja itse toimintatilanteen kehittymiseen. (Linturi 2003.)

3 Opinnäytetyön tärkeimmät käsitteet

Tämän työn keskeisimpiä käsitteitä ovat sosiaalinen media, riski, uhka, verkkorikollisuus ja tietoturva. Käsitteet avataan tarkemmin tutkimuksen myöhemmässä vaiheessa.

Sosiaalisella medialla tarkoitetaan verkkoympäristöä, jossa jokaisella sen käyttäjällä tai käyttäjäryhmällä on mahdollisuus toimia aktiivisena viestittäjänä ja sisällöntuottajana, tiedon vastaanottamisen lisäksi (Vesterinen & Suutarinen 2011, 28).

Riskillä tarkoitetaan haitallisen tapahtuman todennäköisyyttä ja vakavuutta (Työsuojeluhallinto 2014). Lähes kaikki riskit ovat ihmisten aiheuttamia, jonka takia niihin voidaan vaikuttaa ja varautua ja niiltä voidaan suojautua. Jos riskeihin ei ole osattu, huomattu tai ehditty ajoissa varautua, ne pääsevät yllättämään. Pienetkin häiriöt saattavat käynnistää tapahtumaketjun, joka uhkaa koko yrityksen toimintaa. (Suomen Riskienhallintayhdistys ry.)

Uhalla tarkoitetaan haitallista tapahtumaa, joka voi mahdollisesti toteutua ja aiheuttaa tiedoille, muulle omaisuudelle tai toiminnalle ei-toivottuja asioita (VAHTI 8/2008). Uhat on mahdollista tunnistaa, mutta niihin ei useinkaan pystytä vaikuttamaan (Wimmer 2014).

Verkkorikollisuudella tarkoitetaan rikollista toimintaa, jota tehdään hyödyntäen Internetiä. Verkkorikollisuus voidaan jakaa kolmeen eri kokonaisuuteen: hyökkäykset atk-laitteita ja ohjelmistoja vastaan, esimerkiksi haittaohjelmat ja virukset; taloudelliset rikokset, esimerkiksi tietojen kalastaminen, verkkopetokset ja luvattomat tunkeutumiset yrityksen palvelimelle; väärinkäyttö, esimerkiksi laittoman sisällön lataaminen Internet-sivustolle. Laiton materiaali voi olla esimerkiksi materiaalia, johon jakavalla henkilöllä ei ole tekijänoikeuksia tai materiaalia, joka saattaa täyttää laittoman materiaalin tunnusmerkit. (Interpol.)

Tietoturvallisuudella tarkoitetaan tietojen, palveluiden, järjestelmien ja tietoliikenteen suojaamista ja niihin kohdistuvien riskien minimointia hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietoturvallisuustyön päämäärä on turvata liiketoiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen sekä minimoida aiheutuvat vahingot. (Andreasson & Koivisto 2013, 29.)

4 Sosiaalinen media ja sen suosituimmat palvelut

Sosiaalinen media on muuttanut merkittävästi yritysten nykypäiväistä liiketoimintaa ja ihmisten työskentelytapoja (Niemelä 2012, 53). Se on myös muuttanut paljon ihmisten käyttäytymistä, mahdollistamalla ihmisten välisen vuorovaikutuksen, yhteistyön, päätöksenteon, tiedon jakamisen ja yhteisen tiedon luomisen uusilla, helppokäyttöisillä tavoilla (Otala & Pöysti 2008, 9). Yritykset voivat saada monenlaista rahallista hyötyä toimiessaan sosiaalisessa mediassa. Yritykset voivat muun muassa kasvattaa liikevaihtoa lisäämällä myyntiä, laskea kuluja lisäämällä työn tuottavuutta ja lisätä asiakastyytyväisyyttä (Isokangas & Kankkunen 2011, 84). Sosiaalisen median palvelut eivät ole kuitenkaan pelkkää verkostoitumista ja tiedon jakamista, ne muodostavat myös uudenlaisia tietoturvauhkia sekä yrityksille että yksityishenkilöille (Rinta 2011).

Yrityksille suurimmat sosiaalisen median kipupisteet ovat ajanhallinta, epävarmuus omasta osaamisesta, tietoturva sekä perinteinen ylhäältä alas -johtamistapa (Vesterinen ym. 2011, 29). Sosiaalinen media on tehnyt yrityksen toiminnasta läpinäkyvämpää myös ulospäin. Asiakkaiden ja työntekijöiden kautta yritykset ovat mukana sosiaalisessa mediassa riippumatta siitä, haluavatko ne sitä tai ei. (Isokangas ym. 2011, 7.) Sosiaalisen median palvelut eivät sovellu luottamuksellisten tai salaisten työasioiden jakamiseen edes suljetuissa tai salaisissa työtiloissa. Sen sijaan ne soveltuvat mainiosti aktiiviseen avoimuuteen ja yhteistyön tekemiseen eri kohderyhmien kanssa. (Aalto 2012, 135.)

Hyvänä ratkaisuna sosiaalisen median hoitoon yrityksissä ei ole palkata uusia henkilöitä, jotka vastaavat koko yrityksen sosiaalisen median toimenpiteistä, koska sosiaalinen media ei kuulu ainoastaan viestinnälle, vaan myös markkinoinnille, myynnille, johdolle, tuotekehitykselle – oikeastaan tietyssä määrin koko organisaatiolle. Strategia sosiaalisessa mediassa tulee noudattaa organisaation päästrategiaa, jossa kriisiviestinnällä on keskeinen rooli. Sosiaalinen mediaa varten tarvitaan yrityksessä siis omat pelisäännöt, askelmerkit, vastuut, aikataulut ja tavoitteet. Sosiaalisen median käyttö yrityksissä vaatii myös avoimuutta, ketteryyttä, suoruutta ja nopeutta. (Mainostajien Liitto 2012, 249–251.)

Monet yritykset ja organisaatiot ovat tunnistaneet sosiaalisen median mahdollisuudet liiketoimintaa parantavana palveluna. Samalla sosiaaliseen mediaan liittyvä avoimuus ja siihen mielletyt riskit arveluttavat. (Otala ym. 2008, 13.) Monien yritysten johtajat ovat äärimmäisen huolestuneita työntekijöidensä jakamista asioista sosiaalisessa mediassa (Gaudin 2009). Vaarana on, että yrityksen työntekijät jakavat yrityssalaisuuksia käyttäen sosiaalisen median viestintäkanavia. Yritykselle haitallista voi olla myös työntekijöidensä kommentointi tekemäänsä työhön. Esimerkiksi työntekijä saattaa ajattelematta kirjoittaa kiireisestä päivästä yrityksessä, koska asiakkaat valittavat jatkuvasti saamistaan tuotteista (Gaudin 2009). Tämä ei anna muille kovin hyvää kuvaa yrityksen tuotteiden laadusta. On hyvä muistaa, että tiedot elävät verkossa ikuisesti. Väärät, negatiiviset tai yritystä loukkaavat tiedot on useimmiten mahdollista poistaa verkosta, mutta poistaminen ei välttämättä tuo toivottua tulosta, koska sama materiaali saattaa putkahtaa esiin toisaalla (Isokangas ym. 2011, 86).

Ensimmäinen selkeästi tunnistettava sosiaalisen median palvelu julkaistiin vuonna 1997. Sen nimi oli SixDegrees.com ja se muistutti paljon nykyistä supersuosittua Facebookia. Sivusto suljettiin vuonna 2000, koska se oli perustajien mukaan liikaa aikaansa edellä. Nykymuotoisen sosiaalisen median katsotaan saaneen alkunsa vuonna 2007. (Niemelä 2012, 56.)

Tilastokeskuksen mukaan sosiaalista mediaa käyttää aktiivisesti 49 prosenttia suomalaista (Laaksonen, Matikainen & Tikka 2013, 10).

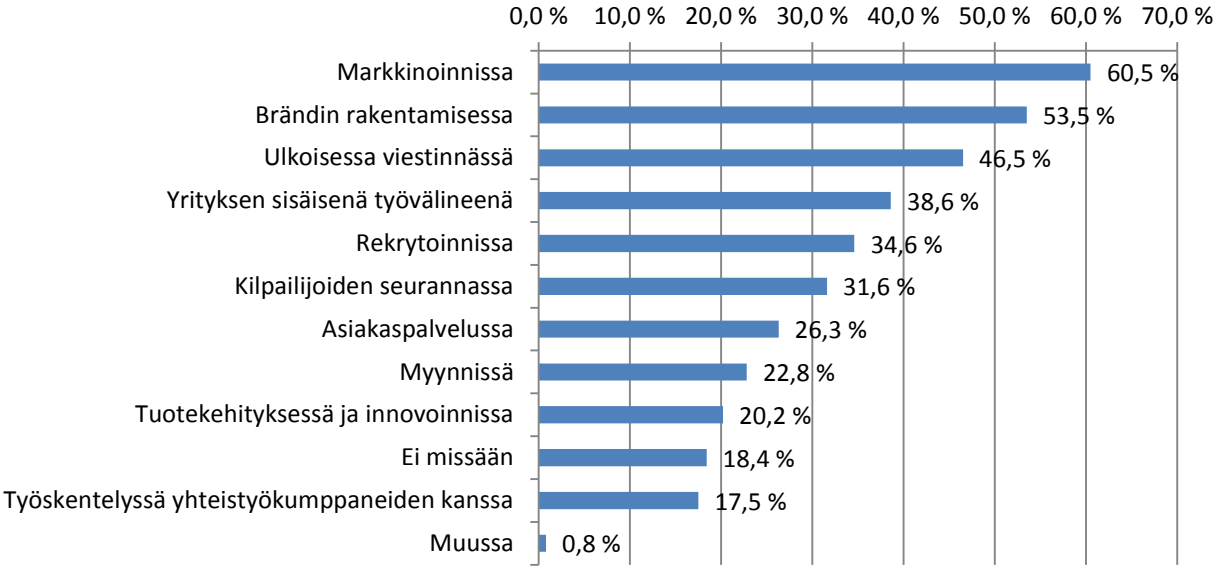
Businessinsider julkaisi vuoden 2011 lopulla tilastot Internetin käytöstä maailmalla ja siitä, mitä siellä tapahtuu 60 sekunnin aikana. Luvuista käy ilmi sosiaalisen median suosio. Facebookissa tehdään minuutissa 695 000 tilapäivitystä, 79 364 seinäpostausta ja 510 040 kommenttia. Twitteristä lähetetään minuutissa yli 98 000 tviittiä ja sinne rekisteröityy yli 320 uutta käyttäjää. LinkedIn-palveluun rekisteröityy yli 100 uutta käyttäjää ja YouTubeen ladataan yli 600 uutta videota, joiden yhteiskesto on yli 25 tuntia. (Andreasson ym. 2013, 152.) Seuraavaksi tässä kappaleessa kerrotaan, mitä sosiaalinen media käytännössä tarkoittaa, minkälaiset tahot sitä käyttävät ja miten sitä hyödynnetään yritysmaailmassa.

4.1 Sosiaalinen media käsitteenä

Sosiaalinen media käsitteellä viitataan median ja Internetin kehitysvaiheeseen, jossa sisällöntuotanto hajautuu ja käyttäjät tuottavat yhä enemmän sisältöä. Samasta ilmiöstä käytetään myös muita nimityksiä. Näitä ovat esimerkiksi sosiaalinen web, web 2.0, vertaisverkko, vertaismedia, yhteisöllinen media ja some. Kyseisistä nimityksistä, sosiaalinen media on juurtunut kaikesta vahvimmin kielenkäyttöön. (Karppinen & Matikainen 2012, 135.)

Luultavasti syynä miksi sosiaalinen media on kaikesta juurtunein ilmaisu, johtuu sanaparista ”sosiaalinen” ja ”media”. ”Sosiaalinen” tarkoittaa jakamista (tiedostojen, mielipiteiden ja niin edelleen) ja ”media” tarkoittaa digitaalisia julkaisupaikkoja. (Cavazza 2008.) Juuri näistä asioista sosiaalisen median palveluissa on kyse.

Sosiaalisen median palveluita käyttävät kaikenlaiset tahot. Sen palveluita käyttävät yritykset, julkishallinnon organisaatiot, viranomaiset, yliopistot ja muut koulut sekä yksityiset henkilöt (Andreasson ym. 2013, 151). Yrityksille sosiaalinen media voi toimia viestintäkanavana, mainonnan- ja myynnin apuvälineenä sekä asiakastietokanavana. EVA:n raporttiin suoritetun tutkimuksen mukaan suomalaiset yritykset hyödynsivät sosiaalista mediaa seuraavasti vuonna 2011:



Taulukko 1 Sosiaalisen median hyödyntäminen yrityksissä vuonna 2011 (mukaillen Isokangas ym. 2011, 47).

Suomalaiset yritykset käyttävät toistaiseksi sosiaalista mediaa paljon hyväkseen markkinoinnissa ja ulkoisessa viestinnässä. Useimmat yritykset kuitenkin uskovat, että tulevaisuudessa yritysten sisäinen viestintä lisääntyy. (Isokangas ym. 2011, 68.) Tosin läheskään kaikki suomalaiset yritykset eivät ole vielä löytäneet sosiaalista mediaa tai nähneet sitä tarpeelliseksi heidän yritystoimintaa ajatellen. Tilastokeskuksen (2014) mukaan 43 prosenttia Suomalaisista yrityksistä käyttää sosiaalista mediaa jollain tavoin hyväkseen liiketoiminnassa. Informaation ja viestinnän toimialoilla sosiaalista mediaa käytetään kaikkein eniten (85 prosenttia yrityksistä). Rakentamisen sekä kuljetuksen ja varastoinnin toimialoilla sosiaalisen median käyttö on vähäisintä. Rakentamisen toimialojen sosiaalisen median käyttö on 15 prosenttia. Kuljetuksen ja varastoinnin aloilla käyttö on puolestaan 24 prosenttia. (Tilastokeskus 2014.)

Sosiaalisen median tunnetuin kanava suomessa on Facebook. Siitä on tullut osittain sähköpostin ja tekstiviestien korvaava työkalu. Facebook ei ole kuitenkaan kaikkialla maailmassa suosituin sosiaalisen median palvelu. Esimerkiksi Kiina on luonut oman sosiaalisen mediansa QQ:n, jossa on yli 600 miljoonaa käyttäjää. (Tuominen 2013, 16–17.)

Venäjällä, Ukrainassa, Valko-Venäjällä ja Kazakstanissa vain harvat käyttävät Facebookia. Näissä maissa suosituin sosiaalisen median palvelu on Vkontakte, jolla on yli sata miljoonaa käyttäjää. (Tuominen 2013, 16–17.) Muita maailmalla suosittuja sosiaalisen median palveluita ovat muun muassa blogit ja Wikipedia (Karppinen ym. 2012, 135).

Sosiaalinen media on käsitteenä melko ongelmallinen, koska on melko hankala hahmottaa missä kulkee sosiaalisen median raja. Katri Lietsala ja Esa Sirkkunen ovat pohtineet sosiaalisen median käsitystä ja jakaneet käsitteen kuuteen eri kategoriaan:

Sisällön luominen ja julkaiseminen	**Sisällön jakaminen**	**Verkostoitumis- tai yhteisöpalvelut**	**Yhteistuotanto**	**Virtuaalimaailmat**	**Liitännäiset**
blogit, wikit ja podcasting	esimerkiksi kirjanmerkkien (del.icio.us), kuvien (Flickr) tai videoiden (YouTube) jakaminen	Facebook, LinkedIn, MySpace, IRC-Galleria	Wikipedia, OhmyNews, StarWreck	Habbo, Second Life	Palvelu jota voidaan hyödyntää toisessa palvelussa, esimerkiksi Googlen kartat

Taulukko 2 Sosiaalinen media käsite jaettuna kuuteen kategoriaan (mukaillen Karppinen ym. 2012, 136).

Sosiaalisen median määrittämisessä ongelmia tuottavat sanaparin molemmat osat, niin sosiaalinen kuin mediakin. Voidaankin kysyä, onko kaikki muu media sitten epäsosiaalista? Sosiaalisella medialla ei tarkoiteta tätä, vaan halutaan korostaa toiminnan entistä sosiaalisempaa luonnetta. Lisäksi voidaan kysyä, mikä sosiaalisessa mediassa on mediaa ja mikä ei? Sosiaalinen media on käsitteenä vasta muutamia vuosia vanha ja sitä käytetään kuvaamaan erilaisia verkkopalveluita ja ympäristöjä. Käsite ei ole syntynyt tieteellisestä keskustelusta, vaan se on sanapari, jota käytetään verkkoympäristöjen kuvaamisessa ja nimeämisessä. (Karppinen ym. 2012, 137.)

4.2 Sosiaalisen median palvelut

Internet on pullollaan erilaisia ja eri käyttötarkoituksiin luotuja sosiaalisen median sivustoja ja palveluita. Tästä huolimatta vain muutamalla sosiaalisen median palvelulla on satoja miljoonia päivittäisiä käyttäjiä. Tämän selittää se, että useat sosiaalisen median palvelut ovat tehty vain tiettyä käyttötarkoitusta varten (Forsgård & Frey 2010, 30). Yhdysvaltalainen sosiaalisen median ja viestinnän asiantuntija Brian Solis ja digitaalisen median suunnittelutoimisto ovat keränneet luonteeltaan erityyppiset sosiaalisen median palvelut yhteen (Forsgård ym. 2010, 30).

Kuva 1 Sosiaalisen median palvelut (Solis & JESS3).

Kuvasta käy ilmi sosiaalisen median palveluiden laajuus. Harva tuskin on kuullut kaikista kuvassa näkyvistä palveluista. Tärkeintä on kuitenkin ymmärtää palveluiden laajuus ja monimuotoisuus. Oli aihe, tarpeet tai käyttötarkoitus mikä hyvänsä, verkosta todennäköisesti löytyy siihen erikoistunut palvelu. (Forsgård ym. 2010, 30.)

Tutkimusten mukaan henkilöiden iällä on vaikutusta sosiaalisen median käyttöön. Vuoden 2013 syksyllä yli 50-vuotiailla blogien lukeminen sekä verkostopalvelujen ja keskustelufoorumien käyttäminen oli paljon vähäisempää verrattuna nuorempaan sukupolveen. (Suominen, Östman, Saarikoski & Turtiainen 2013, 11.)

Tässä opinnäytetyössä käydään seuraavaksi läpi muutamia sosiaalisen median suosituimpia palveluita. Kappaleessa kerrotaan historiaa siitä, miten kaikki alkoi, sekä paljonko rekisteröityneitä käyttäjiä palvelut ovat keränneet. Seuraavaksi käydään läpi myös asioita, joiden ansiosta juuri kyseiset palvelut nousivat suureen suosioon. Tässä opinnäytetyössä tutkitaan myöhemmässä vaiheessa erilaisia riskitekijöitä, seuraavaksi mainittuja sosiaalisen median palveluita käyttäen.

4.2.1 Facebook

Facebook, kuten moni muukin Internetin menestystarina sai alkunsa puolivahingossa. Alun perin sitä ei ollut suunnisteltu kansainväliseksi verkostoksi, vaan pienen kaveriporukan yhteydenpitovälineeksi. Mark Zuckerberg perusti Facebookin vuonna 2004 Dustin Moskovitzin ja Chris Hugheisin kanssa. Palvelun oli tarkoitus mahdollistaa kolmikon yhteydenpidon Harvardin yliopiston vanhoihin opiskelukavereihin. Aluksi Facebook levisi nopeasti Harvardin yliopiston sisällä, ja pian siihen tuli mukaan Yalen ja Stanfordin yliopiston opiskelijoita. Muutamassa kuukaudessa palvelusta oli tullut tunnettu käsite amerikkalaisten yliopisto-opiskelijoiden keskuudessa. (Haasio 2009, 12–13.)

Ensimmäisen toimintavuoden loputtua Facebookilla oli jo miltei miljoona käyttäjää. Vuotta myöhemmin palveluun oli rekisteröitynyt 5,5 miljoonaa henkilöä. Tämän seurauksena Zuckerberg ja Moskovitz keskeyttivät opintonsa vuonna 2005 ja ryhtyivät tekemään töitä Facebookin kehittämiseksi. (Haasio 2009, 12–13.) Facebook oli aluksi suljettu yhteisö, joka oli tarkoitettu vain opiskelijoille. Vuonna 2006 sitä laajennettiin niin, että eri työyhteisöt pääsivät mukaan palveluun. Melko pian tämän jälkeen palvelu avattiin kaikille halukkaille. Suomessa palvelua alettiin laajemmin käyttää vuonna 2007. Facebookista tuli Suomessa suuri ilmiö, sen julkaistessa palvelustaan ensimmäisen suomenkielisten version vuonna 2008. (Haasio 2009, 12–13.)

Yle Uutisten keräämien tietojen mukaan suomalaisia oli rekisteröitynyt Facebookiin maaliskuussa 2013 yhteensä 2,1 miljoonaa henkilöä (Suominen ym. 2013, 11). Joulukuussa 2013 Facebookilla oli noin 1,2 miljardia käyttäjää maailmanlaajuisesti, joista eniten käyttäjiä oli Yhdysvalloissa, Intiassa ja Brasiliassa (Limnéll, Majewski & Salminen 2014, 235).

4.2.2 Twitter

Twitter perustettiin 19.4.2007 (Twitter 2014). Twitter sai alkunsa Noah Glassin suunnittelemalle palvelulle. Palvelu toimi periaatteella, jossa käyttäjä soittaa palvelun puhelinnumeroon ja jättää ääniviestin. Ääniviestin annettua, palvelu tallentaa sen MP3-muotoisena Internetiin. Tämän teknologian myötä Noah perusti yrityksen nimeltä Odeo. Odeon ensimmäisiä sijoittajia oli entinen Googlen työntekijä nimeltään Evan Williams ja the Charles River Ventures yhtiökumppani George Zachary. Evan Williams osallistui Odeon toimintaan enemmän kuin yksikään muu yhtiöön sijoittanut henkilö. (Carlson 2011.)

Odeo toimi alun perin Noah Glassin asunnossa, josta se siirtyi myöhemmin Evan Williamsin vanhaan asuntoon. Evan lahjoitti vanhan asuntonsa Odeon käyttöön, koska hän oli ostanut itselleen uuden asunnon. Hetkeä myöhemmin Odeo siirsi yrityksensä toimistorakennukseen ja rekrytoi palvelukseen lisää työntekijöitä, kuten Web-suunnittelija Jack Dorseyn. Syksyllä 2005 Apple julkaisi uutisen, että iTunes tulee tukemaan tilauspohjaisten äänitietojen sovellusalustaa ja se tulee käyttöön jokaiseen Applen myymään iPod -laitteeseen. George Zacharyn kuultua uutisen, oli hän sitä mieltä, että Odeo ei menesty nykyisellä yritysideallaan. Hetkeä myöhemmin Evan Williams päätti, että Odeon tulevaisuus ei ole tilauspohjaisten äänitiedostojen julkaisua verkossa. Evan käski yrityksen työntekijöitä suunnittelemaan uutta suuntaa Odeonille. Yhtiön suunnitellessa uutta suuntaa, Jack Dorsey keksi idean uudelle palvelulle. Se oli palvelu, jota käyttämällä tietäisi mitä kaverit parhaillaan tekevät. Helmikuussa 2006 Dorseyn idea esiteltiin Odeon jokaiselle työntekijälle. Kyseessä oli palvelu, joka jakoi käyttäjän puhelimitse lähetetyn viestin kaikille hänen ystävilleen. Noah Glass keksi palvelulle nimeksi ”Twttr”. Myöhemmin palvelun nimi vaihdettiin sanaksi ”Twitter”. Kaikki Twitterin perustajajäsenet ovat sitä mieltä, että suurin osa Twitterin ideoista tuli Jack Dorseyltä. Ennen kuin dorsey liittyi Odeoon, hän oli jopa piirtänyt jotain, joka näyttää Twitteriltä. (Carlson 2011.)

Alun perin Twitter oli suunniteltu toimimaan SMS-teknologialla, jonka myötä viestien maksimipituus oli 140 merkkiä. Myöhemmin Twitteristä kehitettiin verkossa toimiva sovellus, jossa viestien maksimipituus päätettiin pitää samana kuin aiemmin. Alun perin käyttäjillä ei ollut mahdollista vastata muiden käyttäjien viesteihin. Tällöin osa Twitterin käyttäjistä käytti @ -merkkiä ennen käyttäjänimeä tunnistaakseen käyttäjät toisistaan. Käytänteestä tuli niin suosittu, että se otettiin myöhemmin virallisesti käyttöön Twitterissä. Samalla # –merkistä (kutsutaan usein nimityksillä hashtag tai risuaita) tuli suosittu, ja se on myös otettu virallisesti käyttöön Twitterissä. # –merkkiä käytetään nykyisin Twitterissä keskusteluaiheen tunnisteena. (Kivimäki 2012; MacArthur.) Kyseinen merkki liittää siis yksittäiset Twitter-viestit osaksi tietyistä aiheista käytävää keskustelua (Nurmi 2013).

Twitter alkoi yleistyä suomalaisten käytössä sen jälkeen, kun Yleisradio aloitti hyödyntämään sitä lähettimissään viihdeohjelmissa. Toukokuussa 2010 Yle toi ensimmäistä kertaa twiitit television ruudulle. Joulukuussa 2011 Twitter kipusi monien suomalaisten tietoisuuteen, kun #linnanjuhlat nousi hetkeksi maailman suosituimpien Twitter aiheiden joukkoon, ja tieto siitä levisi Facebookin keskustelupalstoille ja valtamedian nettiuutisiin. (Tuominen 2013, 20.)

Twitterillä on 271 miljoonaa kuukausittaista käyttäjää ja sen käyttäjät lähettävät 500 miljoonaa viestiä (twiittiä) päivässä. 78 prosenttia Twitterin aktiivisista käyttäjästä käyttää palvelua kännykällä. Twitter käyttäjistä 23 prosenttia asuu Yhdysvalloissa. Twitter työllistää yhteensä noin 3 300 henkilöä ympäri maailmaa. (Twitter 2014.) Suomalaisista Twitter – tilin oli luonut arviolta noin 300 000 henkilöä vuoden 2012 alkupuoliskolla (Tuominen 2013, 21).

4.2.3 LinkedIn

LinkedIn on maailman suurin ja suosituin yritysmaailmaan perustuva sosiaalisen median palvelu. Sen perusti Reid Hoffman vuonna 2002. Virallisesti palvelu otettiin käyttöön viides toukokuuta vuonna 2003. Yrityksen toimitusjohtajana toimii Jeff Weiner ja yrityksen johto koostuu kokeneista päälliköistä yrityksistä, kuten: Yahoo!, Google, Microsoft, TiVo, PayPal ja Electronic Arts. LinkedIn palvelulla on maailmassa yhteensä noin 300 miljoonaa käyttäjää yli 200 maassa. (LinkedIn 2014.)

LinkedIn on kuin Facebook, mutta se on tarkoitettu pääasiassa työelämään. Se on Internetpalvelu, joka mahdollistaa yhteydenpidon omiin työkavereihin, asiakkaisiin, yhteistyökumppaneihin ja muihin kontakteihin. Palvelun avulla voi solmia myös uusia suhteita ja pysyä kärryillä oman alan uutisista. LinkedInistä voi saada myös työtarjouksia, mikäli oma profiili on ajan tasalla ja kiinnostava. (Koistinen 2013.)

Suomessa LinkedIn palveluun rekisteröityjä käyttäjiä oli vuoden 2014 alkupuoliskolla 595 202 eli noin 11 % koko suomen väestöstä. Suomessa sukupuolensa ilmoittaneiden LinkedIn -palvelun käyttäjistä 180 479 on naisia ja 169 840 on miehiä. Naisten keskuudessa palvelua käyttää suurimmaksi osaksi 18–54-vuotiaat ja miesten osalta yli 34-vuotiaat. (Tuominen 2014.)

4.2.4 YouTube

YouTube on maailman suosituin Internetissä toimiva videopalvelu. Sivustolla videoita katsellaan 4 miljardia tuntia joka kuukausi, ja uusia videoita palveluun ladataan 72 tuntia joka minuutti. YouTuben ansiosta esimerkiksi Justin Bieber ja Korealainen popsensaatio Psy nousivat maailman suosioon ennätysajassa. (Dickey 2013.)

YouTube videopalvelun perusti vuonna 2005 entiset PayPal työntekijät Chad Hurley, Steve Chen ja Jawed Karim. Idea YouTuben perustamisesta syntyi illalliskutsulla San Franciscossa noin vuosi ennen palvelun perustamista. (Dickey 2013.) Lokakuussa vuonna 2006 Google osti palvelun itselleen 1,29 miljardilla eurolla, ja siitä lähtien palvelu on ollut Googlen omistuksessa (It-viikko 2006).

YouTube antaa miljardeille ihmisille mahdollisuuden etsiä, katsoa ja jakaa käyttäjien itse luomia videoita. Lisäksi se tarjoaa käyttäjille mahdollisuuden ottaa toisiinsa yhteyttä, jakaa tietoa ja inspiroida muita käyttäjiä ympäri maailmaa. Palvelu tarjoaa myös jakeluympäristön alkuperäisen sisällön luojalle sekä pienille ja suurille mainostajille. (YouTube 2014.)

4.2.5 Keskustelufoorumit

Keskustelufoorumi on verkossa käytävälle keskustelulle tarkoitettu sivusto, jossa rekisteröityneet käyttäjät voivat keskustella, kommentoida tai kysyä heitä askarruttavista aiheista. Foorumit mahdollistavat viestien lukemisen, uusien aiheiden aloittamisen ja viesteihin vastaamisen. Foorumien aiheet voivat olla avoimia tai vain muutamia aiheita koskevia. Foorumin luojalla on niin sanotut administratorin eli ylläpitäjän oikeudet. Tämä tarkoittaa sitä, että kyseinen käyttäjä voi muokata tai poistaa foorumin aiheita. Hänellä on myös oikeudet poistaa käyttäjien viestejä tai käyttäjiä, mikäli sivuston sääntöjä rikotaan tai käyttäydytään muuten asiattomasti. Foorumin luoja voi antaa myös muille käyttäjille erikoisoikeuksia, jos hänellä ei ole esimerkiksi aikaa seurata keskustelua riittävän tarkasti. (WiseGEEK 2014.)

Nicolas Ternisien (2010) mukaan maailman ensimmäisen foorumin Internetiin perusti Ari Luotonen vuonna 1994. Kyseinen foorumi käytti W3 Interactive Talk (WIT) ohjelmaa, joka oli suunniteltu ryhmän päätöksenteon tarkastelemiseen. (Ternisien 2010.) Keskustelufoorumit toimivat eräänlaisina esisosiaalisena mediana (Suominen ym. 2013, 41).

Suomen suurin ja aktiivisin keskustelufoorumi on Suomi24. Suomi24 verkkoyhteisöä käyttää 1,3 miljoonaa suomalaista viikossa ja sinne lähetetään tuhansia uusia viestejä päivässä. (Sivustot.info 2012; Suomi24 2014.)

5 Sananvapaus

Tässä kappaleessa selvennetään käsitettä sananvapaus. Kappaleessa kerrotaan, mitä sananvapaus todella tarkoittaa ja mitkä asiat kuuluvat sananvapauden piiriin. Kappaleessa otetaan myös kantaa yritysmaailmassa vallitsevista sananvapaus käsitteistä ja kerrotaan, mitä asioita yritysten ja työntekijöiden on syytä ottaa huomioon viestittäessään yrityksen nimissä.

5.1 Käsitteenä

Perustuslain mukaan jokaisella henkilöllä on sananvapaus. Sananvapauteen kuuluu oikeus ilmaista, julkistaa ja vastaanottaa tietoja, mielipiteitä ja muita viestejä kenenkään sitä ennalta estämättä. (Aalto & Yoe Uusisaari 2009, 139.)

Sananvapaudella on lähes myyttinen asema nyky-yhteiskunnassa. Sitä pidetään eräänlaisena ideologiana, jonka tulkinnat jäsentävät keskustelua julkisuuden ja demokratian suhteesta sekä viestinnän sääntelyn rajoista. Vaikka kukaan tuskin kiistää sananvapauden merkitystä yhtenä demokratian perusarvoista, itse käsitteen määrittelystä, sen tulkinnasta ja rajoista on vaikeampi päästä yhteisymmärrykseen. Niin juristit, filosofit, poliitikot, journalistit kuin verkkokeskustelijatkin viittaavat useasti sananvapauteen vedoten toistensa ohi. Sananvapaudesta keskusteltaessa ei helposti löydy mitään puhdasoppista ydintä, johon käsitteen sananvapaus voisi tiivistää. Vapaus itsessään on moniulotteinen ihanne, jolle on vaikeaa löytää yksiselitteistä määrittelyä ja se luo aina uusia tulkintakiistoja ja paradokseja. Käsitteet kuten sananvapaus, lehdistönvapaus, viestinnän vapaus ja mediavapaus mielletään usein samaksi asiaksi. (Karppinen ym. 2012, 61–64.)

Karppinen jakaa sananvapaus käsitteen kolmeen eri kategoriaan, joiden jaottelu perustuu lähinnä yhteiskuntafilosofiseen keskusteluun. Nämä käsitteet ovat negatiivinen, positiivinen ja radikaalinen vapaus. Negatiivisella vapaudella tarkoitetaan ulkoisten rajausten puuttumista eli vapautta jostakin. Negatiivisen sananvapauden ihanne on usein yhdistetty sensuuriin ja muun valtion sääntelyn vastustamiseen. Positiivisella vapaudella tarkoitetaan vapautta johonkin eli sitä, minkälaisia mahdollisuuksia ihmisillä on vapauksien käyttämiseen. Positiivisesta vapauskäsityksestä puhutaan siis silloin, kun halutaan korostaa kansalaisten oikeuksia, kuten tasa-arvoisia mahdollisuuksia saada tietoa ja osallistua julkiseen keskusteluun. Radikaalinen vapaus perustuu ihanteisiin ja käsityksiin vapaudesta kiisteltynä tavoitteena, joka hahmottuu suhteessa erilaisiin yhteiskunnallisiin valtasuhteisiin toteutumatta ikinä täydellisesti. (Karppinen ym. 2012, 62.)

Internetissä yksilöllä uskotaan olevan vapaus ilmaista mielipiteensä ja tuomaan esiin poikkeavatkin mielipiteet. Tätä on jo ehditty juhlimaan suurena sananvapauden menestyksenä. Internetin ja sosiaalisen median tuomat vaikutukset tiedon saatavuuteen ja nopeaan liikkuvuuteen ovat kuitenkin herättäneet valtionhallinnon ja yritykset rajoittamaan yksilöiden ilmaisunvapautta. Sosiaalisen median aikakaudella yritysten huoli liiketoimintasalaisuuksien vuotamisesta julkisuuteen ja kollegoihin kohdistuvista vihapuheista on kasvanut. (Limnéll ym. 2014, 97–98.)

5.2 Sosiaalinen media ja yritysmaailma

Työlainsäädännön mukaan työaika on käytettävä työntekoon, ja tämän takia työnantaja voi kieltää sosiaalisen median käytön työaikana kokonaan, myös tauoilla, jos työntekijä käyttää työnantajan tietoverkkoa. (Jarmas.) Tapscottin mielestä sosiaalisen median kieltäminen osoittaa suuria ikäluokkia edustavien työnantajien ymmärtämättömyyden. Hän muistuttaa, että jopa sähköpostin ja Internetin käyttö oli aikoinaan kielletty osassa työpaikoista. Sähköpostia pidettiin aikoinaan täysin tuottamattomana välineenä, ja Internetin käytön työnantajat kielsivät, koska he olivat ilmeisesti huolissaan siitä, että työntekijät katselevat aikuisviihde sivustoja työnantajansa tiloissa. (Tapscott 2010, 183.)

Maailmassa on siis paljon muuttunut. Tuskin yksikään yritys estää enää Internetin tai sähköpostin käyttöä työpaikalla. Tästä huolimatta osa suomalaisista yrityksistä kieltää edelleen sen työntekijöitään käyttämästä sosiaalista mediaa työaikana. Näistä yrityksistä osa on estänyt pääsyn kokonaan kyseisiin palveluihin yrityksen omasta verkosta. Tapscottin mielestä sosiaalisia palveluiden käyttöä ei yrityksissä kannata kieltää, vaan käyttää niitä hyödyksi. Hänen mielestään esimerkiksi wikit, blogit, sosiaaliset verkostot ja RSS-syötteet saattavat olla uuden huipputehokkaan työpaikan sydän. (Tapscott 2010, 200.)

Suomessa sosiaalisen median täyskiellot eivät ole yrityksissä kuitenkaan kovin yleisiä. Yhdysvalloissa 90 prosenttia yrityksistä on rajoittanut sosiaalisen median palveluiden käyttöä. (Isokangas ym. 2011, 63.) Jyri Wuorisalon mukaan tietoturvan ja -suojan ylikorostaminen hidastaa ja estää monissa yrityksissä sosiaalisen median käyttöä (Meriranta 2010, 99). F-Securen tutkimusjohtaja Mikko Hyppösen mukaan valtaosa tietoturvasyillä perustelluista sosiaalisen median käyttökielloista ja rajoituksista on huuhaata. Todellinen syy johtuu siitä, että käytön arvellaan vievän tehokasta työaikaa, mutta sitä ei haluta sanoa suoraan. (Isokangas ym. 2011, 63.) Wuorisalon mukaan tietoturvaa ja -suojaa koskevat asiat pitäisi nähdä sosiaalista mediaa koskeviin pelisääntöihin kuuluvana luonnollisena asiana (Meriranta 2010, 100).

Yritysten ja virastojen viestintästrategia täytyy olla tarkasti mietitty silloin, kun sen työntekijä ottaa aktiivisen roolin sosiaalisessa mediassa yrityksen nimissä. Yritysten työntekijöitä sitoo salassapitovelvollisuus ja virkamiehiä virkavelvollisuus. Nämä säädökset määrittävät, mitä työntekijät ja virkamiehet voivat sanoa ja millä tavalla. (Hakola 2014.) Yrityksillä ei ole oikeutta estää sen työntekijöitä käyttämästä sosiaalista mediaa vapaa-aikana. Jokaisella on oikeus sanan- ja ilmaisuvapauteen. Sananvapauteen kuuluu oikeus ilmaista, julkistaa ja vastaanottaa tietoa, mielipiteitä ja muita viestejä kenenkään sitä ennalta estämättä. Tosin jokaista yrityksen työntekijää koskee lojaliteettivelvollisuus. Tämä tarkoittaa, että yrityksen työntekijä ei saa jakaa yritystä vahingoittavaa tietoa muille esimerkiksi Facebookia käyttäen. Lojaliteettivelvollisuuden rikkomistilanteessa työnantajalla on lailliset perusteet purkaa työsuhde,

ja työntekijän on korvattava aiheutuneet vahingot. Työntekijällä on lain suoma oikeus kritisoida työnantajaansa, mutta lojaalivelvollisuuden takia julkisista kirjoituksista ei saa aiheutua työnantajalle haittaa. Haitallista tietoa ei saa jakaa sosiaalisessa mediassa, vaikka kyseiset tiedot perustuisivat todellisiin ja totuudenmukaisiin tapahtumiin. Sosiaalisessa mediassa on siis ainoastaan tiedonvälitystapa muuttunut, mutta työntekijöiden velvollisuudet työnantajaansa kohtaan eivät. (Hannula, Morad, Järvinen, Nikkilä & Lievonen.)

Verkkoviestintä kuuluu siis sananvapauslain soveltamispiiriin. Sananvapauslaki koskee sosiaalisessa mediassa informaatiota, joka on julkisesti jaettu ja johon kuka tahansa pääsee käsiksi. Sosiaalisessa mediassa esitettyjen tietojen lähdettä ei kirjoittajan tarvitse paljastaa, mikäli ei sitä itse halua. Tiedonvälityksen turvaksi on luotu uutislähteiden suoja, joka suojaa myös niin sanottua tavallista viestin laatijaa. (Pesonen 2013, 117–120.)

6 Sosiaalisen median sääntely

Sosiaalisen median tuoma avoimuus ja kontrolloimattomuus ovat aiheuttaneet paljon epäselvyyttä perinteisessä julkisen keskustelun muodossa. Erilaisia strategioita ja ohjeistuksia on tehty lukuisia eri toimijoiden johdosta. Esimerkiksi virkamiehille valmisteltiin pitkään ohjeita, mutta selkeiden ohjeiden antaminen osoittautui liian vaikeaksi ja lopulta päädyttiin ”Sosiaalisen median mahdollisuudet hallinnolle” -nimiseen asiakirjaan. Ohjeistuksen sijaan dokumentissa esitellään sosiaalisen median positiivisia vaikutuksia hallinnolle. Sääntelyn näkökulmasta suurinta huomiota ovat herättäneet julkiset verkkokeskustelut. Keinot puuttua lain rajoissa tapahtuvalle verkkokeskustelulle ovat vähäiset, vaikka keskustelun luonne olisi arveluttava. Toisinaan on vaadittu, että verkkokeskustelu käytäisiin aina omalla nimellä. Vaatimukset oman nimen käytöstä ovat kuitenkin epärealistiset, koska ”oma nimi” voi verkossa olla mikä tahansa. Pelkän nimimerkin käyttö saattaa globaalisti ajateltuna olla hyvin tärkeä asia. Muun muassa diktatorisissa yhteiskunnissa nimettömyys saattaa olla elinehto. Toisaalta vaatimukset oman nimen käytöstä ovat perusteltuja, koska verkkokeskusteluissa niin julkisuuden henkilö kuin yrityskin voi joutua helpoiksi maalitauluiksi. Tällöin keskusteluasetelma ei ole kovin tasapuolinen. (Karppinen ym. 2012, 152–153.)

Julkisen sanan neuvosto päätti syksyllä vuonna 2011 lisätä Journalistin ohjeisiin liitteen koskien yleisön tuottamaa materiaalia tiedotusvälineiden sivuilla. Ohjeissa kehotetaan seuraamaan ja poistamaan ihmisarvoa tai yksityisyyttä loukkaavat sisällöt. Ohjeessa mainitut asiat ovat vain suosituksia ja koskevat vain tiedotusvälineiden sivuja. Näin ollen suuri osa verkkokeskusteluista jää suositusten ulkopuolelle. Suomen lainsäädännössä ei ole nimenomaisia säännöksiä sosiaaliseen mediaan liittyen. (Koivumäki & Häkkänen 2012, 162.)

Tosin kaikkia verkkokeskusteluja säätelee lainsäädäntö, joka sisältää säännökset muun muassa kunnianloukkauksista, julkisesta kehottamisesta rikokseen, laittomasta uhkauksesta, kiihottamisesta kansanryhmään vastaan, uskonrauhan rikkomisesta ja yksityiselämää loukkaavan tiedon levittämisestä (Karppinen ym. 2012, 153–154).

Sosiaalisen median markkinointiin sovelletaan Suomen lainsäädännön laista markkinoinnin tunnistavuusvaatimusta, hintojen merkitsemistä ja markkinointiarpajaisten sekä kylkiäisten sääntöjä (Koivumäki ym. 2012). Suomessa yritysten keskuudessa suosituiksi tulleet markkinointiarpajaiset kuuluvat samalla tavalla Suomen lainsäädännön piiriin. Niitä sitoo muun muassa kuluttajansuojalaki, henkilötietolaki ja tekijänoikeuslaki. Lainsäädännön lisäksi kampanjoissa on noudatettava palveluntarjoajan omia sääntöjä ja ohjeita, jotka voivat poiketa merkittävästi kotimaan lainsäädännöistä. (Koivumäki & Häkkänen 2013, 96.)

Facebookissa on sääntöjenvastaista järjestää arvontoja, jossa osallistumisen ehdoksi on asetettu statuspäivityksen julkaiseminen, kuvan jakaminen, profiilikuvan muuttaminen tai muu vastaava toiminto. Sen sijaan kampanjaan osallistumiseksi voidaan edellyttää sivusta tykkäämistä, paikkaan kirjautumista tai sovellukseen rekisteröitymistä. Pelkkä sivusta tykkääminen ei kuitenkaan riitä, vaan tykkäämisen jälkeen täytyy esimerkiksi täyttää arvontalomake, jotta kampanja täyttää Facebookin asettamat säädökset. Facebook myös kieltää voitosta ilmoittamisen Facebookin kautta. Lisäksi kampanjan säännöissä tulee aina kertoa selvästi, ettei se ole Facebookin järjestämä, tukema tai sponsoroima. (Tuominen 2013, 48.)

7 Sosiaalinen median tuomat ongelmat ja niiden ehkäisy yritysmaailmassa

Tässä kappaleessa kerrotaan, minkälaisia ongelmia sosiaalinen media nostattaa sen käyttäjissä. Kappaleessa tarkastellaan sosiaalisen median mahdollisia vaikutuksia työelämää silmälläpitäen. Lisäksi tähän kappaleeseen on kerätty käytännön ohjeita, jotta toimiminen sosiaalisessa mediassa olisi yrityksille ja sen työntekijöille turvallisempaa ja tehokkaampaa.

7.1 Sosiaalisen median ongelmia yritysmaailmassa

Useampi kuin joka neljäs on ladannut sosiaalisen median sivustolle kuvan tai kommentin, jonka he pelkäävät koituvan kohtalokseen työelämässä. Thomson Reutersin omistama lainopillinen verkkosivu FindLaw.com teki kyselyn vuonna 2013, joka oli osoitettu sosiaalisen median käyttäjille. Kyselyyn vastasi tuhat 18–34-vuotiasta amerikkalaista. 29 prosenttia kyselyyn vastanneista pelkäsi, että heidän lataamansa kuva tai kommentti vähentäisi heidän

mahdollisuuksiaan saada hakemaansa työtä tai jonka nähdessään nykyinen työnantaja päättäisi heidän työsopimuksensa. 21 prosenttia vastanneista kertoi, että juuri tästä syystä he olivat poistaneet lataamansa kuvan tai kommentin. 82 prosenttia vastanneista oli rajoittanut ainakin jossakin määrin kommenttien ja kuvien näkyvyyttä. (Myllyoja 2013.)

Moni sosiaalisen median palvelun käyttäjä on menettänyt hakemansa työnsä juuri sosiaalisen median takia. Vuonna 2009 henkilöstövuokrausyritys Execunet ilmoitti, että 35 prosenttia potentiaalisista työntekijöistä eivät saaneet heiltä työtä johtuen tiedoista, joita yritys löysi kyseisten henkiöiden sosiaalisen median profiileista. (Cooke 2011, 66.) Microsoftin teettämän tutkimuksen mukaan kahdeksan kymmenestä työnantajasta selvittää hakijoiden verkkomaineen Yhdysvalloissa. Euroopassa verkkomaineen selvittäminen on toistaiseksi vähemmän yleistä. Ruotsissa neljä kymmenestä työnantajasta selvittää työnhakijan sosiaalisen profiilin ja Saksassa vähän yli puolet työnantajista myöntää hankkivansa tietoja hakijasta Internetin välityksellä. (Tranberg & Heuer 2013, 62.) Suomessa työntekijästä ei lain mukaan saa hakea tietoa verkosta ilman työnhakijan lupaa (Isokangas ym. 2011, 56).

Vääränlainen käyttäytyminen sosiaalisessa mediassa voi tietää myös potkuja nykyisestä työpaikasta. Esimerkiksi tarjoilija Pohjois-Carolinasta teki tilapäivityksen, jossa hän valitti joutuvansa olemaan töissä tunnin kauemmin hitaasti syövän pariskunnan takia. Hän myös valitti samassa päivityksessä saavansa vain viisi dollaria tippiä kyseiseltä pariskunnalta. Tilapäivityksen johdosta hänen pomonsa irtisanoi kyseisen tarjoilijan, koska hän oli saattanut yrityksen huonoon valoon ja halventanut yrityksen asiakkaita. (Cooke 2011, 66.)

Niin Suomessa, kuin muuallakin maailmassa yritysjohtajat osallistuvat hyvin vähän sosiaaliseen mediaan (Isokangas ym. 2011, 45). Amerikkalaisen Buy.com-yrityksen toimitusjohtaja Brian J. Dunn uskoo, että yritysjohtajat eivät uskalla käyttää sosiaalista mediaa, koska he sietävät huonosti kritiikkiä. Hänen mukaansa sosiaaliseen mediaan ei mennä vain silloin, kun kaikki on hyvin. ”Siellä ollaan sateessa ja paisteessa”. Dunn tietää varsin hyvin sosiaalisen median sadepäivän, sillä eräänä yönä hänen Twitter-tili oli hakkeroitu. Hakkerin päästyä Donnin tilille, hän lähetti erektiopillerimainoksen Dunnin nimissään. (Tuominen 2013, 21–22.)

Yritysmaailmassa kannattaa harkita tarkkaan, ketä lisää kaverikseen sosiaalisessa mediassa. Esimerkiksi esimiesasemassa olevan henkilön kannattaa pohtia, kutsuuko alaisiaan kavereikseen sosiaalisessa mediassa. Samoin alaisten on hyvä puntaroida, kutsuuko esimiehen kaverikseen. Mikäli alainen käyttää sosiaalista mediaa vain yksityistä käyttöä varten, tilanteesta saattaa tulla kiusallinen. (Aalto ym. 2009, 97.) On myös hyvä miettiä, miltä esimiehen ja alaisen välinen yhteys näyttää muiden silmissä (Forsgård ym. 2010, 100). Näiden asioiden lisäksi kannattaa harkita, lisääkö kavereikseen asiakkaita ja työkavereita (Järvinen 2012, 310).

7.2 Sosiaalisen median käytännön ohjeita yrityksille ja sen työntekijöille

Vaikka sosiaalisen median palvelut ovat olleet olemassa jo useamman vuoden ajan, kuuluu palveluiden käyttäjäkuntaan edelleen useita henkilöitä, jotka eivät täysin ymmärrä sen tuomia vaaroja. Tästä syystä tähän opinnäytetyöhön päätettiin kerätä muutamia käytännön ohjeita, jotta sosiaalisen median aiheuttamia riskejä pystyttäisiin edes hieman vähentämään yritysten ja työntekijöiden keskuudessa.

Sosiaalisessa mediassa kannattaa aina jakaa vain sellaisia asioita, joita voisi missä tahansa ja kenelle tahansa kertoa. Sosiaalisessa mediassa pätevät samat lait kuin muuallakin. Tämä tarkoittaa, että henkilöstölaki, työlainsäädäntö ja tekijänoikeuslaki koskevat myös jokaista sosiaalisessa mediassa jaettua kirjoitusta, videota tai kuvaa. Näin ollen kommenttien, kuvien tai videoiden jakaminen asioista, joista yrityksen, asiakkaan, työkaverin tai työhön liittyvät asiat käyvät ilmi, on laillista jakaa vain luvan saatua. On myös hyvä muistaa, että käyttäjä toimii yhtiön (epävirallisena) edustajana, jos käyttäjän profiilissa on mainittu yhtiö, jossa hän työskentelee. Tämä on syytä ottaa huomioon varsinkin julkisissa kirjoituksissa ja sivustoista tykättäessä. (Jyväskylän kristillinen opisto 2013.)

Henkilökunnalle on hyvä laatia yleiset sosiaalisen median käytön ohjeet, vaikka yritys ei itse toimisi siellä (Pesonen 2012, 206). Organisaation on hyvä järjestää tietoturvakoulutuksia ja niihin on hyvä saada koko henkilökunta osallistumaan. Jos käyttäjä epäilee, että hän on joutunut huijatuksi tai muun hyökkäyksen kohteeksi, kannattaa pyytää apua. Mikäli se täyttää suomen lainsäädännön säädökset, on asiasta hyvä tehdä rikosilmoitus. Sosiaaliseen mediaan ei kannata syöttää liian henkilökohtaista tietoa tai muuta materiaalia. Tämä esimerkiksi siksi, että palvelun tarjoajat voivat hyödyntää profiiliin syötettyjä tietoja laajasti. Yksityisyysasetukset on syytä muuttaa siten, että tiedot eivät leviä laajemmalle kuin omalle käyttäjäjoukolle. Tuntemattomia henkilöitä ei kannata lisätä omaan verkostoon. Työasioista ei kannata keskustella muuta kuin työtehtäviä varten tarkoitetussa ympäristössä, kuten Intranetissä. (Tuominen 2013, 159–160.) Omaa työsähköpostia ei ole suositeltavaa käyttää sosiaalisessa mediassa. (Jyväskylän kristillinen opisto 2013).

Sosiaalisen median palveluissa levitetään roskaposteja ja haittaohjelmia sekä tehdään identiteettivarkauksia. Tämän takia sosiaalisen median käytössä tulee noudattaa samanlaista varovaisuutta kuin muussakin Internetin käytössä. (Suomen Kuntaliitto 2010, 37.) Linkkejä ei kannata avata sosiaalisessa mediassa, varsinkaan jos ne vaikuttavat arveluttavilta tai tulevat tuntemattomalta henkilöltä tai ryhmältä. Salasana sosiaalisen median profiiliin kannattaa pitää

vaikeasti arvattavana. Salasanasta saa turvallisemman ja vaikeammin arvattavan käyttämällä pieniä ja suuria kirjaimia, numeroita ja symboleita. Salasana on myös sitä turvallisempi, mitä pidempi se on. Salasana kannattaa aina pitää ainakin kahdeksan merkkiä pitkänä. (Adrian 2009, 59.)

Tietoturvayhtiö F-Securen mukaan pidemmän salasanan vahvuutta kuvaa hyvin se, että ainoastaan pienistä kirjaimista koostuva viisikirjaiminen salasana voidaan murtaa 19 minuutissa, kun taas yhdeksänkirjaimisen salasanan murtamiseen menee 17 vuotta. Pienistä ja suurista kirjaimista, numeroista ja erikoismerkeistä koostuva yhdeksän merkkisen salasanan murtoon kuluu puolestaan 1,8 miljoonaa vuotta. (Forsgård ym. 2010, 119.)

Sosiaalisen median turvallisuuteen vaikuttavat myös työasemat ja niihin asennetut ohjelmat. Työasemien perusohjelmat, käyttöjärjestelmät ja tietoturvaohjelmat on aina suositeltavaa pitää ajan tasalla. (Adrian 2009, 59.) Omaa profiilia ei kannata pitää julkisena. Sama koskee lähetettyjä tilaviestejä, kuvia ja niin edelleen. Yksityisyysasetuksia muuttamalla voidaan määrittää, ketkä saavat tarkastella esimerkiksi käyttäjän lisäämiä tilapäivityksiä ja kuvia. (Haasio 2013, 52.)

Yrityksen sosiaalisen median sivustoja varten on aina varattava riittävästi osaamista ja aikaa. Sivustoja kannattaa päivittää säännöllisesti ja niiden kautta esitettyihin kysymyksiin ja kommentteihin tulee vastata kuten muuhunkin palautteeseen. Epäasiallinen toiminta sosiaalisessa mediassa saattaa olla haitallista yrityksen maineelle. Sosiaalista mediaa varten yritysten on suositeltavaa nimetä henkilö, joka vastaa sivustojen moderoinnista. (Suomen Kuntaliitto 2010, 37–38.) On kuitenkin hyvä muistaa, että jokainen ihminen ei välttämättä ole hyvä sisällöntuottaja. Lisäksi sisällön luominen on kokopäiväistä työtä, joten useimmiten esimerkiksi markkinointiosaston työntekijöillä ei ole aikaa päivitellä yrityksen sosiaalisen median kanavaa. (Limnéll ym. 2014, 203.) Sosiaalisessa mediassa tapahtuvaa työtä varten on aina hyvä varmistaa sen, mikä on työnantajan tahtotila julkaistavan asian suhteen (Aalto & Yoe Uusisaari 2010, 25). Jokaisen sosiaalista mediaa käyttävän työntekijän onkin hyvä selvittää ja noudattaa oman organisaation sosiaalisen median käyttöpolitiikkaa (Tuominen 2013, 158).

Liikesalaisuudet, asiakkaiden tiedot, hinnoitteluperusteet ja sopimuksen sisällöt eivät yleensä saa joutua julkisuuteen. On myös hyvä sopia, millä tavalla verkossa voi puhua meneillään olevista projekteista, seminaareista, inspiroivista ihmisistä ja asioista, joita on opittu ja keksitty työkavereiden kanssa. (Aalto ym. 2010, 25–26.)

8 Yrityksille tapahtuneet kriisit sosiaalisessa mediassa

Ei tarvita kuin yksi posti tai twiitti pilatakseen yrityksen tai tuotteen maine (Coleman 2013). Yritysten toimintaa protestoivien aktivistien ei enää tarvitse sitoa itseään ketjulla puuhun osoittaakseen mielipiteensä. Nykyään esimerkiksi yrityksen Facebook, YouTube ja Twitter-sivustot mahdollistavat valtaamisen virtuaalisen mielenosoituksen temmellyskentäksi. (Juslén 2010.)

Tässä luvussa käydään läpi muutamia yrityksiä, joille sosiaalisen media on aiheuttanut suuria ongelmia. Kyseiset tapaukset saivat suurta julkisuutta niin perinteisessä mediassa kuin sosiaalisessa mediassakin. Tapaukset vaikuttivat kyseisten yritysten imagoon ja tekevät sitä varmasti edelleenkin, koska tiedot tapauksista ovat edelleen kaikkien nähtävillä verkossa. Tässä kappaleessa käytävät tapaukset on nostettu tähän opinnäytetyöhön varoittavana esimerkkinä sosiaalisen median vaaroista. Samankaltaisia kriisejä on sattunut myös monille muille yrityksille, joista lisätietoa löytyy helposti muun muassa Internetistä.

8.1 Nestlé

Vuonna 2010 ruokajätti Nestlén Facebook sivuista tuli lähinnä yhtiön vastustajien keskustelukanava, kun Greenpeace tiedotti Nestlén makeistuotannon tuhoavan sademetsää. Greenpeace kertoi ruokajätin käyttävän muun muassa Kit Kat makeisissaan palmuöljyä, joka on saatu tuhoamalla orankien asuttamaa sademetsää Indonesiassa. Facebook kirjoittelun lisäksi Greenpeace lisäsi YouTube kanavalleen Nestléä kritisoineen videon, jonka kuitenkin ruokajätti onnistui poistamaan tekijänoikeudellisiin kysymyksiin vedoten. (Pitkänen 2010.) Nestléä kritisoivia videoita lisättiin kuitenkin YouTube-kanavalle, käyttämällä useita eri käyttäjätunnuksia. Tämän takia yritystä kritisoivia videoita on edelleen mahdollista löytää YouTubesta.

Nestlén arvostelu levisi nopeasti yhtiön Facebook sivustolle. Sanallisten kommenttien lisäksi monet Facebook jäsenet vaihtoivat oman profiilikuvansa tilalle muunnellun Nestlé Kit Kat logon, jossa luki ”Nestlé Killer”. Päivää myöhemmin Nestlé ilmoitti poistavansa muunnellut Kit Kat logot sivuilta, koska ne loukkaavat Nestlén tuotemerkkiä. Kyseinen kommentti ei suinkaan vähentänyt yhtiön arvostelua, vaan seuraavaksi keskustelijat alkoivat syyttää yritystä myös sensuurista. Tähän Nestlé vastasi muun muassa ”kiitoksia oppitunnista käytöstavoista…” Päivää myöhemmin Nestlé ilmoitti luopuvansa uusiutumattomista lähteistä hankittavan palmuöljyn käytöstä vuonna 2015. (Pitkänen 2010.)

8.2 Volkswagen

Vuonna 2012 autonvalmistaja Volkswagen toivotti heidän Facebook-sivuillaan kaikille hyvää uutta vuotta ja pyysi samalla ehdotuksia siitä, mitä käyttäjät haluaisivat nähdä yhtiön saavuttavan tulevana vuonna. Hetkeä myöhemmin yrityksen Facebook-sivut täyttyivät muun muassa ympäristöaktivistien kommenteista, joihin yritys ei vaikuttanut suhtautuvan erityisen innokkaasti. (The Huffington Post 2012.)

Kommenteissa otettiin kantaa muun muassa Volkswagenin ympäristöpolitiikkaan. Volkswagen ei ainoastaan vastannut kyseisiin kommentteihin, vaan alkoi myös poistaa negatiivisia kommentteja sivuiltaan. Kommenttien poistaminen aiheutti vihaa kommentin jättäneiden keskuudessa ja pian yritystä alettiin syyttää verkkosensuurista. (The Huffington Post 2012.)

8.3 Red Medicine

Maaliskuussa vuonna 2013 yrityksen pomo turhautui, kun 20 prosenttia pöytävarauksen tehneistä asiakkaista ei koskaan saapunut paikalle. Kyseisenä iltana ravintola oli täyteen varattu, jolloin ravintolaan ei voitu ottaa uusia asiakkaita. Samana iltana ravintolaan olisi kuitenkin tullut asiakkaita ilman pöytävarausta, mutta varausten takia ravintola ei pystynyt ottamaan uusia asiakkaita ravintolaansa. Ravintolalla olisi ollut siis mahdollista tienata noin 20 prosenttiyksikköä enemmän kyseisenä iltana, mikäli nämä 20 prosenttia pöytävarauksen tehneistä olisi saapunut paikalle tai peruuttaneet oman pöytävarauksensa. Tästä turhaantunut yrityksen johtaja päätti julkaista kaikkien varauksen tehneiden asiakkaidensa nimet Twitterissä ja kiittävän heitä ironisesti. Osa ravintola-alalla työskentelevistä kollegoista kehui rohkeaa liikettä, kun taas osa paheksui nimien julkaisua. Red Medicinen johtaja myönsi ABC uutisten haastattelussa, että hän halusi saada keskustelua aikaiseksi ravintola-alaa kauan piinaavasta ongelmasta. (Coleman 2013.)

8.4 Päätelmät

Osa sosiaalisen median kriiseistä voidaan välttää ajattelemalla aina ennen kuvan, videon tai kommentin lisäämistä (Myllyoja 2013). Koska sosiaalinen media on avoin ympäristö, ei kuitenkaan aina ongelmilta voi välttyä. Mahdollisia kriisejä varten on syytä varautua jo ennen niiden syntymistä. Tämä saavutetaan hyvällä kriisinhallinnalla. Tämän lisäksi sosiaalisessa mediassa on osattava keskustella rakentavasti ja nöyrästi.

9 Verkkorikollisuus

Tässä kappaleessa avataan käsitettä verkkorikollisuus ja kerrotaan syitä, miksi rikollisuus on siirtynyt verkkoon. Kappaleessa kerrotaan myös hieman avainlukuja, joita tarkastelemalla selviää verkkorikollisuuden laajuus ja sen kustannukset yhteiskunnalle. Lisäksi kappaleessa selvitetään, minkälaista rikollisuutta esiintyy sosiaalisen median palveluissa.

9.1 Käsitteenä

Verkkorikollisuudella tarkoitetaan tietotekniikkaan ja tietoverkkoihin kohdistuvaa rikollista toimintaa ja tietotekniikkaa sekä tietoverkkoja hyväksi käyttäen tehtyjä rikoksia. Tietotekniikkaan ja tietoverkkoihin kohdistuvaa rikollisuutta ovat esimerkiksi tietomurrot, haittaohjelmien avulla tehdyt tietojen kaappaukset ja erilliset verkkohyökkäykset. Tietotekniikkaa ja tietoverkkoja hyväksi käyttäviä rikoksia voivat olla mitkä tahansa rikokset, joiden tekemisessä on käytetty tietotekniikkaa eri tavoin hyväksi. (Poliisi1.)

9.2 Taustatietoa

Internet on maailmanlaajuinen, mutta lait ja poliisien valtuudet ovat kansallisia. Tämä tekee verkosta erinomaisen alustan rikolliselle toiminnalle. Tilanne muistuttaa vanhoja amerikkalaisia elokuvia, joissa poliisit ajavat takaa rosvoja ja huijareita, mutta joutuvat pysähtymään osavaltion rajalle toimivaltansa loppuessa. Internetissä jokainen maa on osavaltio, joiden rajoja poliisi ei voi ylittää. Ei ole siis ihme, että verkossa rikollinen toiminta lisääntyy. Pienellä vaivalla rikolliset tavoittavat suuren määrän potentiaalisia uhreja, ja kiinnijäämisen riski on pieni. (Järvinen 2012, 22.)
Tietotekniikan ja tietoverkkojen käytön laajenemisen myötä niiden käyttö myös laittoman toiminnan välineenä on lisääntynyt. Verkossa tapahtuvan rikollisen toiminnan taustalla on useimmiten taloudellisen hyödyn saaminen. (Poliisi1.) Verkkorikollisuus aiheuttaa maailmanlaajuisesti arviolta kolmen ja puolen miljardin euron kustannukset vuodessa, josta liiketoiminnan määrä on noin 1,3 miljardia euroa. Pelkästään Amerikassa hakkerit ovat varastaneet yhteensä noin 40 miljoonan henkilön henkilökohtaisia tietoja. (Sandle & Char 2014.)

Virusturvaohjelmia valmistavan Symantecin tekemän kansainvälisen tutkimuksen mukaan jopa 70 prosenttia Internetin käyttäjistä ovat joutuneet verkkorikollisuuden tai haittaohjelman uhriksi (Harala 2012). Microsoftin julkaiseman raportin mukaan vuoden 2013 lopussa maailmalla ja Suomessa putsattujen tietokoneiden määrä nelinkertaistui edelliseen vuosineljännekseen verrattuna. Määrä kävi ilmi pääasiassa Microsoftin tietoturvaohjelmistojen keräämien tietojen pohjalta. Tällainen on muun muassa Windows -käyttöjärjestelmän mukana tuleva Malicious Software Removal Tool. (Takala 2014.)

9.3 Sosiaalisessa mediassa

Sosiaalinen median palvelut ovat täydellisiä paikkoja verkkorikollisille kahdesta eri syystä: erittäin suuri käyttäjäkunta ja suuri luottamus käyttäjien välillä (Qing 2010). Vanhassa sanonnassa kysytään, miksi rikolliset ryöstävät pankkeja. Vastaus tähän sanontaan kuuluu, koska siellä raha on. Samasta syystä monet rikolliset ovat siirtyneet käyttämään sosiaalista mediaa. Sosiaalisen median sivustoilla on satoja miljoonia käyttäjiä, jotka jakavat paljon tietoa niin itsestään kuin muistakin. Tämä tarkoittaa sitä, että rikollisilla on mahdollista kalastaa miljoonien käyttäjien tietoja. Yksi rikollisten eniten käyttämä metodi sosiaalisessa mediassa on nimeltään ”spear phishing” (vapaasti käännettynä ”keihäs kalastaminen”). (Pelgrin 2013.) Metodi perustuu ihmisten luottamukseen toisia ihmisiä tai yrityksiä kohtaan (Rouse 2011).

Kyseistä metodia käyttävät rikolliset keräävät ensin tietoa uhristaan, minkä jälkeen he lähettävät uhrille häntä kiinnostavaa materiaalia, esimerkiksi söpön kuvan. Uhrin avattua hänelle lähetetyn materiaalin, vakoiluohjelma siirtyy uhrin koneelle. Rikolliset käyttävät kyseistä metodia päästääkseen uhrin tietokoneella sijainneihin tiedostoihin käsiksi. Tietoturvayhtiö Symantecin tuottaman tutkimuksen mukaan jopa 43 prosenttia rikollisten hyökkäyksistä sosiaalisen median sivustoille yhdisti vakoiluohjelman käyttö. (Pelgrin 2013.)

Myös keskustelufoorumeita käytetään rikolliseen toimintaan. Keskustelufoorumeita on jo pitkän aikaa käytetty erilaisten ohjelmien ja muiden tekijänoikeudella suojatun materiaalin jakoon. Foorumeilla liikkuvat aineistot voivat täyttää esimerkiksi sananvapausrikosten tunnusmerkistöjä tai loukata tekijänoikeutta. Mikäli yritykseltä löytyy foorumi, jonne kaikilla henkilöillä on pääsy ja oikeudet jakaa sisältöä, on siellä hoidettava moderointia ongelmia välttääkseen. Julkisen sanan neuvosto (JSN) suosittelee verkkokeskustelun seulomista ennen julkaisua. (Pihlajarinne 2012, 25–26,107.)

10 Tietoturvariskit

Suurimmat sosiaalisen median riskit liittyvät tietosuojaan. Sosiaalinen media ja tietosuoja ovat täysin toistensa vastakohdat, koska sosiaalinen media perustuu tiedon jakamiseen ja tietosuoja tiedon piilottamiseen. (Järvinen 2012, 294.)

Tampereen kaupunki jaottelee sosiaalisen median käyttöön liittyvät riskit kolmeen kategoriaan:
1. Riskit, jotka johtuvat sosiaalisen median palveluihin tuotetusta sisällöstä.
2. Riskit, jotka johtuvat verkostoitumisesta ja sosiaalisesta kanssakäymisestä sosiaalisen median palveluissa.
3. Riskit, jotka johtuvat sosiaalisen median palveluiden kautta leviävistä haittaohjelmista, kalasteluyrityksistä sekä roskapostista. (Tampere konsernihallinto 2013.)

Lyhyemmin ilmaistuna sosiaaliseen mediaan liittyy kahdenlaista riski- ja uhkatekijää: käyttäjien omat harkitsemattomat teot, jotka aiheuttavat seuraamuksia, ja käyttäjiin kohdistuneet rikokset tai muut ei-toivotut asiat (Haasio 2013, 50).

Tietotekniikkakirjailija Petteri Järvisen mukaan tietoturvan suurimpia riskejä ovat käyttäjien oma kiire, osaamattomuus ja huolimattomuus. Ihmiset muun muassa unohtavat salasanojaan, keskustelevat vahingossa sivu suunsa ja hukkaavat puhelimiaan. Valtaosa tietoturvaongelmista on tahattomia, joten niistä harvemmin kirjoitellaan mediassa. Suurimman huomion mediassa puolestaan saavat tietovarkaudet ja ulkopuolisten tekemät hyökkäykset. (Järvinen 2012, 19.)

Perinteisiä sosiaalisen median, kuten Facebookin huijaustyyppejä ovat nigerialaiskirjeet, tykkäys-, klikkaus- ja täggäysansat. Pahimmassa tapauksessa huijaus johtaa taloudellisiin seuraamuksiin. (Haasio 2013, 53,55.) F-Securen tietoturvajohtaja Mikko Hyppönen totesi kuitenkin Taloussanomissa 20.8.2009, että sosiaalisen median palveluissa tietoturvauhkat ovat hyvin pieniä. Hänen mukaansa suurin osa yrityksistä on enemmänkin huolissaan työntekijöidensä ajankäytöstä. (Haasio 2009, 69.)

Onko sosiaalinen media siis turvallinen ympäristö yrityksille ja sen työntekijöille? Vastaus tähän kysymykseen löytyy tästä kappaleesta. Kappaleessa tarkastellaan sosiaalisen median tuomia riskejä niin yrityksille, kuin sen työntekijöilleenkin. Kappale on jaoteltu kolmeen pääalueeseen: tietoaineistoon liittyvät riskit, tekniset ja muut uhat.

10.1 Tietoaineistoon liittyvät riskit

Yritysten johdolle sosiaalinen media on aiheuttanut ja aiheuttaa varmasti vielä tulevaisuudessakin paljon erilaisia haasteita. Yksi haasteista on tietoaineiston joutuminen vääriin käsiin. Suurin syy johtuu siitä, että sosiaalisen median palveluita on helppo ja nopea käyttää. Sosiaalisen median sivustot on luotu tiedon jakamista varten, ja tämä saa helposti sitä käyttävät henkilöt jakamaan tietoja myös yrityksistä, joissa he toimivat. Tiedot, joita yrityksen työntekijät saattavat vuotaa joko vahingossa tai tarkoituksella julkisuuteen, voivat olla luottamuksellista tai kiusallista. Viattomanoloisillakin viesteillä (kuten työntekijä on huolissaan lomau-

tuksista tai hän on erittäin kiireinen, koska asiakkaat valittavat heidän tuotteestaan) voi olla haitallisia seurauksia, erityisesti jos viesti leviää sosiaalisessa mediassa henkilöltä toiselle. (Gaudin 2009.) Kansainvälisen tietosuojatyöryhmän raportin mukaan Internetin vaikutuksessa kasvaneella sukupolvella saattaa olla edeltäjistään poikkeava käsitys siitä, minkä katsotaan olevan julkista ja mikä yksityistä, salassa pidettävää tietoa (Hannula ym.).

10.1.1 Käyttäjätunnusvarkaudet

Yrityksen tai sen työntekijän kirjautumistiedot saattavat joutua vääriin käsiin, minkä johdosta kyseisellä toimijalla on täydet valtuudet kyseisille tunnuksille. Hän voi muun muassa muuttaa sisältöä, julkaista materiaalia yrityksen tai työntekijän nimissä, levittää haittaohjelmia ja varastaa henkilötietoja. Luonnollisesti tämä voi aiheuttaa ongelmia yrityksen maineelle ja lisäkustannuksia tilanteen korjaamiseksi. Tämän lisäksi salassa pidettävä materiaali saattaa päätyä ulkopuolisten haltuun vaarantaen tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvät velvoitteet. (Kareinen 2013.)

Viimeaikaisten tutkimusten mukaan käyttäjätunnusvarkaudet koskettavat miljoonia henkilöitä vuodessa, ja jo tapahtuneen ongelman korjaaminen vie usein uhriltaan runsaasti aikaa ja/tai rahaa. Useimmiten käyttäjätunnusvarkauteen liittyviä ongelmia pääsee syntymään heikon tietämyksen takia, siitä, miten henkilötietoja suojataan tehokkaasti. Syynä voi olla myös täydellinen luottamus sosiaalisen median palveluita kohtaan. Monissa sosiaalisen median sivustoissa kysytään tunnuksia luodessa kysymyksiä, joihin ei välttämättä kannata vastata mitään. Näitä kysymyksiä ovat esimerkiksi syntymäpäivä, kotikaupunki, työpaikka ja siviilisääty. Antamalla julkisuuteen jo nämä tiedot, on mahdollista joutua verkkorikollisuuden uhriksi. (Lewis.)

Henkilökohtaiset tiedot on aina syytä pitää omana tietonaan tai maksimissaan jakaa ne vain luotettaville kavereille, yrityksille ja yhteistyökumppaneille. Mikäli luotettavaa tietoa jakaa liikaa sosiaalisessa mediassa, saattaa käydä niin kuin eräälle Amerikkalaiselle sotilaalle. Kyseisessä tapauksessa rikollinen pääsi käsiksi hänen verkkopankkiin, tietämällä vain kyseisen sotilaan nimen, sähköpostin ja Facebook profiilin. (Lewis.)

Vaikka omat tai yrityksen henkilökohtaiset tiedot olisivatkin jaettu vain kavereille, ei se välttämättä estä rikollisia näkemästä näitä tietoja. Esimerkiksi Facebookissa on monenlaisia ladattavia sovelluksia, joista osa on tehty vain rikollisiin tarkoituksiin. Facebookissa 95 prosenttia käyttäjistä on ladannut ainakin yhden sovelluksen sivustolleen. (Lewis.) Lisätietoa haitallisista sovelluksista kerrotaan kohdassa 10.2.2 - Haittaohjelmat.

10.1.2 Identiteettivarkaudet

Identiteettivarkaudella tarkoitetaan ilman lupaa tapahtuvaa toisen nimellä tai muilla henkilötiedoilla esiintymistä. Identiteettivarkauden taustalla voi olla erilaisia motiiveja, kuten kiusaaminen, taloudellisen edun tavoittelu tai ”hyvä vitsi”. (Lakiasiaintoimisto Fiducius Oy 2014.) Identiteettivarkauksia on kahta eri tyyppiä: toisen nimellä esiintyminen ja petokset (Järvinen 2012, 256).

Sosiaalisessa mediassa suuri osa identiteettivarkauksista liittyy kiusaamiseen (Poliisi2). Työpaikkakiusaaminen, juoruilu ja työkavereiden haukkuminen ovatkin yleistyneet verkossa lähivuosien aikana (Andreasson ym. 2013, 160). Tällä hetkellä identiteettivarkaus ei ole Suomen lainsäädännössä rangaistava teko. Tähän saattaa tulla kuitenkin muutos vuonna 2015, jos oikeusministeriön lakiehdotus menee eduskunnassa läpi. (Poliisi2.) Vaikka toisen nimellä esiintyminen ei ole vielä rangaistava teko, voi se kuitenkin täyttää jonkin toisen rikoksen tunnusmerkit. Näitä ovat esimerkiksi petos, kunnianloukkaus tai yksityiselämää loukkaavan tiedon levittäminen. (Lakiasiaintoimisto Fiducius Oy 2014.)

Suomessa nettipoliisit saavat ilmoituksia valeprofiileista päivittäin. Identiteettivarkauden uhreiksi joutuvat Suomessa pääasiassa yksityishenkilöt ja julkisuuden henkilöt, mutta myös pienet ja suuret yritykset voivat olla uhrina. Suurin syy, miksi yrityksiin kohdistuu identiteettivarkauksia, johtuu rikollisten tekemistä talousrikoksista. (Liekki 2014.) Talousrikoksissa identiteettivaras useimmiten hankkii tietoonsa uhrin sosiaaliturvatunnuksen, luottokortin numeron ja osoitteen, joita hän käyttää hyväkseen esimerkiksi tilaamalla tavaraa uhrinsa laskuun. Näillä perustiedoilla rikollinen voi tehdä uhrilleen paljon taloudellista vahinkoa, koska muun muassa verkkokaupassa tekemiin ostoksiin riittää jo nämä tiedot. (Haasio 2013, 46–47.)

10.1.3 Vakoilu ja tietojen kalastelu

Tietojen kalastelulla tarkoitetaan huijausyritystä, jolla yritetään saada henkilöitä paljastamaan tietoja itsestään tai yrityksestä aidoilta näyttävillä kyselyillä (Yhteislyseon lukio 2011). Usein kyseiset huijausyritykset tulevat ulkomailta, ja ne on mahdollista tunnistaa joko vieraan kielen käytöstä tai huonosta suomen kielestä (Rongas 2012).

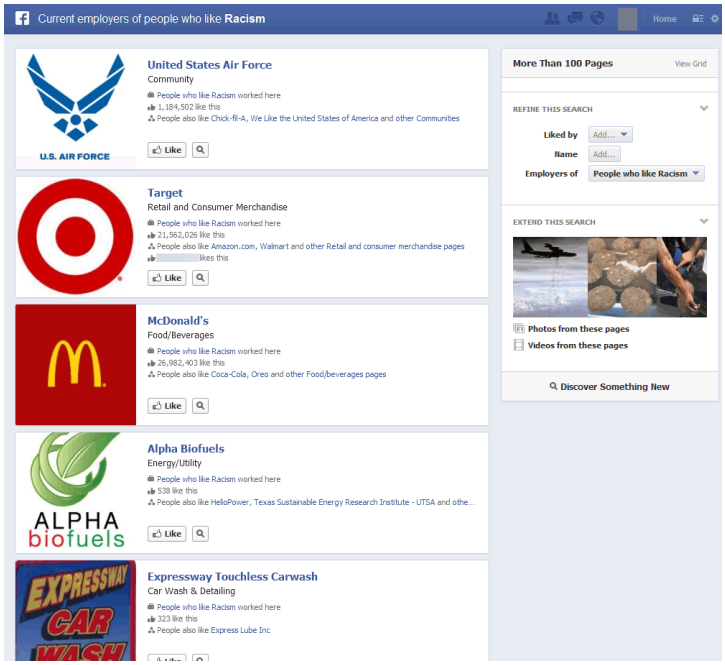
Monet tutkimustulokset ovat osoittaneet, että ihmiset hyväksyvät helposti omaan verkostoonsa henkilöitä, joita he eivät tunne. Tämä yhdistettynä liialliseen luottamukseen, huolimattomaan toimintaan ja osaamattomuuteen lisää organisaatioiden tietoturvariskiä. Yrityksen toiminta, maine ja yksityisyys saattavat vaarantua, jos soluttautuja käyttää verkostoja hyväkseen esimerkiksi vakoiluun, virheellisen tiedon tai haittaohjelmien levittämiseen tai henkilötietojen anastamiseen. Eräs turvallisuustutkija tutki, kuinka helposti sosiaalisessa mediassa on

soluttautua ja vakoilla muita ihmisiä. Hän onnistui muun muassa soluttautumaan Yhdysvaltojen sotilas- ja tiedusteluorganisaatioihin luomalla valeprofiilin Facebookiin, LinkedIniin ja Twitteriin ja liittämällä niihin naisen kuvan. Muutaman viikon sisällä tutkijalla oli satoja ystäviä ja seuraajia muun muassa Yhdysvaltojen puolustushallinnosta ja kansallisesta turvallisuusjärjestö NSA:sta. Hän onnistui myös saamaan verkostojen avulla käsiinsä arkaluonteista tietoa, nimiä, osoitteita, pankkitilejä ja sähköposteja. Lisäksi hän sai lukuisia esiintymiskutsuja hänen verkostossaan olevilta henkilöiltä. (Tuominen 2013, 52–53.)

Sosiaalisessa mediassa yritetään kalastella käyttäjien tietoja erilaisin menetelmin. Esimerkiksi Facebookissa on liikkunut linkki, jota klikkaamalla sivu ilmoittaa, että käyttäjä ei ole enää kirjautuneena Facebookissa. Kyseisessä tilanteessa näytölle tulee ikkuna, jossa käyttäjää pyydetään kirjautumaan uudelleen Facebookiin. Sivusto on täydellinen kopio Facebookin kirjautumisikkunasta. Mikäli käyttäjä kirjoittaa valesivulle oman käyttäjätunnuksensa ja salasanansa, saa rikollinen siepattua kirjautumistiedot. (Ferguson 2013.)

Sosiaalisen median päätarkoitus on jakaa ja vastaanottaa tietoa. Tästä syystä kenellä tahansa on mahdollista esimerkiksi lukea käyttäjän julkaisemat viestit ja nähdä käyttäjän kuvat. Yksityisyysasetuksia tiukentamalla tiedot voi jakaa vain esimerkiksi kavereille tai yhteistyökumppaneille, mutta tämä ei täysin poista tietojen vakoiluun tai kalastamiseen liittyviä ongelmia. Petteri Järvinen on todennut sanomalehti Keskisuomalaiselle antamassa haastattelussa, että suurimpana vaarana sosiaalisen median palveluissa ovat ystävälistalle pääsevät ulkopuoliset henkilöt, jotka voivat olla huijareita. Tällöin huijarit voivat saada hyvinkin henkilökohtaisia asioita selville. (Haasio 2009, 70.)

Tammikuussa, 2013 Facebook otti käyttöön yhteisöhaun (englanniksi Graph Search). Kyseisellä hakutoiminnolla pystyy hakemaan esimerkiksi henkilöitä, jotka työskentelevät tietyissä yrityksissä ja tykkäävät rasismista. Tämä saattaa koitua ongelmaksi sekä yritykselle että sen työntekijälle, mikäli hakutuloksesta käy ilmi, että yrityksessä työskentelee esimerkiksi monia rasismista tykkääviä henkilöitä. Yhteisöhaku myös helpottaa tietojenkalastajien työtä, koska sitä käyttävät tahot voivat saada entistä tarkempia tietoja esimerkiksi henkilön parisuhteista, asuinalueesta, työpaikasta, harrastuksista ja niin edelleen. Näiden tietojen pohjalta on helppo laatia esimerkiksi luotettavilta kuulostavia sähköpostiviestejä, joilla kalastella luottokorttitietoja, pankkitunnuksia ja salasanoja. (Ajankohtaista uskosta 2013.)



Kuva 2 Yritykset, joissa työskentelee rasistista tykkääviä henkilöitä (Scott 2013).

Eri sosiaalisen median palveluissa, kuten Facebookissa ja Twitterissä, on ollut jo jonkin aikaa käytössä paikantamispalvelu. Paikantamispalvelu saattaa muuttua tietoturvauhaksi varsinkin mobiililaitteella käytettynä, koska sijainnin päädyttyä vääriin käsiin, saa rikollinen tietää käyttäjän sen hetkisen sijainnin. Tämä nostaa sijainnin jakajan riskiä joutua esimerkiksi taskuvarkauden uhriksi. Lisäksi se saattaa paljastaa sen, että uhri ei ole kotona tai työpaikalla. Näiden tietojen avulla rikollinen saattaa iskeä uhrin kotiin tai työpaikalle (mikäli rikollinen tietää uhrin koti- tai työosoitteen). Sosiaalisessa mediassa on tiedettävästi sattunut tapauksia, joissa rikollinen on seurannut ihmisten tilapäivityksiä ja suunnitelleen niiden perusteella asuntomurtoja (Haasio 2013, 52). Paikantamispalvelun käyttöön vaikuttavien riskien takia muutama hollantilainen teki sovelluksen nimeltään ”Rob me”.

Rob me -sovellus kerää sosiaalisesta mediasta tietoa viesteistä, joissa sen käyttäjät ilmoittavat olevansa muualla kuin kotona. Sovellus myös päivittää henkilöiden nykyisen olinpaikan, mikäli kyseinen tieto on saatavilla. Kyseinen sovellus on saanut melko paljon kritiikkiä juuri siitä syystä, että se on tehokas työkalu rikollisille. (Web Wise Business News.)

Sovelluksen perustajien mukaan he kuitenkin tekivät sovelluksen ainoastaan varoittaakseen paikantamispalvelun huolimattomasta käytöstä (Web Wise Business News). Paikantamispalveluiden tuomien riskien takia esimerkiksi Suomen varusmiesten operaatioissa on aina kielletty paikkatiedon jakaminen (Puolustusvoimat).

LinkedIn-palvelussa piilee omanlaisensa riskinsä vakoilun ja tietojen kalastelun saralla. Esimerkiksi kyseisessä palvelussa käyttäjän jakama työhistoria saattaa auttaa huijareita tekemään kohdistettuja hyökkäyksiä käyttäjää vastaan tai lähettämään tekaistuja työtarjouksia (Järvinen 2012, 301).

Erityisesti tietojen kalastelu on muodostunut merkittäväksi ongelmaksi sosiaalisessa mediassa. Käyttäjiä muun muassa yritetään huijata paljastamaan tietoa itsestään tai työnantajastaan aidoilta näyttävillä kyselyillä. (Tuominen 2013, 52.) Tietojenkalastelu on vuosien saatossa kuitenkin vähentynyt haittaohjelmien yleistymisen takia (Nikulainen 2007).

10.2 Tekniset uhat

Suurimmat teknilliset uhat sosiaalisessa mediassa ovat siellä liikkuvat haittaohjelmat, jotka leviävät palveluiden välityksellä käyttäjien tietokoneisiin (Hämäläinen & Heikkilä 2011, 15). Tässä kappaleessa käydään läpi sosiaalisen median teknisiä uhkia. Aluksi käydään läpi tietokoneessa käytettäviä sovelluksia, jotka saattavat aiheuttaa tietoturvaongelmia. Tämän jälkeen kerrotaan sosiaalisessa mediassa liikkuvista sovelluksista, jotka saattavat aiheuttaa pahimmassa tapauksessa taloudellista vahinkoa, tietokoneen saastumisen vakoiluohjelmista ja viruksista tai sosiaalisen median käyttäjätilin menettämisen rikolliselle. Lisäksi tässä kappaleessa käydään tarkemmin läpi haittaohjelmia, joita sosiaalisessa mediassa liikkuu. Lopuksi tässä kappaleessa kerrotaan asiaa roskaposteista ja niiden tuomista harmeista.

10.2.1 Sovellushaavoittuvuudet

Vanhat selaimet ja ohjelmat sisältävät paljon tietoturva-aukkoja, jotka mahdollistavat hakkereiden ja muiden rikollisten pääsyn muun muassa käyttäjien sosiaalisen median tilille ilman salasanaa. Googlen turvallisuusasiantuntijat julkaisivat löytämänsä tietoturva-aukon 15.10.2014, josta kävi ilmi, että SSLv3-salaustekniikkaa hyväksi käyttämä selain mahdollistaa ulkopuolisen pääsyn tietokoneelle. Esimerkiksi Windows XP:n Internet Explorer 6 käyttää ainoastaan kyseistä salaustekniikkaa. Salaustekniikkaa hyväksi käyttävä hyökkäys pystyy kaappaamaan tietokoneen käyttäjän ja verkkosivustojen välillä kulkevan pienen tiedoston eli cookien. Cookieta käyttäen hyökkääjä voi jatkossa kirjautua kohteensa sosiaalisen median tilille ilman salasanaa. Kyseistä haavoittuvuutta on mahdollista käyttää hyväksi vain avoimissa langattomissa verkoissa, joten kotikoneella tietoturva-aukosta ei ole vaaraa. (Lapintie 2014.)

Sosiaalisessa mediassa liikkuu paljon sovelluksia, jotka keräävät tietoa sen käyttäjistä. Sovellusten kehittäjiltä vaaditaan käyttöehdoissa, että sovellukset kunnioittavat käyttäjien yksityisyysasetuksia, mutta käytännössä tätä ei pystytä millään tavalla valvomaan. (Aalto ym. 2009, 95.) Sovellukset vaativat aina pääsyn joihinkin käyttäjän tietoihin silloin, kun niitä asennetaan sosiaalisen median palveluissa (Facebook).

Kuva 3 Facebook sovelluksen käyttöehdot (Facebook).

Kuvassa näkyvä Facebook sovellus saa käyttöönsä käyttäjän perustiedot (johon sisältyy käyttäjän nimi, profiilikuvat, käyttäjätunnus, kaverilista sekä muut julkiseksi tiedoksi määritetyt asiat). Näiden tietojen lisäksi sovellus saa käyttöönsä myös käyttäjän sähköpostiosoitteen. Sovelluksella on myös oikeus julkaista kohteet, joista käyttäjä tykkää Facebookissa. Painamalla ”Pelaa nyt” painiketta, käyttäjä hyväksyy palvelun käyttöehdot ja yksityisyydensuojaperiaatteet. (Facebook.) Osa sovelluksista saattaa päästä käsiksi myös muihin käyttäjän henkilökohtaisiin tietoihin käsiksi. Näitä ovat esimerkiksi käyttäjän koulutushistoria, työhistoria ja kurssitiedot, sekä kuvat ja niiden metadata, käyttäjän saamien ja lähettämien viestien määrä, lukemattomien viestien määrä, käyttäjän lähettämien ja vastaanottamien tökkäysten määrä, käyttäjän seinällä olevien viestien määrä, Facebook kavereiden käyttäjätunnukset, käyttäjän yhteisöllisen aikataulun ja Facebook-profiiliin liittyvät tapahtumat. (Tapscott 2010, 79.)

Mikäli kyseessä on ei-toivottu sovellus, saa sovelluksen kehittäjä paljon yksityiskohtaista tietoa käyttäjästä. Tämä saattaa johtaa esimerkiksi identiteettivarkauteen ja pahimmassa tapauksessa taloudellisiin menetyksiin. Haitallinen sovellus voi julkaista sisältöä kaverilistalla olevien henkilöiden tai yritysten aikajanoilla (Facebook).

10.2.2 Haittaohjelmat

”Haittaohjelma on ohjelma, joka on suunniteltu tekemään ei-toivottuja toimintoja käyttäjän puolesta.” Haittaohjelman avulla voidaan ohittaa muun muassa Facebookissa turva-asetuksia ja kaapata käyttäjän tilejä. Haittaohjelma voi kerätä tietoa sen uhristaan, lähettää tilapäivityksiä tai viestejä uhrinsa nimellä. (Facebook 2014.)

Haittaohjelma voi myös lähettää uhrilleen jatkuvasti mainosviestejä, jonka johdosta uhrin tietokone saattaa lakata toimimasta. Facebookin oman turvallisuustiedotteen mukaan haittaohjelman voi saada esimerkiksi avaamalla linkin shokeeraavalle sivustolle, käymällä sivustolla, joka väittää tarjoavansa erityisiä toimintoja Facebookiin tai lataamalla selaimeen laajennuksen, joka on liian hyvä ollakseen totta. (Facebook 2014.)

Monet ihmiset ovat jo oppineet suhtautuvan epäillen sähköpostilla tuleviin viesteihin, mutta sosiaalisen median viesteihin eivät. Useimmat sosiaalisen median haittaohjelmat liikkuvat roskapostin tai niin sanotun uudemman sosiaalisen roskapostin välityksellä. Sosiaalinen roskaposti käyttää sosiaalista mediaa, perinteistä mediaa ja uutisiin liittyviä verkkosivuja linkkien levittämiseen. Tyypillisessä Facebookin haittaohjelmassa tai huijaussivustossa huijataan käyttäjää klikkaamaan hiirellä jotain, mutta samalla käyttäjä tuleekin sallineeksi jotain muuta. Ensin huijaussovellus huijaa käyttäjältä riittävät oikeudet, jonka jälkeen se kirjoittaa käyttäjän tai kaverin seinälle mielenkiintoiselta vaikuttavan viestin, kuten uutisen. Sen avulla huijaussovellus pyrkii saamaan käyttäjän kaverit avaamaan linkin ja levittämään huijausta eteenpäin. Tämän tyyliset sovellukset keräävät yleensä käyttäjien sähköpostiosoitteita ja muita tietoja, joita myydään eteenpäin muun muassa roskapostittajille. Myydyillä tiedoilla haittaohjelman tekijä tienaa rahaa itselleen. (Andreasson ym. 2013, 165–166.)

Vuonna 2008 sosiaalisen median eri palveluissa levitettiin yhteensä yli 20 000 haittaohjelmaa (Haasio 2013, 53). Sosiaaliseen mediaan liittyviä haittaohjelmia on siis lukuisia. Esimerkiksi Facebookissa on liikkunut jo pitkän aikaa haittaohjelma nimeltään Koobface. Kyseinen haittaohjelma monistaa itseään ja tartuttaa muita tietokoneita. Koobfacen tehtävä on varastaa Facebook käyttäjien käyttäjätunnuksia ja salasanoja. Koobface luo myös automaattisesti vale Facebook-profiileita kaappaamien uhrien tiedoilla. Koobface tai muu samankaltainen haittaohjelma leviää usein ylimääräisen ohjelman mukana. (Ferguson 2013.)

Tämän kaltaiset ohjelmat mainostavat, että laitteeseen on asennettava jokin ylimääräinen ohjelma, jotta sillä voidaan toistaa esimerkiksi valheellinen YouTube-video. (Ferguson 2013.) Koobface pystyy varastamaan kaikki tiedot, jotka käyttäjä on lisännyt omalle sosiaalisen median tililleen. Sen toimintaympäristöjä ovat: Facebook, MySpace ja Twitter. (Boquiron.)

Toinen Facebookissa liikkuva epämiellyttävä ja melko yleinen haittaohjelma on Facebookin väriteemaa muuttava palvelu ”Facebook Color Changer”. Niin ainakin Facebookissa liikkuva linkki lupaa. Tosin kyseessä on huijausyritys, joka todellisuudessa tekee ikäviä asioita käyttäjän tietokoneessa tai muussa laitteessa. Linkki vie käyttäjän haitalliselle tietojenkalastelusivulle. Käyttäjän katsellessa kalastelusivustolla olevaa videota, pääsevät rikolliset hetkeksi käsiksi käyttäjän Facebook kavereiden profiiliin. Kiinalaisen tietoturvayrityksen Cheetah Mobilen mukaan tämä ilmeisesti mahdollistaa virusten haitallisen koodin upottamisen Facebook-sovelluksiin. Haitallinen koodi puolestaan ohjaa käyttäjät tietojenkalastelu sivustoille. (Digitoday 2014.)

Myös LinkedIn -palvelussa on omanlaiset riskit saada haittaohjelma omaan laitteeseen. LinkedIn mahdollistaa sen käyttäjien lisäävän muun muassa WordPress blogeja omaan profiiliin. Osa näistä blogeista saattaa olla kolmansien osapuolten tekemiä ja sisältää haittaohjelmia. Näin ollen tietokoneeseen saattaa päästä haittaohjelma blogien välityksellä, ja tämä saattaa aiheuttaa vakavia tietoturvariskejä. (Sophos.)

10.2.3 Roskaposti

Roskapostilla tarkoitetaan ei-toivotun sisällön tai pyynnön lähettämistä muille palvelua käyttäville henkilöille. Esimerkkejä tästä ovat massaviestit, kuvien tai linkkien julkaiseminen käyttäjien aikajanoilla ja kaverikutsujen lähettäminen henkilöille, joita toinen käyttäjä ei tunne henkilökohtaisesti. Roskapostit voivat levitä haitallisten ohjelmien välityksellä tai huijareiden kaapattua muiden sosiaalisen median profiileita, joilta he lähettävät roskapostia. (Facebook.) Roskapostia saattaa esiintyä sosiaalisessa mediassa samalla tavalla kuin sähköpostissa (Hirvonen 2011).

Monet roskapostit ovat useimmiten ulkomaalaisia, mutta myös suomalaishuijarit ovat alkaneet tekemään niitä. Esimerkiksi Facebookissa on liikkunut linkki, johon oli sisällytetty mato. Tämä mato urkki käyttäjien profiilissa ilmoitetut puhelinnumerot, pyytämällä niitä kilpailua varten. Puhelinnumeron saatua, käyttäjältä laskutettiin puhelinlaskussa 19 euroa kuussa mobiilisovelluksesta, josta käyttäjä ei ollut tietoinen. Tämän lisäksi käyttäjä saattoi tietämättään suositella linkkiä myös Facebook-kavereilleen. (Haasio 2013, 55.)

Pelkästään Facebookissa roskapostia sai vuonna 2010 yli neljä miljoonaa käyttäjää päivittäin. Roskapostien määrä lisääntyy vauhdilla (jopa nopeampaa kuin käyttäjäkunta Facebookissa). Facebookin mukaan kaikista sen palvelussa lähetetyistä viesteistä neljä prosenttia on jonkinlaista roskapostia. Twitterissä määrä oli vuonna 2010 maltillisempi. Kaikista palvelussa

lähetetyistä viesteistä 1,5 prosenttia oli roskapostiksi luokiteltua postia. (Lyytikäinen 2010.) Sosiaalisessa mediassa liikkuvat roskapostit naamioidaan usein kiinnostaviksi posteiksi, jotka toimivat syötteinä. Roskapostin tehtävä on saada käyttäjiä avaamaan niiden tarjoamia linkkejä. Useimmat roskapostin linkeistä sisältää vakoiluohjelman. (Boquiron.)

10.3 Muut uhat

Aiemmin mainittujen riskien lisäksi saattaa sosiaalisessa mediassa ja sen käytössä esiintyä vielä muutamia muita riskejä. Näitä ovat palveluiden epäselvät ja muuttuvat sopimusehdot, henkilöturvallisuuteen liittyvät asiat, yksityisyyden suoja ja siihen rinnastettavat asiat sekä maineen hallinta.

10.3.1 Palveluiden epäselvät ja muuttuvat sopimusehdot

Sosiaalisen median palvelut vaativat käyttäjää hyväksymään palvelun sopimusehdot (käyttöehdot) käyttääkseen palvelua. Harva kuitenkaan tietää, mitä kaikkea sopimusehdot sisältävät ja mihin kaikkeen on sitoutunut hyväksyttyään sopimusehdot. Ehdoissa on yleisesti ottaen kolme kompastuskiveä: ehtojen kieli, niiden esitystapa ja olemassaolo. Ehdot ovat usein kirjoitettu englanniksi, eivätkä kotimaiset käännökset ole välttämättä kovin korkeatasoisia. Sopimusehdot ovat usein myös pitkiä ja täynnä yksityiskohtaisia, raskaita juridisia lauseita. Kieliasusta aiheutuu ehkäpä suurimmat ongelmat. Harva käyttäjä lukee sopimusehtoja, vaan hyväksyy ne saman tien. (Aalto & Liesvirta 2014.)

Monen sosiaalisen median palvelun ehdoissa on kohta, jonka mukaan käyttäjä myöntää palveluntarjoajalle käyttöoikeuden käyttäjän lataamaan sisältöön. Tämä oikeuttaa palveluntarjoajaa lisensoida käyttäjän sisältöä eteenpäin kolmansille tahoille. (Aalto ym. 2014.) Yleisesti ottaen yhdessäkään sosiaalisen median palvelussa ei kannata jakaa arkaluonteista materiaalia, lukematta ensin tarkkaan sopimusehtoja.

Mikäli käyttäjä rikkoo sopimusehtoja, on hän vastuussa mahdollisista seurauksista. Näitä saattavat olla esimerkiksi vahingonkorvaukset tai pahimmassa tapauksessa rikosoikeudelliset toimenpiteet. (Aalto ym. 2014.)

Sosiaalisessa mediassa sopimusehdot muuttuvat melko tiuhaan tahtiin. Esimerkiksi Facebookissa päivityksiä sopimusehtoihin on tullut vuosien saatossa lukuisia. Sosiaalisen median palveluita tarjoavat yritykset kuten Facebook, ovat varanneet itselleen yksipuolisen oikeuden muuttaa palvelun sääntöjä milloin tahansa (Koivumäki ym. 2013).

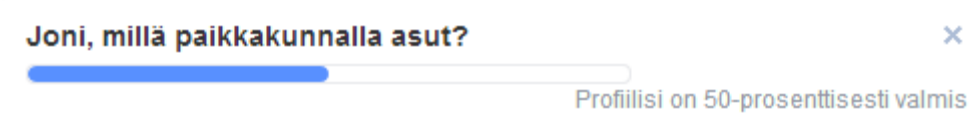
Esimerkkinä sopimusehtojen muutoksista kertoo se, että tätä opinnäytetyötä tehdessäni Facebook julkaisi uudet sopimusehdot, jotka tulivat voimaan 1.1.2015. Uusien sopimusehtojen mukaan Facebook saa oikeuden käyttää sen käyttäjien julkaisemaa materiaalia maailmanlaajuisesti. (Facebook5.)

Eniten kritiikkiä ovat varmasti herättäneet juuri Facebookin tekemät muutokset sopimusehtoihin. Sopimusehtojen muuttuminen saattaa tulla ongelmalliseksi, jos ehdot muuttuvat merkittävästi, kuten kävi Facebookissa tammikuussa vuonna 2013. Tällöin Facebook poisti käyttäjiltä mahdollisuuden piiloutua hakutuloksilta (Talouselämä 2013). Tämä mahdollisti esimerkiksi käyttäjien etsimisen Graph Search -hakukoneella, josta kerrottiin aiemmin tässä opinnäytetyössä.

Facebookilla on ollut myös aiemmin kyseenalaisia ominaisuusmuutoksia heidän palvelussaan. Muun muassa yksi kyseenalainen muutos tapahtui marraskuussa vuonna 2007. Tällöin käyttäjän ostaessa tuotteen kauppiaalta, joka oli mukana Facebookissa, lähti ostoksesta automaattisesti tieto käyttäjän kaverilistalla oleville henkilöille. Tämä ominaisuusmuutos sai paljon kohua aikaiseksi. Kohun takia Facebook muutti järjestelmää siten, että käyttäjät pystyvät itse päättämään, ottavatko kyseisen ominaisuuden käyttöön vai ei. (Tapscott 2010, 81–82.)

10.3.2 Henkilöturvallisuus

Sosiaalisen median palveluissa, kuten Facebookissa kannustetaan käyttäjiä antamaan paljon tietoa itsestään. Liiallisen tiedon jakaminen saattaa kuitenkin olla vaarallista. Tietoja, joita eri palvelut saattavat kysyä ovat esimerkiksi: kotiosoite, syntymäpäivä ja puhelinnumero. Kyseiset tiedot ovat kaikkien nähtävillä, mikäli yksityisyysasetuksista ei ole tiukennettu. (Wheeler.) Vaikka tiedot olisi määritelty profiilissa yksityisiksi, ei se täysin estä tietojen joutumista ulkopuolisille tahoille. Jos esimerkiksi hakkeri pääsee murtautumaan käyttäjän profiilitilille, saa hän kaikki profiilissa olevat tiedot itselleen (myös yksityiseksi määritellyt). Profiilista saatuja tietoja voidaan käyttää muun muassa identiteettivarkauksiin ja talousrikosten tekoon. (Wheeler.)



Kuva 4 Profiilitietojen kysely Facebookissa.

Sosiaalisessa mediassa käytössä oleva paikantamispalvelu saattaa myös olla vaarallinen lisäosa, mikäli paikantamistiedot joutuvat ulkopuolisten käsiin. Paikantamispalvelu paljastaa käyttäjän sijainnin ja paikat, joissa käyttäjä on aiemmin ollut (mikäli käyttäjällä on paikantamispalvelu ollut käytössä). Myös kaverit voivat merkitä toisia käyttäjiä omaan viestiinsä tai kuvaansa paikantamispalvelua käyttäen. Paikantamispalvelun käyttö saattaa aiheuttaa henkilöturvariskin, jonka johdosta käyttäjällä on riski tulla muun muassa ryöstetyksi. (Wheeler.)

Myös sosiaalisen median palveluun ladattu valokuva saattaa ääritapauksissa olla haitallista henkilöturvallisuuden kannalta. Jos valokuvassa näkyy käyttäjän oma auto ja sen rekisteritunnus, on rikollisella helppo selvittää omistajan kotiosoite soittamalla ajoneuvohallintokeskukseen. (Thorslund 2009, 35.)

Yritykseen tai työyhteisöön kuuluvaan henkilöön saattaa kohdistua ulkopuolista vaaraa. Tästä syystä sosiaalisessa mediassa kannattaa toimia varovaisesti, oli kyseessä sitten oma yksityinen profiili tai yrityksen julkinen profiili. Erityisesti korkeassa asemassa toimivilla henkilöille on äärimmäisen tärkeää kiinnittää huomiota turvallisuusasioihin myös työpaikan ulkopuolella (Kreus). Erään tietoturvayrityksen johtaja on kertonut, ettei hän käytä sosiaalisen median palveluita oman ja perheensä fyysisen turvallisuutensa takia (Candolin 2011).

10.3.3 Yksityisyyden suoja

Yksityisyydellä tarkoitetaan ihmisten omaa kykyä itse päättää, kuka tietää hänestä mitä, milloin ja missä yhteydessä (Tranberg ym. 2013, 15).

Henkilötiedoista on tullut ikään kuin uutta raakaöljyä, joka pyörittää Internet-taloutta. Esimerkiksi sosiaalisessa mediassa ”ilmaisella” sovelluksella tai palvelulla on todellisuudessa myös hintansa. Ne maksetaan omilla henkilötiedoilla ja tiedot ovat sitä parempia, mitä yksityiskohtaisempia ne ovat tietoa keräävien näkökulmasta. (Tranberg ym. 2013, 13.)

Keväällä 2010 Facebookissa yritettiin saada käyttäjiä liittymään IKEA.com-sivuston faneiksi ja huijata samalla käyttäjiä paljastamaan suuren määrän henkilötietojaan. Kyseessä oli erityisen suuri ongelma Suomessa, mutta samankaltaisia tapauksia sattuu maailmalla jopa päivittäin. (Tuominen 2013, 51.)

Sosiaalisen median käyttäjistä voidaan kerätä heidän tahdostaan riippumatta tietoa muun muassa mainostajien käyttöön (Seppänen & Väliverronen 2014, 164). Muun muassa käyttäjien jakama aineisto Facebookissa vaikuttaa siihen, mitä mainoksia käyttäjälle näytetään (Järvinen 2012, 300). Kyseisestä ilmiöstä käytetään nimitystä kohdistettu mainonta. Mo-

net sosiaalisen median palvelut, kuten Facebook pyytää käyttäjiltä monenlaista tietoa, jolla on taloudellista arvoa mainostajille (Seppänen ym. 2014, 164). Käyttäjän kirjatessa Facebookiin oman nimen, syntymäajan, sukupuolen, yhteystiedot, harrastukset, listan lempielokuvista, -musiikista tai – kirjoista, työpaikkatietonsa ynnä muut, käyttäjä kertoo paljon maailmankuvastaan tai kulutustottumuksistaan. Käyttäjä saattaa luulla, että nämä tiedot ovat vain hänen Facebook-kavereilleen, mutta käytännössä nämä tiedot saattavat levitä paljon laajemmalle. Facebook on yrittänyt helpottaa näiden tietojen leviämistä yksityisyysasetuksia ja muita sovelluksia muuttamalla, jotta siitä tulisi houkuttelevampi ympäristö mainostajille. (Seppänen ym. 2014, 164–165.) Lisäksi Facebook saattaa kerätä käyttäjistä tietoja myös muista lähteistä, kuten sanomalehdistä, blogeista, pikaviestimistä ja muilta Facebookin käyttäjiltä palveluiden toimintojen kautta (esimerkiksi valokuvien merkinnöistä) (Haasio 2009, 66).

Mainostajien, sovellusten ja palveluiden kehittäjien lisäksi myös tiedustelupalvelulla on pääsy sosiaalisessa mediassa jaettuihin asioihin. Esimerkiksi CIA (Central Intelligence Agency), NSA (National Security Agency, Yhdysvaltojen sähköinen tiedustelupalvelu) ja vastaavat organisaatiot hyötyvät paljon saamistaan tiedoista, joita ihmiset ympäri maailmaa jakavat (Järvinen 2012, 294–295). Merkityksettömiltä vaikuttavista tiedonmurusista tiedustelupalvelut pystyvät kaivamaan esiin muun muassa kehitystrendejä, jotka ovat hyödyksi päätöksenteoille. Näin ollen Yhdysvaltojen hallinto tietää jo etukäteen, millaista kehitystä eri maissa tulee tapahtumaan lähitulevaisuudessa. (Järvinen 2012, 295.)

Monissa sosiaalisen median ohjelmissa, kuten Facebookissa on oletuksena, että käyttäjän jakamat tiedot ovat julkisia. Facebookin turvallisuusjohtajan mukaan vuonna 2011, kaikista Facebookin käyttäjistä vain 20 prosenttia oli muokannut omia yksityisyysasetuksia. Loput 80 prosenttia eivät tienneet yksityisyysasetuksista, pitivät yksityisyysasetusten muuttamista liian vaivalloisena tai eivät piitanneet, että kaikki heidän tietonsa ovat julkisia. (Aboujaoude 2011, 240.)

Seija Ridellin teettämän tutkimuksen mukaan suurin ongelma Facebookissa ovat palvelun yksityisyyttä koskevat asiat. Tutkimusta varten oli haastateltu noin kahta tuhatta suomalaista, joista yhteensä 441 pitivät Facebookin yksityisyyden suojaa heikkona. (Ridell 2011, 90–91.) Sosiaalisen median palveluissa on muutenkin melko hankala toimia yksityisyyden suojissa. Syitä tähän löytyy monia. Ensimmäiseksi, sosiaalisen median palveluihin saattaa ilmestyä uusia ominaisuuksia ja toiminnallisuuksia. Nämä uudet ominaisuudet ja toiminnallisuudet saattavat paljastaa käyttäjästä tietoa toiselle osapuolelle, vaikka käyttäjä olisi aiemmin säätänyt turvallisuusasetuksensa kuntoon. (Juslén 2010.) Toiseksi, henkilöiden tykkäämiset ja käyttäjien merkitseminen kuviin ja tilapäivityksiin saattaa aiheuttaa ongelmia myös yksityisyyden kannalta (Facebook3 2014).

Lisäksi lähipiirille jaettu aineisto voi vuotaa eteenpäin, kun joku piiriin kuuluvista jakaa sen omille kavereilleen (Järvinen 2012, 306). Käyttäjien lisääminen kuviin saattaa nousta ongelmaksi, jos esimerkiksi käyttäjä lisää yksityiseksi luokitellun kuvan, johon arvovaltainen tuttava on lisätty eli niin sanotusti tägätty, ja kuva on avoin sekä sen lisääjälle että arvovaltaisen henkilön kavereille (Facebook3 2014).

Myös paikantamispalvelun käyttö sosiaalisen median palvelussa saattaa vaikuttaa merkittävästi yksityisyyden turvaan. Se voi paljastaa muun muassa yritysten yhteistyöneuvottelujen vireilläolon tai asiakassuhteen olemassaolon. Molemmat näistä kuuluvat salassapitositoumuksen piiriin. Tästä syystä sosiaalisessa mediassa työaikana toimiessa on aina oltava varovainen paikantamispalvelua käyttäessä. (Koivumäki ym. 2013, 177.) Korkeassa asemassa olevien henkilöiden osalta yksityisyyden suojaan on syytä perehtyä kunnolla. Tätä kuvastaa seuraava esimerkki.

Vuonna 2009 Brittien ulkomaan tiedustelupalvelun tulevan johtajan sir John Sawersin vaimo lisäsi valokuvia Facebookiin. Tulevan johtajan perhe- ja lomakuvat olivat kaikkien nähtävillä, koska yksityisyysasetuksia ei ollut tiukennettu. Kuvissa esiintyi Sawers perheineen rantalomalla sekä miehen pojat tyttöystävineen. Lisätyissä kuvissa esiintyi myös miehen ystäviä ja hänen vanhempansa. Turvallisuusriskinä pidetyt tiedot ja valokuvat poistettiin palvelusta välittömästi erään lehden otettua yhteyttä maan ulkoministeriöön. (Laurio 2009.)

10.3.4 Maineen hallinta

Yrityksen maine rakentuu mielikuvista ja kokemuksista, joita syntyy yrityksen ja sen sidosryhmien välisissä kohtaamisissa (Seeck 2009, 58). Yrityksen maineella on suuri vaikutus sen tuotteiden ja palveluiden myyntiin. Tämän takia hyvin hoidettu maineenhallinta on erittäin tärkeä asia yritysmaailmassa. Kuluttajia ei kiinnosta vain yrityksen tarjoamat palvelut ja tuotteet, vaan yritystoiminta laajemmin. Sosiaalinen media voi tuoda yritykselle lisää mainetta ja kunniaa tai se voi vaikuttaa negatiivisesti yrityksen maineeseen. Sosiaalisen median mukaan tulo yritysmaailmaan mahdollistaa sen käyttäjille oivan apuvälineen tuoda esille yrityksen epäkohdat muutamalla napin painalluksella. Pahimmillaan tämä saattaa johtaa yrityksen maineen menettämiseen. Sosiaalisessa mediassa leviävällä aineistolla tai videolla voi olla suuri vaikutus yrityksen maineeseen, mikäli siihen ei osata heti vastata ja suhtautua oikein. (Marttinen 2014.) Yritysten onkin hyvä muistaa, että sosiaalista mediaa voi vain ohjata, mutta sitä ei voi hallita (Limnéll ym. 2014, 186).

Sosiaalisen median mukaantulo yritysmaailmaan tuo sisällään siis uusia odotuksia ja uskomuksia. Näitä voivat olla muun muassa käyttäjien vahvistamat odotukset eettisestä liiketoiminnasta tai toiminnan avoimuudesta. New York Stern School of Businessin ja Eurooppalaisen INSEADin rahoituksen hallinnon ja etiikan professori Ingo Walterin mielestä mainetta ei tuhoa kriisitapahtuma itsessään, vaan tuho on seurausta huonosta kriisihallinnasta. (Seeck 2009, 57–63.)

Konkreettinen esimerkki tästä on Aamulehden toiminta heinäkuussa vuonna 2011. Tällöin Aamulehden toimittaja spekuloi Norjan tragedian yhteydessä, että nuori mies äityy joukkosurmaajaksi jäädessään vaille vastakkaista sukupuolen huomiota. Kyseinen artikkeli sai monet pahastumaan, jonka seurauksena Facebookiin luotiin Aamulehti boikottiin ryhmä, joka keräsi lyhyessä ajassa parituhatta tykkääjää. Salla-Maaria Laaksonen toteaa Journalismikritiikin vuosikirjassa, että Aamulehden olisi pitänyt olla nöyrempi ja pyytää epäonnistuneita sananvalintoja anteeksi sosiaalisen median yhteisöltä. Aamulehden toimittaja ei kuitenkaan koskaan pyytänyt anteeksi, vaan puolusti jutun pääviestiä. (Aalto 2012, 38.)

Yrityksen maineeseen saattaa vaikuttaa myös siitä luodut valesivustot. Näin kävi esimerkiksi kansainväliselle energia-alan yritykselle nimeltä BP. Yksityinen henkilö loi yrityksestä parodioivan Twitter-tilin, jossa hän otti kantaa yrityksen toimintaan Meksikon-lahden öljykatastrofissa. Hänen mukaansa yhtiö ei saanut ratkaisuja aikaiseksi, ei pitänyt kiirettä, eikä se ollut vilpitön katastrofin sattuessa. Kyseinen tili keräsi lähes 200 000 seuraajaa. (Forsgård ym. 2010, 49–50.)

Vuorovaikutus sosiaalisessa mediassa on avointa, ja siellä jaetut viestit ja muut materiaalit saadaan helposti näyttämään rehellisiltä ja uskottavilta. Niiden avulla on helppo vaikuttaa muiden tunteisiin ja mielipiteisiin. Lisäksi sosiaalisessa mediassa jaetut materiaalit eivät välttämättä sisällä edes faktaa vaan tunnetiloja, mielipiteitä ja näkemyksiä. Sosiaalisessa mediassa on siis melko helppoa manipuloida ja ”aivopestä” muita käyttäjiä. (Rautanen 2011, 100.) Sosiaalisessa mediassa leviävät valheelliset viestit yrityksestä ja sen toiminnasta saattavat aiheuttaa suuria ongelmia muun muassa yrityksen maineelle.

Maineenhallinnan kannalta on myös kiinnitettävä huomiota työntekijöiden sosiaalisen median sisältöön. Esimerkiksi, jos käyttäjän profiilista käy ilmi, että hän työskentelee yrityksessä, saattaa hänen käyttäytyminen sosiaalisessa mediassa vaikuttaa jollakin tasolla tämän yrityksen maineeseen.

11 Suojautuminen sosiaalisen median uhilta ja haitoilta

Tässä kappaleessa kerrotaan erilaisia toimenpiteitä, joilla sosiaalisen median riskit saadaan minimoitua. Kappaleessa pyritään löytämään tarvittavat ja riittävät ratkaisut edellisessä kappaleessa käytyihin sosiaalisen median vaaroihin. Tässä kappaleessa käytetään samoja otsikoita, kuin edellisessä kappaleessa. Tällä tavoin pyritään lisäämään raportin helppolukuisuutta ja saavuttamaan selkeän ulkoasun ongelmista ja niiden ratkaisuista.

11.1 Tietoaineistoon liittyvät riskit

Yritysten on hyvä kiinnittää huomiota siihen, millä tavalla he ottavat kantaa työntekijöidensä viestittelyyn sosiaalisessa mediassa. Jokaisella henkilöllä on sananvapaus, johon yksikään yritys ei pysty vaikuttamaan. Kaikkien yritysten kannattaa luoda työntekijöillensä ohjeistukset siitä, mitä asiaa sosiaalisessa mediassa ei saa jakaa ja miten siellä olisi syytä toimia. Ohjeistukset vähentävät muun muassa työntekijöiden tekemiä salassapito- ja lojaalivelvollisuusrikkomuksia, koska suurin osa rikkomuksista syntyy tietämättömyyden takia. (Gaudin 2009.) Ohjeistukset on syytä olla niin selkeät, että kuka tahansa aikuinen osaa niiden avulla toimia. Tämä saavutetaan käyttämällä paljon käytännön esimerkkejä. (Rousku, 22.)

11.1.1 Käyttäjätunnusvarkaudet

Verkko on täynnä erilaisia palveluita, jotka vaativat salasanan. Jokainen verkkopalvelu vaatii omansa. Tästä johtuen on usein vaikeaa keksiä uusia salasanoja jokaiselle eri palvelulle. Useimmiten tietotekniikkaa vähemmän käyttäneet henkilöt tai henkilöt, jotka eivät ole perehtyneet tietoturvallisuuteen, antavat salasanaksi helposti arvattavan sanan. Yleisimpiä helposti arvattavia salasanoja ovat lasten nimet ja syntymäajat, lemmikkieläinten nimet, tyttönimet ja yksinkertaiset kirjain- ja numeroyhdistelmät kuten ”a1b2c3”. Kyseistä salasanaa saatetaan käyttää jokaisessa kirjautumista vaativassa palvelussa. (Aalto ym. 2009, 21–22.) Sosiaalisen mediassa ja muissa palveluissa käytetyt helposti arvattavat salasanat ovat yksi syy, miksi lehdistä saa melko usein lukea tietoturvamurroista.

Ensimmäinen hyvä muistisääntö salasanaa luodessa on, että hyvä salasana sisältää vähintään 8 merkkiä, joista ainakin osa on numeroita ja erikoismerkkejä. Salasana on sitä turvallisempi, mitä pidempi se on. (Aalto ym. 2009, 21–22.) Salasanaksi ei koskaan kannata asettaa jotakin tuttua sanaa, joka löytyy sanakirjasta. Toinen hyvä muistisääntö palveluissa käytettävistä salasanoista on, että jokaisessa palvelussa käytetään eri salasanaa, sillä tuskin kukaan käyttäisi samaa avainta kotioveensa ja polkupyöräänsäkään. Mikäli jokaisessa palvelussa käytetään samaa salasanaa, on henkilöllä, joka tietää käyttäjän salasanan yhteen palveluun, helppo päästä kirjautumaan käyttäjän toiseen palveluun. (Aalto ym. 2009, 21–22.)

Salasanat on aina syytä pitää omana tietonaan ja niitä ei kannata jakaa edes puolison tai lasten kanssa. Kenenkään toisen henkilön ei ole syytä kysyä salasanaasi. Esimerkiksi ATK-tukihenkilö tai palveluntarjoaja ei tarvitse käyttäjien salasanoja mihinkään. Mikäli salasanaa jostain syystä kysytään esimerkiksi puhelimitse tai sähköpostitse, ei sitä missään nimessä kannata antaa. Salasanaa ei myöskään kannata kirjoittaa mihinkään, minne muilla henkilöillä on pääsy, kuten paperilapulle monitorinkulmaan tai laatikkoon. (Aalto ym. 2009, 21–22.) Salasana kannattaa myös vaihtaa säännöllisesti (Lewis).

Selaimen ei kannata antaa tallentaa omia salasanoja, varsinkaan jos samaa tietokonetta käyttää useampi muu henkilö. Muuten seuraava käyttäjä pääsee yhdellä klikkauksella palveluun, jota juuri käytettiin. Lisäksi sosiaalisen median palveluista on syytä muistaa kirjautua ulos sen jälkeen, kun palveluja ei enää tarvitse. (Aalto ym. 2009, 23.) Tietoturvallisuutta parantaakseen on hyvä myös tyhjentää selaimen selailuhistoria ja evästeet silloin, kun tietokoneen käyttö lopetetaan (Tranberg ym. 2013, 225).

Sosiaaliturvatunnusta tai ajokortin lisenssinumeroa ei kannata antaa kenellekään, eikä niitä pidä kirjata sosiaalisen median palveluun. Tiedot, joita itsestään antaa, kannattaa pitää minimaalisena. Syntymäaikaa, kotikaupunkia, kotiosoitetta tai sähköpostiosoitetta ei kannata jakaa julkisesti. Kaveriksi ei kannata lisätä muuta kuin henkilöitä, joita tuntee. Salasanan turvatarkistekysymykseen, kuten mikä on lemmikkisi nimi, kannattaa syöttää jonkinlainen salasana, toisin kuin vain vastata kysymykseen. Näin kannattaa toimia, koska asiaankuulumaton henkilö on saattanut saada lemmikin nimen selville esimerkiksi Facebookin seinäkirjoituksesta tai käyttäjän jakamasta kuvasta. (Lewis.)

Mikäli käyttäjän sosiaalisen median tili on hakkeroitu, kannattaa käyttäjän vaihtaa välittömästi oman tilinsä salasana (Tranberg ym. 2013, 97). Tämän jälkeen avoimet istunnot on syytä sulkea, jotta hakkerin on kirjauduttava uudelleen uhrinsa profiiliin. Uuden salasanan myötä, hakkeri ei enää pääse kirjautumaan uhrinsa sosiaalisen median profiiliin.

11.1.2 Identiteettivarkaudet

Paras tapa suojautua ja ennaltaehkäistä identiteettivarkauksia on omistaa ajan tasalla oleva virustorjuntaohjelma. On myös suositeltavaa päivittää kaikki merkittävät tietokoneohjelmat, jotta parhaillaan tiedossa olevia tietoturva-aukkoja ei löydy. (Oikeusministeriö 2013.) Tietoturva-aukolla tarkoitetaan usein haitallista ohjelmaa, joka pystyy vaikuttamaan tietokoneen toimintaan käyttäjän sitä haluamatta. Käyttöjärjestelmävalmistajat ja ohjelmantarjoajat laativat tällöin ilmaisen päivityksen, joka paikkaa aukon ja tekee ohjelmasta tai käyttöjärjestelmästä jälleen turvallisen. Tietoturva-aukon päivitystiedostoa kutsutaan useimmiten englanniksi sanoilla ”patch” tai ”security update”. (Aalto ym. 2009, 25.)

Tietosuojavaltuutetun toimiston mukaan jo huolellisuudella pystytään ehkäisemään identiteettivarkauksia ennakolta (Aalto ym. 2009, 126). Omassa profiilissa kannattaa asettaa yksityisyysasetukset mahdollisimman tiukoiksi ja miettiä, ketä hyväksyy kaverikseen (Andreasson ym. 2013, 161). Mikäli yrityksestä tai yksityishenkilöstä on luotu valeprofiili, saa sen helpoiten poistettua ottamalla yhteyttä palvelun ylläpitoon (Mäkelä 2013).

Kannattaa myös tutustua sosiaalisen median palveluiden tarjoamiin mahdollisuuksiin ilmiantaa ilkivaltainen käyttäjä, koska vaikka toiminta ei olisikaan laitonta, saattaa toiminta olla kuitenkin palvelun käyttöehtoja rikkovaa, ja tämä oikeuttaa palveluntarjoajan katkaisemaan ehtoja rikkoneen käyttäjän pääsyn palveluun (Andreasson ym. 2013, 161).

Vaikka identiteettivarkaus ei ole Suomen lainsäädännössä rangaistava teko, voi se kuitenkin täyttää jonkin toisen rikoksen tunnusmerkit. Näitä ovat: kunnianloukkaus, laiton uhkaus, petos, luvaton käyttö, tietomurto ja viestintäsalaisuuden loukkaus. Jos tekijän toiminta on rinnastettavissa joihinkin edellä mainituista rikosnimikkeistä, kannattaa asiasta olla yhteydessä poliisiin, koska nämä ovat aina rangaistavia tekoja. (Poliisi2.)

11.1.3 Vakoilu ja tietojen kalastelu

Internetiä käyttävien henkilöiden on osattava tunnistaa tietojenkalastelu, jolla rikolliset yrittävät saada haltuun muun muassa yrityssalaisuuksia ja salasanoja. Hyvät tietoturvaohjelmat sisältävät useimmiten tietojen kalastelun eston ja sähköpostiohjelmat roskapostin suodattimen. Tästä huolimatta mikään suojaus ei ole täysin aukoton. On myös hyvä muistaa, että salasanoja ei koskaan kysytä puhelimitse tai sähköpostitse. (Rongas 2012.) Huijaussivuston tunnistaminen saattaa olla joskus vaikeaa. Paras keino on tarkkailla selaimen osoiteriviä, jossa domain-nimi on ratkaisevassa asemassa. Tästä syystä se esitetään Internet-selaimessa tummempana. Joskus valenimi saattaa erota oikeasta vain muutamalla merkillä. Toinen ero oikean ja väärän sivun välillä on ssl-salauksen puuttuminen. Jokainen tärkeä sivusto käyttää palvelinvarmennetta, jonka aitouden selain tarkistaa. Joten jos osoitteen alussa ei ole https-tekstiä, eikä osoiterivillä ole lukon kuvaa, sivu on todennäköisesti huijausta. (Järvinen 2012, 73.)

Sosiaalisen median yksityisyysasetuksia säätämällä hakutoiminnan tuloksia voi rajoittaa, ja näin ollen esimerkiksi paikantamispalvelun keräämät tiedot eivät pääse vuotamaan ulkopuolisille tahoille (MTV3 2013). Kavereiksi kannattaa lisätä vain tuttuja ja luotettavia henkilöitä. Kavereiden luokittelu esimerkiksi työ- ja harrastuskavereihin antaa profiilin omistajalle paremman mahdollisuuden jakaa tietynlaista tietoa vain määrätyille henkilöille. (Haasio 2009, 72.)

11.2 Tekniset uhat

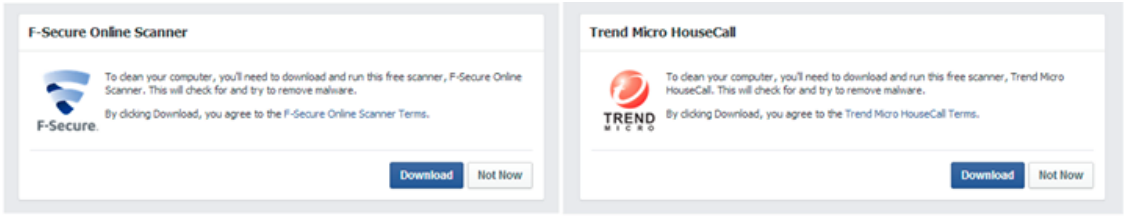
Tässä kappaleessa käydään läpi ratkaisuja jo aiemmin mainittuihin ongelmiin. Aluksi käydään läpi ratkaisuja, joilla sovellushaavoittuvuudet saadaan ehkäistyä parhaalla mahdollisella tavalla. Tämän jälkeen käydään läpi asioita, joilla haittaohjelmat saadaan pidettyä poissa käyttäjän tietokoneelta ja sosiaalisen median palveluista. Lisäksi tässä kappaleessa kerrotaan, millä tavalla toimia Internetissä ja sosiaalisessa mediassa, jotta roskaposteja ei pääse käyttäjän sosiaalisen median palveluihin. Lopuksi kappaleessa kerrotaan, miten roskaposteihin kannattaa reagoida.

11.2.1 Sovellushaavoittuvuudet

Tietoturvasyistä johtuen tietokoneohjelmat, kuten Internet selain kannattaa pitää ajan tasalla. Uudet päivitykset parantavat ohjelman tietoturvaa ja paikkaavat löytyneitä tietoturva-aukkoja. Päivitysten myötä myös laitteiston käytettävyys useimmiten paranee. (Helpson.) Myös virustorjunta ohjelma kannattaa pitää ajan tasalla, koska se ehkäisee virusten ja vakoiluohjelmien pääsyn tietokoneeseen (Viestintävirasto 2014).

Terve epäluulo varsinkin ilmaisia sovelluksia ja palvelua tarjoavan motiiveita kohtaan on paras ratkaisu estää haitallisten sovellusten pääsy laitteeseen tai omiin sosiaalisen median tietoihin. Sovelluksia kopioitaessa on suositeltavaa tarkastella, minkälaisia oikeuksia kyseinen sovellus vaatii. Viestintäministeriön mukaan esimerkiksi mediatoistin, joka tarvitsee lupaa lähettää tietoa käyttäjän nimissä, on joko todella huolimattomasti tai pahat mielessä ohjelmoitu. (Viestintävirasto 2014.)

Toukokuussa vuonna 2014 Facebook otti F-Securen ja Trend Micron kanssa käyttöön vakoiluohjelmien poiston tietokoneelta. Mikäli Facebookiin tulee joko F-Securen tai Trend Micron alla oleva ilmoitus, kannattaa siihen reagoida ja poistaa sen löytämät vakoiluohjelmat välittömästi. (Facebook2 2014.)



Kuva 5 Ilmainen vakoiluohjelman poisto Facebookissa (Facebook2 2014).

Yllä olevan ilmoituksen voi saada silloin, kun Facebook havaitsee laitteen toimivan epäilyttävällä tavalla. Skanneri asennetaan laitteeseen vain ongelman poiston ajaksi, jonka jälkeen se poistuu laitteesta automaattisesti. (Facebook2 2014.)

11.2.2 Haittaohjelmat

Sosiaalisessa mediassa kannattaa aina olla varovainen sovelluksia kopioitaessa tilille, koska ne voivat kerätä paljon tietoa käyttäjästä. Jos sovellus kerää mielestäsi liikaa tietoa itsestäsi, älä kopioi sitä. Tämä ei kuitenkaan aina riitä, koska myös kavereiden lataamat sovellukset, pelit ja Internetsivut vaikuttavat toisten käyttäjien yksityisyyteen. (Cluley 2013.)

Palkitun Computer Security Blogin mukaan siis myös käyttäjän sosiaalisen median kaverien käyttämät sovellukset, pelit ja Internetsivut saavat käyttäjän tiedot, vaikka käyttäjä itse ei kyseisiä asioita olisi edes asentanut itselleen. Tämän voi kuitenkin välttää esimerkiksi Facebookissa menemällä yksityisyysasetuksiin ja valitsemalla asioita, joita käyttäjä ei halua jakaa kolmansille osapuolille. (Cluley 2013.)

Jos tiedetään varmasti, että haittaohjelma on päässyt omaan tai yrityksen sosiaalisen median profiiliin, on syytä vaihtaa profiilin salasana välittömästi. Myös haitalliset sovellukset on syytä poistaa profiilista heti ongelman selvittyä. (Digitoday 2014).

11.2.3 Roskapostit

Sosiaalisessa mediassa toimii hyvin samat perussäännöt, kuin sähköpostissa ja Internetissä (Boquiron). Tämä tarkoittaa muun muassa sitä, että kannattaa aina harkita, mitä linkkejä sosiaalisen median palveluissa avaa. Jos linkissä luvataan helppoa rahaa tai shokeeraava sisältöä, ei sitä kannata avata, koska kyseessä on melko varmasti huijaus. (Hirvonen 2011.) Kannattaa aina lukea julkaisu ja tarkastaa keneltä ja mistä sovelluksesta se tulee. Jos julkaisun sisältöä on vaikea ymmärtää, ei linkkiä kannata avata. Jos linkin avaa, kannattaa katsoa minne linkki vie. Jos linkki vie lupapyyntö-sivulle, on hyvä lukea mihin se pyytää lupaa. Skriptejä ja komentosarjoja ei kannata koskaan kopioida selaimen osoiteriville. (Haasio 2013, 54–55.)

Vaikka tuttu ja luotettava ystävä on ”lisännyt” mielenkiintoisen, mutta arveluttavan linkin, ei sitä kannata avata. Kyseinen ystävä on saattanut saada koneelle vakoiluohjelman, joka käyttää ystävän profiilia linkin jakamiseen. Kyseessä saattaa siis olla roskaposti, joka leviää käyttäjien profiilien välillä ja käyttää ihmisten luottamusta omiin ystäviinsä hyväkseen. (Boquiron.)

Yritysten markkinoinnin kannalta on suositeltavaa, että he eivät päivittäisi jatkuvasti omaa markkinointikanavaansa sosiaalisessa mediassa. Tämä saattaa aiheuttaa käyttäjissä samankaltaisia tunteita kuin roskapostien saanti esimerkiksi sähköpostissa. (Mackey.) Yritysten on kuitenkin oltava aktiivisia omilla kanavillaan, jotta henkilöiden mielenkiinto yritystä ja sen toimintaa kohtaan pysyvät kunnossa. Hyvää aktiivisuutta sosiaalisessa mediassa on mielenkiintoisen tiedon jakaminen ja yritystä koskeviin kysymyksiin vastaaminen. (Korpi 2010, 43–44.)

11.3 Muut uhat

Tässä kappaleessa käydään läpi ratkaisuja, joilla vältetään ikävät yllätykset yrityksen tai sen työntekijän toimiessa sosiaalisessa mediassa. Lisäksi kappaleessa käydään läpi asioita, joilla henkilöturvallisuutta saadaan parannettua ja vältettyä uhkaavat tilanteet. Tämän jälkeen kappaleessa käydään läpi asioita, joilla voidaan parantaa omaa tai yrityksen yksityisyyden suojaa sosiaalisessa mediassa. Lopuksi kerrotaan, miten yrityksen maine pystytään säilyttämään mahdollisimman positiivisena sosiaalisen median aikakaudella.

11.3.1 Palveluiden epäselvät ja muuttuvat sopimusehdot

Ikävät yllätykset palveluiden sopimusehdoissa voidaan välttää lukemalla tarkkaan, mitä kaikkea palvelun käyttö edellyttää sen käyttäjiltä. Sopimusehdoissa määriteltyjä ehtoja on syytä noudattaa palveluita käyttäessä. Yleisesti ottaen sopimusehdot kieltävät sellaisen sisällön julkaisemisen, joka loukkaa tai rikkoo lakia tai jonkun muun oikeuksia. Ehdoissa saatetaan myös edellyttää, että käyttäjä hankkii ja vakuuttaa tällä olevan tarvittavat oikeudet, lisenssit ja muut luvat sisältöön tai sen julkaisemiseen. Käyttäjien on olennaista myös tiedostaa, että valtaosa sosiaalisen median sivustoista sisältää kohdan sopimusehdoissa, joka antaa palveluntarjoajalla käyttöoikeuden sen jäsenten materiaaliin. Tämä antaa palveluntarjoajalle oikeuden lisensoida käyttäjien materiaalia kolmansille osapuolille. (Aalto ym. 2014.)

Sosiaalisen median sopimusehdot on hyvä lukea aina silloin, kun niitä päivitetään. Tämä on erityisen tärkeää silloin, kun yritys käyttää sosiaalista mediaa esimerkiksi markkinointitarkoituksiin. Näin varmistutaan siitä, että yrityksen toimiminen sosiaalisessa mediassa ei ole palveluntarjoajan sääntöjen vastaista. Moni yritys, kuten esimerkiksi SAS on rikkonut sosiaalisen median sopimusehtoja, jonka seurauksena sen täytyi lopettaa sopimusehtoja rikkova kampanja. (Koivumäki & Häkkänen 2014, 101.)

11.3.2 Henkilöturvallisuus

Tietoa itsestään tai yrityksestä ei kannata jakaa liikaa sosiaalisessa mediassa. Esimerkiksi omat osoitetiedot ja puhelinnumerot kannattaa pitää poissa sosiaalisen median palveluista. Tiedot saa toki piilotettua ulkopuolisilta, mutta jos profiilin onnistuu hakkeroimaan ulkopuolinen henkilö, saa hän kaikki profiiliin kirjatut tiedot itselleen. (Wheeler.)

Korkeassa asemassa olevan henkilön kannattaa aina harkita paikantamispalvelun käyttöä, koska se nostaa riskiä joutua rikollisen tai vihamielisen henkilön uhriksi (Wheeler). Tärkeissä luottamustehtävissä paikantamispalvelun käyttö saattaa aiheuttaa suuren turvallisuusriskin. Paikantamispalvelun aktiivinen käyttö paljastaa sen käyttäjän suosimat paikat ja mahdollisesti myös oman koti- ja työosoitteen. Myös paikantamispalvelun tiedot saattavat päätyä samalla tavalla kolmansille osapuolille, kuin käyttäjän omat tiedot. (Wheeler.)

Sosiaalisessa mediassa jaetuista valokuvista on hyvä poistaa aika- ja paikkatiedot, jotta saavutetaan parempi henkilö- ja yksityisyysturvallisuus. Tämä on tärkeää, varsinkin jos kyseisistä tiedoista käy ilmi käyttäjän kotiosoite tai se, että hän ei ole parhaillaan kotona. (Tranberg ym. 2013, 103.) Monet digikamerat ja matkapuhelimet sisältävät paikannustyökalut, jotka saattavat liittää valokuvien metatietoihin tarkat gps-koordinaatit (Andreasson ym. 2013, 160). Sosiaalisessa mediassa ei ole myöskään viisasta kertoa lomasuunnitelmista, eikä loman ajankohdasta (Tranberg ym. 2013, 228).

Pelkästään tietosuoja-asetuksia muuttamalla, saadaan sosiaalisen median palvelusta parannettua henkilöturvallisuutta ja radikaalisesti vähennettyä mahdollisten uhkien syntyminen. Liian heikot tietosuoja-asetukset ovat suurin syy, miksi esimerkiksi varkaiden sosiaalisen median palveluita hyödyntäviä murtoja pääsee syntymään. (Andreasson ym. 2013, 159.)

11.3.3 Yksityisyyden suoja

Yksityisyysasetukset kannattaa aina asettaa niin, että vain luotettavat kaverit ja yhteistyökumppanit saavat sosiaalisessa mediassa jaetut asiat. Vaikka jotkut henkilöt ajattelevat että heillä ei ole mitään salattavaa, on aina mahdollista joutua esimerkiksi identiteettivarkauden uhriksi. (Myllyoja 2013.)

Silloin, kun sosiaalisen median palveluita tarjoava yritys päivittää palveluaan, on syytä tarkastaa mitä kaikkea uusi päivitys pitää sisällään. Tämän lisäksi kannattaa tarkistaa yksityisyysasetukset jokaisen päivityksen jälkeen, jotta mikään yksityinen viesti, kuva tai muu materiaali ei ole vaihtunut päivityksen myötä julkiseksi. Esimerkiksi Facebook on tähän mennessä aiheuttanut monelle sen käyttäjälle harmia monilla yllättävillä muutoksella, ja lisää on todennäköisesti vielä tulossa (Juslén 2010).

Monissa sosiaalisen median palveluissa saa rajoitettua itsensä lisäämistä kavereiden kuviin ja tilapäivityksiin. Esimerkiksi Facebookin asetuksista on mahdollista ottaa julkaisujen esikatselu käyttöön. Esikatselulla voidaan joko hyväksyä tai hylkää kaverien tekemät lisäykset. Tämän lisäksi esikatselulla voidaan rajata sitä, kuka julkaisun näkee. (Facebook4 2014.) Henkilöstölain yksityisyyden suoja koskee myös verkossa jaettuja valokuvia. Tämä tarkoittaa sitä, että on lainvastaista julkaista toisesta ihmisestä kuvia ilman hänen lupaansa. Yksityisyyden suoja on osittain voimassa silloin, kun kuvaan lisätty henkilö on tunnistettavissa. Mikäli kuvan yhteydessä julkaistaan vielä kohteen nimi, henkilöstölain tunnusmerkit täyttyvät varmasti. Jos käyttäjästä julkaistaan kuva ilman hänen suostumustaan, voi hän pyytää henkilöä poistamaan kuvan. Jos hän ei suostu poistamaan kuvaa, voidaan ottaa yhteyttä palvelun ylläpitäjään ja vaatia kuvan poistoa. Kyseiset säädökset eivät tosin koske tiedotusvälineitä, journalismia, eikä taiteellisia tarkoituksia. (Aalto ym. 2009, 140–141.)

Facebookiin ja Twitteriin on luotu suojatun yhteyden (HTTPS) mahdollisuus, jonka saa käyttöön asetuksista. Suojattu yhteys mahdollistaa turvallisemman toimimisen palveluissa, koska liikenne on salattua. (Boquiron.)

Yritysmaailmassa on tärkeää pitää huolta, että mikään kallisarvoinen tieto ei pääse vuotamaan yrityksen ulkopuolelle. Jokaista työntekijää on hyvä muistuttaa yksityisyyden suojaamisesta. (Koikkalainen.) Jokaisen henkilön tulee kuitenkin itse huolehtia omasta yksityisyyden suojasta sosiaalisen median palveluita käyttäessä (Etelä-Pohjanmaan sairaanhoitopiirin kuntayhtymä).

11.3.4 Maineen hallinta

Yrityksen toimiessa sosiaalisessa mediassa on sen valmiussuunnitelmat syytä suunnitella hyvin. Maineenhallintaan on tarjolla erilaisia työkaluja, joilla kyetään tarkkailemaan ja arvioimaan sosiaalisen median vaikutuksia yrityksen imagoon. Ennakoivat analyyttiset työkalut helpottavat negatiivisten viestien sisällön ja mahdollisten uhkien arviointia sosiaalisessa mediassa. Riskiarvioiden avulla yritysjohto voi valita ne ennalta päätetyt tavat, joilla erilaisiin uhkiin reagoidaan. (Pervilä 2010.)

Sosiaalisessa mediassa asiakaspalvelu on kuuntelua, reagointia ja nopeutta. Lisäksi se on ennen kaikkea suhteiden ja luottamuksen rakentamista. Silloin, kun organisaatio vastaa, se kuuntelee. Silloin, kun se vastaa nopeasti, se välittää. Jos organisaatio ei vastaa, sen sosiaalisesta kanavasta saattaa tulla purnaamisen taistelutanner. (Forsgård ym. 2010, 41–42.)

Tästä syystä yritystä, sen tuotetta tai palvelua koskevaan kritiikkiin kannattaa aina vastata rehellisesti, nopeasti ja rakentavasti. Kritiikki saadaan muutettua voitoksi hyvittämällä julkisesti kaikkia, jotka ovat kärsineet kritiikin kohteena olevasta puutteesta. Yrityksen kommentointi vaikeina aikoina osoittaa asiakkaalle, että yritys hoitaa asiansa hyvin ja henkilökohtaisesti. (Korpi 2010, 64–66.)

Tämä lisää yrityksen uskottavuutta ja toiminnan läpinäkyvyyttä. Avoin viestintä on yrityksen kannalta pitkässä juoksussa parempi vaihtoehto piileskelyyn verrattuna. (Korpi 2010, 66.) Mikäli yrityksellä ei ole mahdollisuutta, resursseja tai halua avoimeen ja monimuotoiseen vuorovaikutukseen, on viisainta pysyä poissa sosiaalisen median palveluista (Forsgård ym. 2010, 46). Lisäksi työ- ja yksityisroolit on syytä tehdä itselle ja muille selväksi sosiaalisessa mediassa.

12 Yhteenveto

Sosiaalinen media on muuttanut merkittävästi nyky-yhteiskuntaa ja ihmisten päivittäistä elämää sekä tapaa käsitellä ja julkaista tietoa. Samalla se on luonut uusia ihmisten yksityisyyteen ja tiedon luottamuksellisuuteen liittyviä riskitekijöitä. Se on myös avannut uusia ovia verkkorikollisuudelle.

Useimmilta sosiaalisen median riskeiltä on mahdollista suojautua toimimalla siellä harkiten. Ihmiset ovat luonteeltaan uteliaita ja tämä motivoi vahvasti varomattomuuteen. Keskeisimmät riskit sosiaalisen median käytössä luovat siis käyttäjät itse. Ei pidä kuitenkaan unohtaa keskittynyttä rikollisuutta, jota usein ilmenee siellä, missä on paljon varastettavaa eli sosiaalisessa mediassa käyttäjiä. Facebookissa ilmenee kaikkein eniten kysymyksiä sen tietoturvasta. Tämä ei sinänsä ole mikään ihme ottaen huomioon aktiivisten käyttäjien määrän, sen käyttötarkoituksen ja kaikenlaiset lisäsovellukset, joita Facebook on pullollaan. Sangen moni Facebookin aktiivinen käyttäjä pitää ulkopuolisia sovelluksia Facebookin yhtenä suurimmista tietoturvariskinä. On syytä muistaa, että myös kännykällä ja tabletilla toimiessa samat tietoturvariskit ovat myös olemassa. Sosiaalisen median palvelut ovat kännykällä ja tabletilla vain pienennetty kyseisiin laitteisiin sopiviksi.

Opinnäytetyön ensimmäisenä tutkimuskysymyksenä oli, minkälaisia riskejä sosiaalinen media saattaa tuoda yrityksille. Kysymyksen tarkastelu aloitettiin kartoittamalla keskeisimpiä ongelmakohtia sosiaalisen median palveluissa. Pääpaino tutkimuksessa oli kuitenkin selvittää vakavampia riskitekijöitä, joita sosiaalinen media saattaa aiheuttaa yrityksille ja sen työntekijöille. Tutkimuskysymystä tarkasteltaessa huomattiin, että riskitekijöitä löytyi useita. Keskeisimmät uhat sosiaalisen mediassa johtuvat ihmisten varomattomasta ja huolimattomasta palvelun käytöstä sekä sosiaalisuuden tarpeesta. Keskeisimmät riskit sosiaalisessa mediassa aiheuttavat verkossa toimivat rikolliset. Myös käyttäjien liiallinen turvallisuuden tunne saattaa aiheuttaa erilaisia riskejä sosiaalisessa mediassa.

Opinnäytetyön toisena tutkimuskysymyksenä oli, miten yritykset ja sen työntekijät voivat suojautua sosiaalisen median riskeiltä. Kysymykseen haettiin vastausta käyttämällä ensimmäisestä tutkimuskysymyksestä ilmi käyneitä ongelmia. Vastaukset toiseen tutkimuskysymykseen pyrittiin pitämään melko lyhyinä ja niiden tavoitteena oli löytää ratkaisut vain sosiaalisen median yleisimpiin ja vakavampiin ongelmiin sekä niiden ehkäisyyn ja minimointiin. Jotta yritys osaisi suojautua sosiaalisen median riskeiltä, on sen myönnettävä, että sosiaalisen median riskeiltä ei aina voi välttyä. Paras keino ennaltaehkäistä riskien syntyminen on selkeä ohjeistus työyhteisössä, henkilöstön koulutus ja turvallisuustietoisuuden lisääminen.

Opinnäytetyön kolmantena tutkimuskysymyksenä oli, miksi riskejä pääsee syntymään yritysten ja sen työntekijöidensä toimiessa sosiaalisessa mediassa. Kysymystä varten tarkasteltiin asioita, jotka vaikuttavat yrityksen maineeseen kielteisesti. Tutkimuskysymystä tarkasteltaessa kävi ilmi, että suurin syy, miksi ongelmia syntyy, johtuu yritysten johdon tai sen työntekijöiden huonosta maineenhallinnasta. Lisäksi ongelmiin vaikuttavat yrityksen toiminnalliset strategiat ja ääriryhmien sosiaalinen painostaminen.

Tämä opinnäytetyö antaa lukuisia vaihtoehtoja jatkotutkimuksille. Tässä opinnäytetyössä lähtökohtana oli tarkistella sosiaalisen median tuomia riskejä yrityksille ja niiden työntekijöille. Opinnäytetyössä tutkittiin sosiaalisen median ongelmia pääasiassa Facebookin, YouTuben ja Twitterin näkökulmasta. Jatkotutkimuksessa tarkastelun kohteena voisivat olla jotkin muut sosiaalisen median palvelut. Lisäksi sosiaalisen median hyödyt yritysmaailmaa ajatellen voisi olla mielenkiintoinen jatkotutkimuksen aihe. Myös hakukoneiden toiminnallisuuksien ja niiden käytön tarkastelu yritysten liiketoiminnassa, saattaisi tuoda uutta ja mielenkiintoista tietoa. Tutkimuksessa voitaisiin analysoida muun muassa sitä, miten yritykset voisivat tuoda lisää näkyvyyttä omalle yritykselleen.

Sosiaalinen media on laaja käsite, joka sisältää paljon muitakin palveluita kuin ne, mihin tässä opinnäytetyössä keskityttiin. Valitsin työn aiheeksi sosiaalisen median, koska se on edelleen melko uusi ja ajankohtainen aihe. Samasta syystä keskityin tässä työssä Facebookin, Twitterin, LinkedIn:in, YouTuben ja keskustelufoorumien tarkastelemiseen. Päätin kirjoittaa sosiaalisen median uhista ja haitoista yritysten ja työntekijöiden näkökulmasta, koska mielestäni kyseisestä näkökulmasta ei ole vielä kirjoitettu muutamien artikkelin lisäksi kovinkaan kattavia raportteja tai kirjoja.

Lopullisessa opinnäytetyössä käytetty aineisto on vain murto-osa siitä kokonaisuudesta, mitä tämän työn aikana on käsitelty. Sosiaalisesta mediasta ja sen hyödyistä organisaatioille on kirjoitettu melko paljon kirjallisuutta, mutta sen tuomista riskeistä ja uhista melko suppeasti. Opinnäytetyön rajaamisen takia jouduin jättämään aluksi hyvältä vaikuttavia kirjoja ja muita lähteitä pois lopullisesta työstä.

Lähivuosina on paljon keskusteltu uudenlaisista tietoturvaongelmista, jotka johtuvat muun muassa yritysten omista työntekijöistä. He muun muassa jakavat yrityssalaisuuksia ja kritisoivat omia työnantajiansa. Tämä herättää muutamia kysymyksiä muun muassa siitä, miten sosiaalisen median aikakaudella työntekijöitä ohjeistetaan sen käytössä. Ovatko yritykset tehneet minkäänlaisia ohjeita työntekijöilleen siitä, mitä he saavat jakaa yrityksestä ja mitä eivät? Varmasti kuitenkin jokainen työnantaja tekee työntekijänsä kanssa salassapitosopimuksen. Lisäksi lojaalivelvollisuudet ovat luonnollisesti voimassa missä tahansa tilanteessa. Joten voidaankin kysyä, miten näin pääsee käymään? Johtuuko esimerkiksi yrityssalaisuuksien leviäminen vain siitä, että sosiaalinen median käyttö on avointa ja nopeaa? Vai voiko taustalla olla joitakin muita syitä? Näihin kysymyksiin tuskin on mahdollista saada lyhyttä ja yksinkertaista vastausta. Jokainen tapaus on omanlaisensa. Varmasti osassa tapauksissa yritystenkin toiminnassa on saattanut olla jotakin ongelmaa, ei vain sen työntekijöissä.

Tämän työn tarkoitus ei ole olla kattava ja sisältää kaikki varteenotettavat sosiaalisen median ongelmat, vaan sen tarkoitus on olla helposti lähestyttävä ja toimia herättävänä kirjoituksena siitä, että turvallisuusasioihin on syytä kiinnittää huomiota myös sosiaalisessa mediassa toimiessa.

Vaikka sosiaalinen media sisältääkin paljon uhkatekijöitä, on se siitä huolimatta erinomainen palveluympäristö niin yritysmaailmassa kuin normaalissa yksityiskäytössä. Kuten tämä opinnäytetyö osoittaa, sosiaalisessa mediassa on toimittava harkiten ja jakaa vain asioista, joista voisi missä tahansa ja kenelle tahansa kertoa.

Lähteet

Aalto, S., Liesvirta, P. 2014. Viitattu 30.11.2014. Sosiaalisen median sudenkuopat. http://www.iprinfo.com/julkaisut/iprinfo-lehti/lehtiarkisto/2013/IPRinfo_4_2013/fi_FI/sosiaalinen_media/

Aalto, T. 2012. Kuinka olla avoin: työelämän uudet viestintätaidot. Oy Finn Lectura Ab.

Aalto, T., Yoe Uusisaari, M. 2009. Nettielämää. Jyväskylä: Gummerus Kirjapaino.

Aalto, T., Yoe Uusisaari, M. 2010. Löydy: Brändää itsesi verkossa. Vantaa: Hansaprint Oy.

Aboujaoude, E. 2011. Virtually You. New York: W. W. Norton & Company, Inc.

Adrian, A. 2009. The Internet for the Older and Wiser. United Kingdom: John Wiley & Sons, Ltd.

Ajankohtaista Uskosta. 2013. Viitattu 27.11.2014. Facebook - uhka yksityisyydelle. https://ajankohtainen.wordpress.com/category/isoveli-valvoo-2/

Andreasson, A., Koivisto, J. 2013. Tietoturvaa toteuttamassa. Helsinki: Tietosanoma Oy.

Anttila, P. 1998. Viitattu 25.2.2015. Tutkimuksen eettiset kysymykset. http://www.metodix.com/fi/sisallys/01_menetelmat/01_tutkimusprosessi/02_tutkimisen_taito_ja_tiedon_hankinta/11_tutkimuksen_eettiset_kysymykset/

Boquiron, R. Viitattu 4.12.2014. Spam, Scams and Other Social Media Threats. http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/75/spam-scams-and-other-social-media-threats

Candolin, C. 2011. Viitattu 3.12.2014. Virkamiehenä verkossa. http://www.slideshare.net/THLfi/virkamiehen-verkossa

Carlson, N. 2011. Viitattu 3.9.2014. The Real History of Twitter. http://www.businessinsider.com/how-twitter-was-founded-2011-4

Cavazza, F. 2008. Viitattu 11.11.2014. Social Media Landscape. http://www.fredcavazza.net/2008/06/09/social-media-landscape/

Cluley, G. 2013. Viitattu 4.12.2014. How to stop your friends' Facebook apps from accessing *your* private information. https://nakedsecurity.sophos.com/2013/04/03/how-to-stop-your-friends-facebook-apps-from-accessing-your-private-information/

Coleman, B. 2013. Viitattu 26.5.2014. Social Media #Fails Every Company Should Learn From. http://www.searchenginejournal.com/social-media-fails-every-company-should-learn-from/63031

Cooke, T. 2011. Help! I'm a Facebookaholic: Inside the Crazy World of Social Networking. London: John Blake Publishing Ltd.

Dickey, M. 2013. Viitattu 28.7.2014. The 22 Key Turning Points In The History Of YouTube. http://www.businessinsider.com/key-turning-points-history-of-youtube-2013-2?op=1

Digitoday. 2014. Viitattu 28.11.2014. Nyt tarkkana: Facebookin värihuijaus teki paluun. http://www.digitoday.fi/tietoturva/2014/08/11/nyt-tarkkana-facebookin-varihuijaus-teki-paluun/201411114/66?rss=6

Etelä-Pohjanmaan sairaanhoitopiirin kuntayhtymä. Viitattu 3.12.2014. Sosiaalisen median ohje. http://www.epshp.fi/files/3698/Ohje_sosiaalisesta_mediasta_tyA_ntekijA_ille.pdf

Facebook. 2014. Viitattu 27.11.2014. Haittaohjelmat. https://fi-fi.facebook.com/help/320234818071511/

Facebook2. 2014. Viitattu 28.11.2014. Making malware cleanup easier. https://www.facebook.com/notes/facebook-security/making-malware-cleanup-easier/10152050305685766

Facebook3. 2014. Viitattu 3.12.2014. Merkitseminen. http://fi-fi.facebook.com/help/366702950069221/

Facebook4. 2014. Viitattu 3.12.2014. Miten tarkistelen merkintöjä, joita käyttäjät lisäävät julkaisuihini, ennen kuin ne tulevat näkyviin?. http://fi-fi.facebook.com/help/247746261926036

Facebook5. Viitattu 5.12.2014. Oikeus- ja vastuulauseke. https://www.facebook.com/legal/terms/update

Ferguson, R. 2013. Viitattu 27.11.2014. Suojaa Facebook-tilisi. http://kotimikro.fi/uutiset/tietoturva/nain-suojaat-facebook-tilisi-rikollisilta

Forsgård, C., Frey, J. 2010. Suhde - Sosiaalinen media muuttaa johtamista, markkinointia ja viestintää. Vantaa: Hansaprint Oy.

Gaudin, S. 2009. Viitattu 7.9.2014. Execs Worry That Facebook, Twitter Use Could Lead to Data Leaks. http://www.computerworld.com/article/2526978/web-apps/execs-worry-that-facebook--twitter-use-could-lead-to-data-leaks.html

Haasio, A. 2009. Facebook – opas. Latvia: InPrint.

Haasio, A. 2013. Netin pimeä puoli. Saarijärvi: Saarijärven Offset Oy.

Hakola, E. 2014. Viitattu 4.6.2014. Virasto ryhdistäytyi somessa. http://lehtiarkisto.talentum.com/lehtiarkisto/search/show?eid=2708109

Hannula, A., Morad, L., Järvinen, S., Nikkilä, A., Lievonen, L. Viitattu 28.10.2014. Sosiaalisen median ABC työsuhteet. http://www.oikotie.fi/sites/all/files/Sosiaalisen_median_ABC_-_tyosuhteet_Oikotie_Tyopaikat_ja_Aldea.pdf

Harala, S. 2012. Viitattu 14.10.2014. TS: Verkkorikollisuus lisääntyy tulevaisuudessa. http://yle.fi/uutiset/ts_verkkorikollisuus_lisaantyy_tulevaisuudessa/5051529

Helpson. Viitattu 4.12.2014. Miten käyttöjärjestelmä päivitetään?. http://www.helpson.fi/tietokone-netti/miten-ohjelmisto-ongelmat-ratkaistaan/miten-kayttojarjestelma-paivitetaan

Hirsjärvi, S., Remes, P., Sajavaara, P. 2012. Tutki ja kirjoita. 15. Painos. Hämeenlinna: Karis-ton Kirjapaino Oy.

Hirvonen, S. 2011. Viitattu 28.11.2014. Sosiaalisen median tietoisku eläkeläisille. http://www.slideshare.net/sirkkulaine/sosiaalisen-median-tietoisku-elkelisille

The Huffington Post. 2012. Viitattu 26.5.2014. Volkswagen's Social Media Fail: Car Firm Engages Facebook Users – Then 'Deletes Unfavourable Comments'. http://www.huffingtonpost.com/2012/01/10/volkswagens-social-media-facebook-_n_1196745.html

Hämäläinen, P., Heikkilä, J. 2011. Sosiaalisen median käytön ohjeistus. Tampere: VTT.

Inspirans. Viitattu 5.1.2015. Mitä laadullinen tutkimus on ?. http://www.inspirans.fi/laadullinen-tutkimus

Interpol. Viitattu 5.11.2014. Cybercrime. http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

Isokangas, A., Kankkunen, P. 2011. Suora yhteys: Näin sosiaalinen media muuttaa yritykset. Helsinki: Unigrafia Oy.

It-viikko. 2006. Viitattu 28.7.2014. Google torjuu YouTube-käräjöintiä neuvotteluin. http://www.itviikko.fi/talous/2006/11/06/google-torjuu-youtube-karajointia-neuvotteluin/200619780/7

Jarmas, T. Viitattu 3.12.2014. Maltti on valttia myös sosiaalisessa mediassa. http://www.eilakaisla.fi/eilakaisla_asiakkaalle/blogit/blogi-maltti-on-valttia-myos-sosiaalises

Juslén, J. 2010. Viitattu 19.5.2014. Kun yrityksen Facebook-sivusta tuleekin painajainen. http://akatemia.fi/2010/03/kun-yrityksen-facebook-sivusta-tuleekin-painajainen

Jyväskylän kristillinen opisto. 2013. Viitattu 7.11.2014. SOME-ohjeet. http://www.peda.net/veraja/jko/opo/yhteisetkaytannot/some

Järvinen, P. 2012. Arjen tietoturva. Saarijärvi: Saarjärven Offset Oy.

Kareinen, A. 2013. Viitattu 18.11.2014. Sosiaalinen media oppilaitoksen arjessa. http://www.theseus.fi/bitstream/handle/10024/65448/Kareinen_Anne.pdf?sequence=1

Karppinen, K., Matikainen, J. 2012. Julkisuus ja demokratia. Jyväskylä: Bookwell Oy.

Kivimäki, P. 2012. Viitattu 3.9.2014. Hashtag on tunniste. http://yle.fi/uutiset/hashtag_on_tunniste/6351631

Koikkalainen, J. Viitattu 3.12.2014. Joko teillä on sosiaalisen median pelisäännöt?. http://www.dagmar.fi/uutiset/joko-teill%C3%A4-sosiaalisen-median-pelis%C3%A4%C3%A4nn%C3%B6t

Koistinen, O. 2013. Viitattu 28.7.2014. Puoli miljoonaa suomalaista käyttää LinkedIniä - onko siitä hyötyä?. http://www.hs.fi/tyoelama/a1386442273928

Koivumäki, E., Häkkänen, P. 2012. Markkinointijuridiikka 2012. Jyväskylä: Bookwell Oy.

Koivumäki, E., Häkkänen, P. 2013. Markkinointijuridiikka 2013. Jyväskylä: Bookwell Oy.

Koivumäki, E., Häkkänen, P. 2014. Markkinointijuridiikka 2014. Porvoo: Bookwell Oy.

Korpi, T. 2010. Älä keskeytä mua! – Markkinointi sosiaalisessa mediassa. Tampere: Werkkom-merz.

Koskennurmi-Sivonen, R. Viitattu 24.2.2015. Tapaustutkimus. http://www.helsinki.fi/~rkosken/tapaus

Kreus, J. Viitattu 3.12.2014. Henkilöturvallisuus. http://johtaminen.kauppalehti.fi/book/turvallisuuden-hallinta/turvallisuus-ja-riskit/henkiloturvallisuus

Kuula, A. Viitattu 4.1.2015. Toimintatutkimus. http://www.fsd.uta.fi/menetelmaopetus/kvali/L5_4.html

Laaksonen, S-M., Matikainen, J., Tikka, M. 2013. Otteita verkosta - Verkon ja sosiaalisen median tutkimusmenetelmät. Jyväskylä: Bookwell Oy.

Lakiasiaintoimisto Fiducius Oy. 2014. Viitattu 19.11.2014. Onko identiteettivarkaus rikos?. https://fiducius.fi/onko-identiteettivarkaus-rikos/

Lapintie, L. 2014. Viitattu 17.10.2014. Varo tätä verkkokahvilassa - puudeli vie käyttäjätunnuksesi. http://www.iltalehti.fi/digi/2014101518747125_du.shtml

Laurio, J-M. 2009. Viitattu 3.12.2014. MI6-pomon vaimo laittoi perhekuvat kaikkien nähtäville. http://www.mpc.fi/kaikki_uutiset/article306301.ece

Lewis, K. Viitattu 18.11.2014. How Social Media Networks Facilitate Identity Theft and Fraud. http://www.eonetwork.org/octane-magazine/special-features/social-media-networks-facilitate-identity-theft-fraud

Liekki, T. 2014. Viitattu 19.11.2014. Tällaisia ovat suomalaisiin kohdistuvat identiteettivarkaudet – ”Harvemmin nämä selviävät”. http://yle.fi/uutiset/tallaisia_ovat_suomalaisiin_kohdistuvat_identiteettivarkaudet__harvemmin_nama_selviavat/7303477

Limnéll, J., Majewski, K., Salminen, M. 2014. Kyberturvallisuus. Saarijärvi: Saarijärven Offset Oy.

LinkedIn. 2014. Viitattu 28.7.2014. http://www.linkedin.com/about-us?trk=hb_ft_about
Lyytikäinen, S. 2010. Viitattu 28.11.2014. http://www.tivi.fi/kaikki_uutiset/facebookissa+liikkuu+roskapostia+kolme+kertaa+enemman+kuin+twitterissa/a752103?service=mobile&page=5

Linturi, H. 2003. Viitattu 4.1.2015. Toimintatutkimus. http://www.futunet.org/fi/materiaalit/metodit/2_metodit/5_actix?C:D

MacArthur, A. Viitattu 3.9.2014. The Real History of Twitter, in Brief. http://twitter.about.com/od/Twitter-Basics/a/The-Real-History-Of-Twitter-In-Brief.htm

Mackey, J. Viitattu 5.12.2014. Social Networking Spam - 5 Rules for Marketers. http://www.convinceandconvert.com/guest-posts/social-networking-spam-5-rules-for-marketers/

Mainostajien Liitto. 2012. Klikkaa tästä – Internetmarkkinoinnin käsikirja 2.0. Vaasa: KTMP / Ykkös-Offset.

Marttinen, M. 2014. Viitattu 3.12.2014. Maineenhallinta sosiaalisen median aikakaudella. http://mslgroup.fi/news/maineenhallinta-sosiaalisen-median-aikakaudella/

Meriranta, M. 2010. Mediakasvatuksen käsikirja. EU: UNIpress.

MTV3. 2013. Viitattu 27.11.2014. Uusi Facebook-haku hämmästyttää: Paljastaa arkaluontoisia tietoja. http://www.mtv.fi/uutiset/it/artikkeli/uusi-facebook-haku-hammastyttaa-paljastaa-arkaluontoisia-tietoja/1798402

Myllyoja, N. 2013. Viitattu 4.6.2014. Pelko kasvaa: väärä kommentti somessa vie työpaikan. http://lehtiarkisto.talentum.com/lehtiarkisto/search/show?eid=2611020

Mäkelä, P. 2013. Viitattu 19.11.2014. Käytössäännöt. http://www.slideshare.net/PauliinaMakela/icf-1452013-kaytossaannot

Niemelä, M. 2012. Puheenvuoroja yrittäjyyden opetuksesta ja sosiaalisesta mediasta. Vaasa: Mustasaaren Painotalo Oy.

Nikulainen, K. 2007. Viitattu 27.11.2014. Tietojenkalastelu vähenee, haittaohjelmat tilalle. http://www.digitoday.fi/tietoturva/2007/04/19/tietojenkalastelu-vahenee-haittaohjelmat-tilalle/20079466/66

Nurmi, E. 2013. Viitattu 3.9.2014. Risuaita, ruutu ja hashtag eli kuinka #-merkki päätyi elämäämme. http://yle.fi/uutiset/risuaita_ruutu_ja_hashtag_eli_kuinka_-merkki_paatyi_elamaamme/6686797

Otala, L., Pöysti, K. 2008. Wikimaniaa yrityksiin: Yritys 2.0 tuottamaan. Porvoo: WS Bookwell Oy.

Pelgrin, W. 2013. Viitattu 7.11.2014. 3 reasons why criminals exploit social networks (and tips to avoid getting scammed). http://www.csoonline.com/article/2133563/social-engineering/3-reasons-why-criminals-exploit-social-networks--and-tips-to-avoid-getting-scamme.html

Pervilä, M. 2010. Viitattu 9.12.2014. Maineenhallinta on CIO:n uusi työkenttä. http://www.tivi.fi/cio/maineenhallinta+on+cion+uusi+tyokentta/a960837?service=mobile&page=3

Pesonen, P. 2012. Yritysviestinnän säännöt. Jyväskylä: Bookwell Oy.

Pesonen, P. 2013. Sosiaalisen median lait. Viro: Meedia Zone Oű.

Pihlajarinne, T. 2012. Internetvälittäjä ja tekijänoikeuden loukkaus. Vantaa: Hansaprint Oy.

Piippo, J. 2013. Viitattu 24.2.2015. Toimintatutkimuksen laatukriteerit ja niiden soveltaminen osallistuvan innovaatiotoiminnan johtamisen tutkimisessa. http://www.researchgate.net/publication/259842892_Toimintatutkimuksen_laatukriteerit_ja_niiden_soveltaminen_osallistuvan_innovaatiotoiminnan_johtamisen_tutkimisessa

Pitkänen, P. 2010. Viitattu 19.5.2014. Nestlé pahensi pr-ongelmiaan Facebook-uhkailulla. http://www.digitoday.fi/yhteiskunta/2010/03/24/nestl-pahensi-pr-ongelmiaan-facebook-uhkailulla/20104288/66

Poliisi1. Viitattu 5.11.2014. Tietotekniikkarikollisuus. https://www.poliisi.fi/poliisi/krp/home.nsf/pages/63B3FC75928EFB7EC2256C8B0043A41E

Poliisi2. Viitattu 19.11.2014. Identiteettivarkaudet. https://www.poliisi.fi/poliisi/helsinki/home.nsf/pages/4AA4B4D403026EC2C2257A7E0034F614?opendocument

Puolustusvoimat. Viitattu 27.11.2014. Sosiaalisen median ohjeet. http://www.puolustusvoimat.fi/wcm/af105c004a98546a8138ebe337ad1452/some_ohjeistus.pdf?MOD=AJPERES

Qing, Y. 2010. Viitattu 8.9.2014. Top 5 social networking business threats. http://www.zdnet.com/top-5-social-networking-business-threats-2062060912/

Rautanen, K. 2011. Aineettomien riskien hallinta johdon työkaluna. WSOYpro Oy.

Ridell, S. 2011. Elämää Facebookin ihmemaassa. Tampere: Juvenes Print - Tampereen yliopistopaino Oy.

Rinta, N. 2011. Viitattu 28.11.2014. Yrityksen viisi suurinta sosiaalisen median tietoturvauhkaa. http://www.tivi.fi/kaikki_uutiset/yrityksen+viisi+suurinta+sosiaalisen+median+tietoturvauhkaa/a635238

Rongas, A. 2012. Viitattu 19.11.2014. Hyvät toimintatavat. http://www.edu.fi/materiaaleja_ja_tyotapoja/tvt_opetuksessa/mika_ihmeen_sosiaalinen_media/hyvat_toimintatavat

Rouse, M. 2011. Viitattu 7.11.2014. Spear phishing. http://searchsecurity.techtarget.com/definition/spear-phishing

Rousku, K. Tietoturva-asetus ja VIPin tietoturvapalvelut. Valtiokonttori.

Saaranen-Kauppinen, A., Puusniekka, A. Viitattu 6.1.2015. Mitä laadullinen tutkimus on: lyhyt oppimäärä. http://www.fsd.uta.fi/menetelmaopetus/kvali/L1_2.html

Sandle, P., Char, P. 2014. Viitattu 5.11.2014. Cyber crime costs global economy $445 billion a year: report. http://www.reuters.com/article/2014/06/09/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609

Scott, T. 2013. Viitattu 27.11.2014. Actual Facebook Graph Searches. http://actualfacebookgraphsearches.tumblr.com/

Seeck, H. 2009. Kriisit ja työyhteisöt - kriisijohtaminen työyhteisöjen tukena. Tampere: Tampereen yliopistopaino Oy - Juvenes Print.

Seppänen, J., Väliverronen, E. 2014. Mediayhteiskunta. 3. Painos Tallinna: Raamatutrükikoda.

Sivustot.info. 2012. Viitattu 22.12.2014. Suomi24 keskustelu. http://www.sivustot.info/detail/link-469.html

Solis, B., JESS3. Viitattu 15.1.2015. The Conversation Prism. https://conversationprism.com/

Sophos. Viitattu 28.11.2014. An Introduction to Social Networking – Applications for IT Managers. http://www.sophos.com/en-us/security-news-trends/security-hubs/social-networks/social-networks-article.aspx

Suomen Kuntaliitto. 2010. Kuntien verkkoviestintäohje. Helsinki: Hakapaino Oy.

Suomen Riskienhallintayhdistys ry. Viitattu 23.2.2015. SRHY-riskienhallinta.

Suomi24. 2014. Viitattu 22.12.2014. Perustiedot. http://www.suomi24.fi/yhteis%C3%B6/suomi24/#page=126

Suominen, J., Östman, S., Saarikoski, P., Turtiainen, R. 2013. Sosiaalisen median lyhyt historia. Tallinna: Tallinna Raamatutrükikoja OÜ.

Takala, M. 2014. Viitattu 14.10.2014. Verkkorikollisuus muutti muotoaan - tietokoneita putsattiin Suomessa nelinkertainen määrä. http://www.iltasanomat.fi/digi/art-1288686837163.html#comments-anchor

Talouselämä. 2013. Viitattu 30.11.2014. Facebook poisti käyttäjiltä mahdollisuuden piiloutua hakutuloksilta. http://www.talouselama.fi/uutiset/facebook+poisti+kayttajilta+mahdollisuuden+piiloutua+hakutuloksista/a2164438?s=r

Tampere konsernihallinto. 2013. Viitattu 18.11.2014. Konsernimääräys. http://www.tampere.fi/material/attachments/t/69i5KPHYy/Konsernimaarays_sosiaalisen_median_kaytto13.pdf

Tapscott, D. 2010. Syntynyt digiaikaan. Porvoo: WS Bookwell.

Ternisien, N. 2010. Viitattu 28.7.2014. Forum Software Timeline 1994 - 2012. http://www.forum-software.org/forum-software-timeline-from-1994-to-today

Thorslund, E. 2009. Nuoret, netti j@ mobiili – kodin turvaopas. Hämeenlinna: Kariston Kirjapaino Oy.

Tilastokeskus. 2014. Viitattu 4.1.2015. Yritysten käyttämät sosiaaliset mediat 2014. http://www.stat.fi/til/icte/2014/icte_2014_2014-11-25_tau_002_fi.html

Tranberg, P., Heuer, S. 2013. Älä kerro kaikkea! – Itsepuolustusopas verkkoon. Helsinki: Talentum.

Tuominen, P. 2013. Virtuaalimaine. Helsinki: Talentum.

Tuominen, P. 2014. Viitattu 28.7.2014. LinkedIn Suomessa Infograafi. http://www.slideshare.net/tuominenjaripekka/linkedin-suomessa-infograafi-digipeople

Twitter. 2014. Company. https://about.twitter.com/company

Työsuojeluhallinto. 2014. Viitattu 23.2.2015. Riskien arvionti. http://www.tyosuojelu.fi/fi/riskienarviointi

Vesterinen, P., Suutarinen, M. 2011. Y-sukupolvi työ(elämä)ssä. Vantaa: Hansaprint Oy.

Viestintävirasto. 2014. Viitattu 28.11.2014. Huijaavat sovellukset. https://www.viestintavirasto.fi/tietoturva/tietoturvanyt/2014/08/ttn201408191156.html

Web Wise Business News. Viitattu 27.11.2014. Please Rob Me - Why Using Twitter or Facebook Could See Your Insurance Go Up. http://www.webwisebusiness.co.uk/please-rob-me--why-using-twitter-or-facebook-could-see-your-insurance-go-up/tabid/85/article/161/default.aspx

Wheeler, T. Viitattu 2.12.2014. Social Networking Safety. http://www.ncpc.org/topics/internet-safety/social-networking-safety

Wimmer, B. 2014. Viitattu 23.2.2015. Risk vs Threat vs Vulnerability - and Why You Should Know the Differences. http://www.pinkerton.com/blog/risk-vulnerability-threat-differences

WiseGEEK. 2014. Viitattu 14.10.2014. What is Internet Forum?. http://www.wisegeek.org/what-is-an-internet-forum.htm#comments

Yhteislyseon lukio. 2011. Viitattu 19.11.2014. Sosiaalinen media opetuksessa. http://moodle.luku.fi/file.php/1/Veso_5.9.11_LYL_Sosiaalinen_media_koulussa_1_.pdf

YouTube. 2014. Viitattu 28.7.2014. Tietoja YouTubesta. https://www.youtube.com/yt/about/fi/

Kuvat

Taulukot