Pasi Lintusaari

SOSIAALISEN MEDIAN TIETOTURVAUHKIEN ENNALTAEHKÄISY YRITYKSESSÄ

Tietojenkäsittelyn koulutusohjelma

2017

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

SOSIAALISEN MEDIAN TIETOTURVAUHKIEN ENNALTAEHKÄISY YRITYKSESSÄ

Lintusaari, Pasi
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Tammikuu 2017
Ohjaaja: Nuutinen, Petri
Sivumäärä: 73

Asiasanat: sosiaalinen media, tietoturva, riskienhallinta, opastus

---

Tämän työn tarkoituksena oli selvittää yleisellä tasolla sosiaalisten medioiden muodostamat tietoturvauhat yrityksille ja sen pohjalta luoda yleispätevä opas, kuinka yrityksissä voidaan suojautua sosiaalisen median erilaisilta tietoturvauhkilta. Työssä selvitettiin ja tutustuttiin erilaisiin uhkatyyppeihin sekä siihen miten sosiaalisessa mediassa tapahtuva verkkorikollisuus voi vaikuttaa yrityksen tietoturvaan. Työssä myös käsitellään sosiaalisen median eri uhkatyyppien muuttumista viime vuosien aikana, niiden leviämistapoja sekä yhtymäkohtia ns. ”perinteisiin” tietoturvauhkiin.

Työn teoriaosuudessa käsiteltiin sosiaalista mediaa käsitteenä sekä selvitettiin Suomessa käytetyimmät sosiaalisen median palvelut. Teoriaosuudessa tutustuttiin myös yleisimpiin yrityksen tietoturvalle uhkia muodostaviin uhkatyyppeihin, niiden leviämistapoihin sekä riskienhallintaan työelämässä.

Oppaassa asetettiin ensin ideaalitilanne, johon sosiaalisen median tietoturvauhista työntekijöitään ohjeistavan yrityksen tulisi pyrkiä. Tämän jälkeen työssä käsiteltiin asioita, joita yrityksen tietoturvasta vastaavan henkilön tulisi huomioida ennen sosiaalisen median tietoturvaoppaan laatimista, työntekijöiden opastamiseen liittyviä yleisiä huomioita sekä uhkien ennaltaehkäisyyn liittyviä ongelmia.

Oppaassa käytiin kategoria kerrallaan läpi kuinka yrityksessä voitaisiin huomioida eri uhkatyypit, kuinka niiden konkretisoituminen voidaan ennaltaehkäistä mahdollisimman tehokkaasti ja kuinka yrityksessä tulisi reagoida mahdollisesti realisoituneisiin uhkiin.

SECURITY THREATS OF SOCIAL MEDIA AND HOW TO PREVENT THEM IN COMPANIES

Lintusaari, Pasi
Satakunta University of Applied Sciences
Degree Programme in Business Information Technology
January 2017
Supervisor: Nuutinen, Petri
Number of pages: 73

Keywords: social media, data security, risk management, guidance

---

The purpose of this thesis was to find out the security threats of social media for companies and to create a universal guide how to avoid and prepare for them. First, the threat types and how cybercriminality in social media could affect companies cyber security were clarified and familiarized. Also, the work covers the change of threat types, their ways of spreading and confluences to the so called traditional security threats in the social media over the past years.

The theory part of the thesis covers social media as a concept and examines the most used services in Finland. The theory part explores also the most common cyber security threats in social media, how they spread and how to manage the risks in general.

The guide starts with setting up an ideal situation, to which companies that instructs its employees of the security threats of social media should aim at. After that the guide covers things the IT-security correspondent should pay attention to before creating the social media security guide. It also handles what to take into account when guiding employees and what issues prevention of threats may include.

The guide categorises and goes through different threat types, how to notice them and maximize the prevention of threats that social media sheds to an average company. It also addresses different ways to react to realized threats.

SISÄLLYS

1 JOHDANTO

Sosiaalista mediaa ylistetään usein täysin uudenlaisena alustana yritysmaailmassa: se tarjoaa uusia työpaikkoja, se antaa pienillekin yrityksille mahdollisuuden tuoda itsensä parhaassa tapauksessa suurenkin yleisön tietouteen lähes olemattomalla rahallisella panostuksella. Joidenkin mukaan se on muuttanut täysin työntekijöiden tapaa ratkaista arjen ongelmia ja haasteita. Kuten Internetissä yleisestikin, myös sosiaalisessa mediassa on omat varjopuolensa: massojen mukana palveluihin ovat tulleet myös erilaiset huijarit, verkkorikollisuus ja muut tekniset uhat. Tässä työssä käsitellään näitä kyseisiä varjopuolia yrityksen näkökulmasta, minkälaisia uhkia työntekijöiden itsenäinen sekä yrityksen ”virallinen” sosiaalisen median käyttö tuo mukanaan yrityksen tietoturvan kannalta? Työn tarkoituksena on ensin selvittää ja kategorisoida sosiaalisen median yleisimmät tietoturvauhat, jotka voivat uhata yrityksen tietoturvaa. Tämän jälkeen määritellään tavoitteet, joihin yrityksen tulisi sosiaalisen median tietoturvauhilta varautuessaan pyrkiä. Työssä myös käsitellään erilaisia tekijöitä, jotka vaikuttavat sosiaalisen median tietoturvaohjeistuksen suunnitteluun ja valmistelemiseen erityyppisissä organisaatioissa. Lopuksi työssä käydään alussa määritellyt uhkatyypit uudelleen läpi ja pohditaan erilaisia tapoja valmistautua eri uhkatyyppien varalta, kuinka ennaltaehkäistä riskien konkretisoituminen ja miten valmistautua uhkien toteutumiseen.

Työntekijöiden sosiaalisen median käyttö työaikana joko viihde- tai työtarkoituksessa on kasvanut viime vuosina räjähdysmäisesti, joten työssä on otettu huomioon yrityksen virallisten ”sometilien” lisäksi myös työntekijöiden omat, henkilökohtaiset käyttäjätunnukset ja laitteet. Työnantajalle suurin uhka-tekijä sosiaalisessa mediassa onkin oma työntekijä, joka joko tarkoituksella tai tarkoituksettomasti paljastaa yrityssalaisuuksia tai lataa Facebookissa näkemänsä huijauslinkin kautta haittaohjelman työ- ja viihdekäytössä olevalle laitteelleen.

Sosiaalisen median uhat ovat yritykselle nimensä veroisesti tekniikan sijaan varsin ihmislähtöisiä. 2010-luvulla roskapostisuodatin suodattaa aiempaa tehokkaammin huijaussähköpostit ja keskivertotyöntekijä on oppinut itsekin varomaan sähköpostin kautta tulevia epäilyttäviä kalasteluyrityksiä. Sama työntekijä ei välttämättä kuitenkaan osaa varoa samaisia huijauksia tai kalasteluyrityksiä sosiaalisessa mediassa, vaan luottaa esimerkiksi kontaktiensa kautta tulleisiin linkkeihin ja viesteihin. Sosiaalista mediaa selataan usein myös nopeasti, joten huolimattomuus aiheuttaa myös esimerkiksi huijauslinkkien klikkaamista.

Ennen työn aloittamista aihe rajattiin kattamaan sosiaalisen median kentältä niin sanotut uudet yhteisömediat. Suuntaa antavana rajauksena käytettiin Yleisradion Taloustutkimuksella teetättämää tutkimusta, jonka mukaan suomalaisten vuonna 2014 käytetyimpiin sosiaalisiin medioihin kuuluvat Facebook (56 %), WhatsApp (37 %), Google+ (18 %), Instagram (16 %), Twitter (10 %) ja LinkedIn (9 %). (Yleisradio 2015). Työn tarkoituksena ei ole keskittyä minkään tietyn verkkopalvelun uhkiin spesifisti, vaan havainnoida ja esitellä erilaisia riskejä, joita palvelut voivat erilaisille yrityksille aiheuttaa yleisellä tasolla. Työssä selvitetään ensin erilaiset sosiaalisen median uhkatekijät yrityksen tietoturvalle. Tämän jälkeen työssä etsitään erilaisia tapoja ja käytännön esimerkkejä, joiden avulla näiltä voitaisiin yrityksessä ennakoida.

1.1 Toiminnallinen opinnäytetyö

Toiminnallinen opinnäytetyö tavoittelee usein ammatillisessa ympäristössä ohjeistamista käytännön toimintaan, erilaista opastamista, tai toiminnan järjestämistä sekä järkeistämistä. Tutkimuksellisille töille vaihtoehtoina toimivat toiminnalliset opinnäytetyöt ovat esimerkiksi erilaiset perehdyttämis-oppaat, ympäristöohjelmat, turvallisuusohjeistukset tai vaikkapa erilaisten tapahtumien tai konferenssien järjestämiset. Aiheensa ne saavat usein työelämälähtöisesti esiin nousevasta ongelmasta tai ideasta. Töiden toteutustavat voivat poiketa toisistaan selvästi alasta riippuen, mutta niitä

yhdistää niiden käytännön toteutuksen sekä raportoinnin yhdistyminen yhdeksi kokonaisuudeksi (Vilkka, Airaksinen 2003, 9-10.) Työn aihe heräsi useista oman lähipiirin työelämän kokemuksista sekä useista valtiollisen uutiskynnyksen ylittäneistä tapauksista, joissa yritykseen oli kohdistunut tietovuoto tai muu tietoturvaan liittyvä uhka juuri sosiaalisen median osalta. Sosiaalinen media nähdään usein ainoastaan viestintä- tai markkinointi-osastojen temmellyskenttänä vailla sen suurempia uhkatekijöitä organisaation tietoturvalle. Useissa yrityksissä sosiaalisen median ongelmiin tai uhkiin havahdutaankin yleensä liian myöhään, yleensä jonkin kriisin tai ongelman ilmettyä. Tästä syystä halusinkin luoda yleispätevän, informatiivisen oppaan erilaisille yrityksille, jotka ovat eri tavoin mukana sosiaalisessa mediassa.

2 SOSIAALINEN MEDIA

2.1 Käsitteenä

Sosiaalisesta mediasta, joskus myös ’yhteisöllinen media’, kuulee 2010-luvulla puhuttavan hyvin paljon, vaikka aina ei olekaan täysin selvää mitä kyseisellä sanaparilla välttämättä tarkkaan ottaen tarkoitetaan. Tällä hetkellä kuitenkin sosiaalisella medialla viitataan käsitteenä tietyn aikakauden digitaaliseen verkkoviestintään sekä sen monikanavaisuuteen. Käsitteen määrittelyä hankaloittaa myös se, että tunnetuimmat sosiaaliset mediat, niiden palvelut sekä käyttötavat muuttuvat nopealla tahdilla jatkuvasti: palvelut käyttäjineen tulevat ja menevät välillä merkittävälläkin vuosivaihtuvuudella. Sosiaalisen median kenttä on jo vuosien ajan muodostunut muutamasta kansainvälisesti suositusta suurpalvelusta, joiden toiminta perustuu sisällön jakamiseen ja erilaisten yhteisöjen perustamiseen ja hallinnointiin. (Suominen, Saarikoski, Turtiainen, Östman 2013, 13, 17, 196.) Sosiaalisessa mediassa palvelun käyttäjä voi olla vuoroin viestijän, vuoroin vastaanottajan asemassa ja palveluita voidaan esimerkiksi kutsua eräänlaiseksi virtuaalitoriksi, jossa käyttäjät voivat keskenään kommunikoida (Pesonen 2013, 23).

Tässä työssä käsitteen sosiaalinen media määrittelemisessä käytetään muun muassa Haasion (2013, 49) käyttämää selitettä, jonka mukaan kyseisellä käsitteellä tarkoitetaan verkkoalustoja, joissa palvelun käyttäjä voi passiivisen selailun lisäksi toimia myös aktiivisena kommunikoijana ja tuottaa uutta sisältöä. Useimmat sosiaaliseksi mediaksi luokiteltavat nettipalvelut tarjoavat tietyt samat perusominaisuudet: profiilin luonnin, mahdollisuuden kommentointiin sekä statuspäivityksiin, listoja erilaisista kontakteista ja rajatumman pikaviestimen. Alustasta ja palvelusta riippumatta sosiaalisen median yhdistävin tekijä on kuitenkin käyttäjien itse tuottama sisältö sekä osallistuminen (Hinton & Hjorth 2012, 34, 55). Työssä käsiteltävien sosiaalisten medioiden rajaamisessa on käytetty suuntaa-antavasti alla tarkemmin käsiteltävää Taloustutkimuksen tutkimusta Suomen käytetyimmistä sosiaalisten medioiden palveluista vuonna 2014.

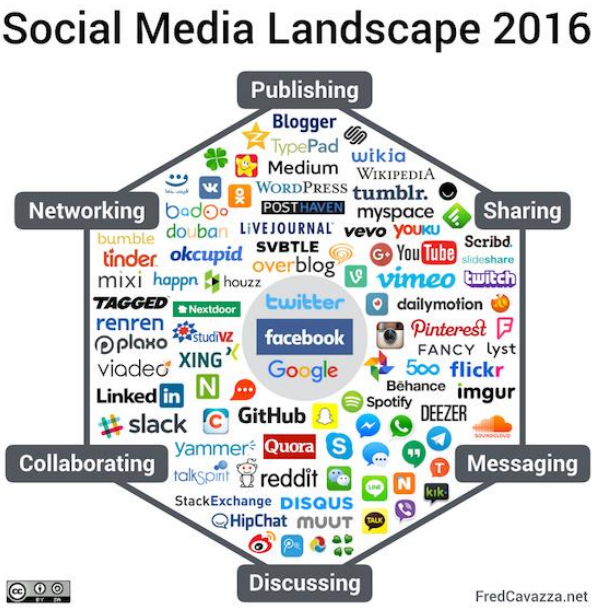
2.2 Käytetyimmät palvelut Suomessa

Tammikuussa 2015 Yleisradio julkaisi Taloustutkimuksen tekemän tutkimuksen, jossa selvitettiin suomalaisten sosiaalisten medioiden käyttötottumuksia. Kyselyn perusteella Facebook on suomalaisten eniten käyttämä sosiaalinen media, vastaajista yhteensä 56 % ilmoitti käyttävänsä palvelua. Tutkimuksen mukaan 34 % vastanneista ei käytä mitään sosiaalista mediaa. Sosiaalisten medioiden suosio yhdistettynä yritysten digitalisoitumiseen muodostaa työnantajille uusia haasteita myös tietoturvan osalta. Työntekijä tuokin tutkimuksen vastausten perusteella melko suurella todennäköisyydellä jonkin sosiaalisen median työpaikalle puhelimen, tietokoneen tai tabletin mukana.

Sosiaaliset mediat voidaan kategorisoida esimerkiksi karkeasti niiden pääkäyttötarkoituksen mukaan, kuten alla olevassa FredCavazza.net-verkkojulkaisun (Cavazza 2016) sosiaalisen median kenttää esittelevässä kuvassa (Kuva 1) on tehty. Jaotteluja tehtäessä tulee kuitenkin huomioida, että palvelut sisältävät lähes aina useita erilaisia ominaisuuksia. Lisäksi siihen voidaan myöhemmin julkaisun jälkeen julkaista uusia erilaisia lisä-

ominaisuuksia. Palvelu voi olla keskittynyt esimerkiksi kuvien jakamiseen, mutta se voi sisältää myös pikaviestimen.

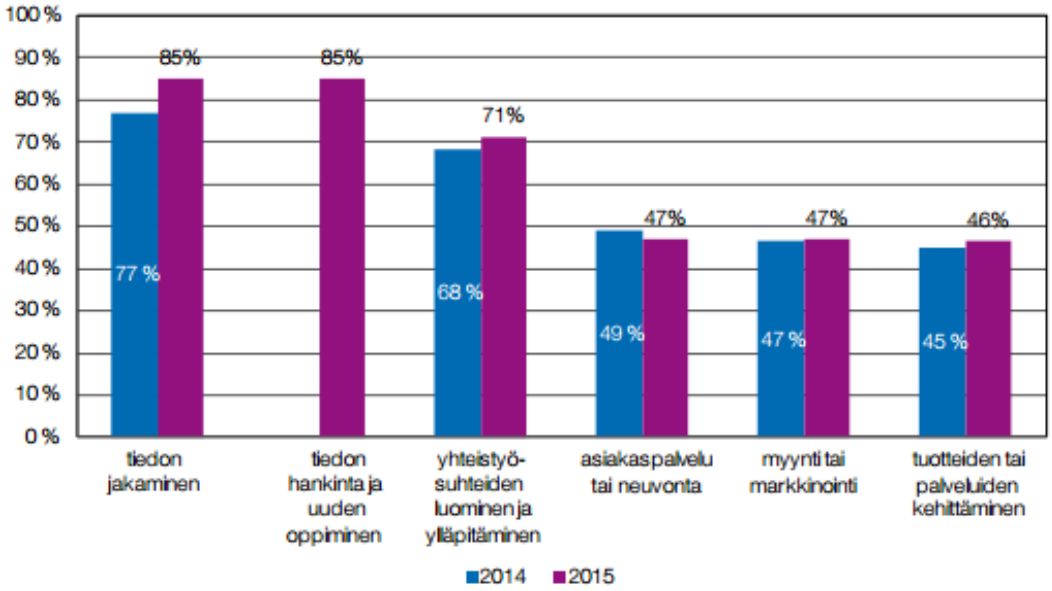
Tilastokeskuksen tekemän tutkimuksen mukaan 16-24 vuotiaista lähes jokainen vastaajista (96 %) on rekisteröitynyt jonkun yhteisöpalvelun käyttäjäksi. 25-34 vuotiailla luku on yhä melko korkea (89 %) ja 35-44 vuotiaistakin 74 % tutkimukseen osallistuneista on rekisteröitynyt jonkinlaiseen sosiaaliseen mediaan. Työelämässä olevista, kaiken ikäisistä vastaajista 67 % on luonut tilin ainakin yhteen sosiaaliseen mediaan. Tutkimuksesta käy myös ilmi, että työelämässä olevista vastaajista 60 % käyttää viikon aikana ainakin kerran jotain yhteisöllistä palvelua. Työllisistä vastaajista päivittäin tai useammin yhteisöllisiä palveluita kertoo seuraavansa 52 prosenttia. (Tilastokeskus 2015, 37.)



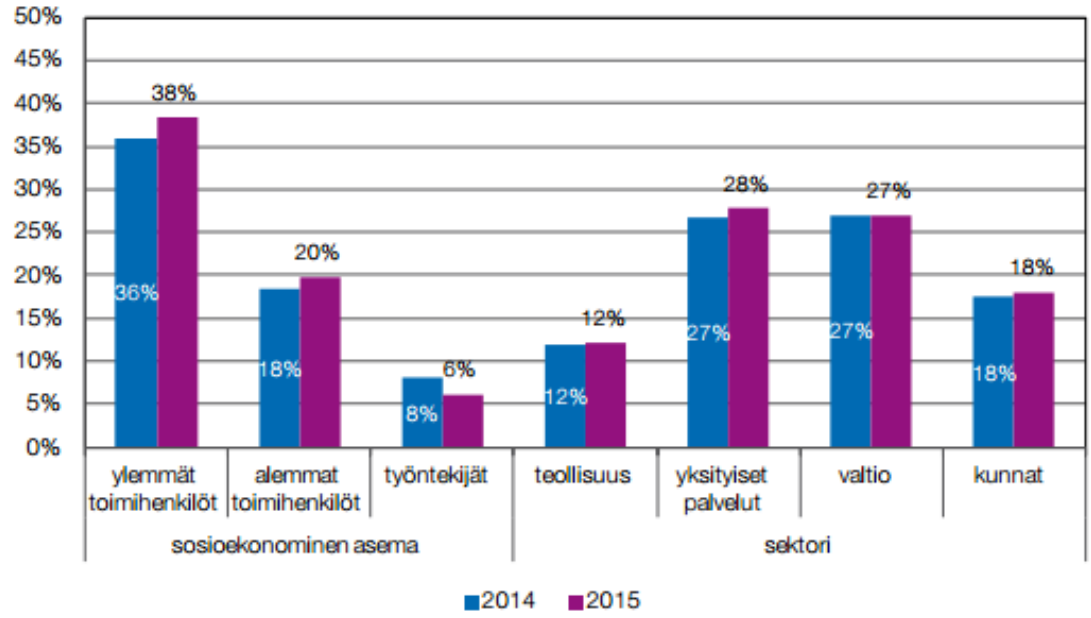
Kuva 1: Sosiaalisen median kentän voi jakaa esimerkiksi niiden pääominaisuuden perusteella, kuten verkkojulkaisu FredCavazzassa on tehty. (FredCavazza.net, 2016)

Työ- ja elinkeinoministeriön työstämistä Työolobarometreista ja niiden sisältämistä kuvista (Kuva 2, Kuva 3) selviää, että sosiaalisen median käyttö on vuosien mittaa yleistynyt myös suomalaisten työelämässä. Viimeisimmästä barometristä selviää, että sosiaalista mediaa käytetään suomalaisilla työpaikoilla useimmiten joko tiedon jakamiseen tai sen hankkimiseen (85 %).

Myös erilaisten yhteistyösuhteiden ylläpitäminen ja luominen on melko yleistä (71 %) (Työ- ja elinkeinoministeriö 2016).



Kuva 2. Sosiaalisen median käyttötarkoitukset työssä v. 2014 & 2015 (%) (Työ- ja elinkeinoministeriö 2016, 38)



Kuva 3. Sosiaalisen median käyttö työssä sosioekonomisen aseman ja sektorin mukaan v. 2014 & 2015 (%) (Työ- ja elinkeinoministeriö 2016, 38).

2.3 Sosiaalisen median uhat

2.3.1 Yleisesti

Sosiaalisen median erilaisissa huijauksissa ja hyökkäyksissä pyritään usein hyödyntämään niin sanotun ”sosiaalisen hyväksynnän” voimaa. Huijaussivuista pyritään tekemään ulospäin aidolta vaikuttavia ja suositun oloisia. ”Perinteisen” automatisoidun levittämisen lisäksi aiempaa enemmän huijauksissa nojataan ihmisten luontaiseen haluun jakaa sisältöä sosiaalisissa medioissa. Aidoilta vaikuttavissa uutisjutuissa, kilpailuissa, videoissa tai vastaavissa saattaa esimerkiksi olla upotettuina linkkejä haittaohjelmiin, affiliate-linkkejä tai vastaavia. Symantecin mukaan vuonna 2013 loppukäyttäjien avulla leviäviä uhkia oli kokonaisuudesta kaksi prosenttia, vuotta myöhemmin luku oli jo 70 %. Vuonna 2015 haittalinkkejä jaettiin manuaalisesti 76 % prosenttia. (Symantec 2016, 30.) Sosiaalisen hyväksynnän voimasta on klassinen arjen esimerkki kahdesta ravintolasta: toiseen ravintolaan on kadulla jonoa, toinen on täysin tyhjä. Ihmiset hakeutuvat mielellään vilkkaampaan ravintolaan, koska suositun ravintolan oletetaan olevan myös laadultaan tyhjempää kilpailijaa parempi (Symantec 2015, 46).

Sosiaalisen median tietoturvaongelmat ovat usein ”perinteisten” tietoturvauhkien ja uusien palveluiden yhdistelmä (Valtiovarainministeriö 2010). Sosiaalisen median uhat yritykselle voi jakaa yleistasolla kahteen eri ryhmään: työntekijöiden omiin harkitsemattomiin tekoihin, jotka johtavat seuraamuksiin ja suoraan käyttäjiin kohdistuviin hyökkäyksiin tai iskuihin (Haasio 2013, 50). Ulkopuolelta kohdistuvat uhat voivat olla myös osa ammattimaista ja järjestelmällistä toimintaa, jossa esimerkiksi rikolliset, valtiot tai ääriryhmät yrittävät saada itselleen kriittistä tietoa (luottokortti- & henkilötiedot, yrityssalaisuudet, valtiosalaisuudet). Motiivina voi toimia myös halu vaikuttaa esimerkiksi yrityksen, kuluttajien tai valtionjohdon päätöksentekoon tai tahrata tietyn organisaation tai yksilön mainetta (Tuominen 2013, 157).

Henkilöihin suoraan kohdistuvat hyökkäykset voivat olla esimerkiksi erilaisia tietojen kalasteluyrityksiä, yksilöön kohdistuvaa kiristystä arkaluontoisella materiaalilla tai verkostoitumisyritykset valeprofiileilla. Sosiaalisessa mediassa yrityksen työntekijöiden työasiat voivat myös levitä tarkoitettua laajemmalle lukijakunnalle, jolloin ulkopuoliset voivat kalastella yrityksen tietoja huomaamatta (Andreasson, Koivisto & Ylipartanen 2013, 55).

Yksi sosiaalisen median yleisimpiä uhkia on identiteettivarkaus, joka voi kohdistua käytännössä keneen tahansa. Yleisesti sosiaaliseen mediaan liittyvät lieveilmiöt ovat viimeisten vuosien aikana lisääntyneet voimakkaasti: vuonna 2010 sana Facebook mainittiin Suomen poliisin rikosilmoitus-tietojärjestelmä Patjassa noin 2000 kertaa, kolme vuotta myöhemmin sama luku oli noin 5700 (Forss 2014, 13).

Yksittäiseen henkilöön tai organisaatioon kohdistuvien hyökkäysten lisäksi sosiaalisen median uhkiin kuuluu myös eri tavoin leviävät haittaohjelmat. Niin sanottu sosiaalinen roskaposti käyttää sosiaalisen median alustaa esimerkiksi linkkien levittämiseen. Linkki voi johtaa esimerkiksi Facebook-sovellukseen, joka pyytää käyttäjää sallimaan käyttäjää pääsyn haluttuihin tietoihin, kuten tämän syöttämiin henkilötietoihin. Kerättyjä profiilitietoja voidaan esimerkiksi myydä eteenpäin aktiivisina kuluttajina mainostajille tai muille roskapostittajille. Usein samalla klikkauksella käyttäjä tulee myös jakaneeksi saastuneen linkin joko pikaviestimen tai julkisen ”seinänsä” kautta ja näin saastunut linkki tavoittaa jälleen uusia käyttäjiä (Andreasson, Koivisto 2013, 166).

2.3.2 Työelämässä

Internet sisältää reaalimaailman tavoin myös rikollista ja ”harmaata” toimintaa. Varkaudet, uhkailut, huijaukset ja erilaiset tietomurrot ovat verkossa arkipäivää ja huijarit liikkuvat siellä missä käyttäjämassatkin. Esimerkiksi Facebookin kaltaiset, suositut sosiaalisen median palvelut vetävät puoleensa myös erilaista verkkorikollisuutta. Verkkorikollisuudella (cyber crime) tarkoitetaan käsitteenä rikoksia, jotka tehdään jonkinlaisia tietojärjestelmiä hyödyntäen tai

jotka kohdistetaan erilaisiin tietoverkkoihin tai –järjestelmiin. Tyypillisiä esimerkkejä edellä mainituista ovat ”perinteiset” huijauskirjeet ja erilaiset tietomurrot. Verkkorikokset voivat kohdistua joko henkilöihin, omaisuuteen tai tiettyä valtiota vastaan (Haasio 2013, 13).

Vuonna 2012 julkaistusta, Stonesoftin Yritysjohto ja verkkorikollisuus –barometrissä yli 40 prosenttia vastanneista yritysjohtajista uskoi verkko-rikollisuuden aiheuttamien uhkien kasvavan tulevien 12 kuukauden aikana. 25 prosenttia uskoi uhkien kasvaneen viimeisen vuoden aikana. Kuitenkin 91 prosenttia vastaajista uskoo, että heidän edustamassaan yrityksessä uhkiin on suojauduttu riittävän hyvin (Korpimies 2012).

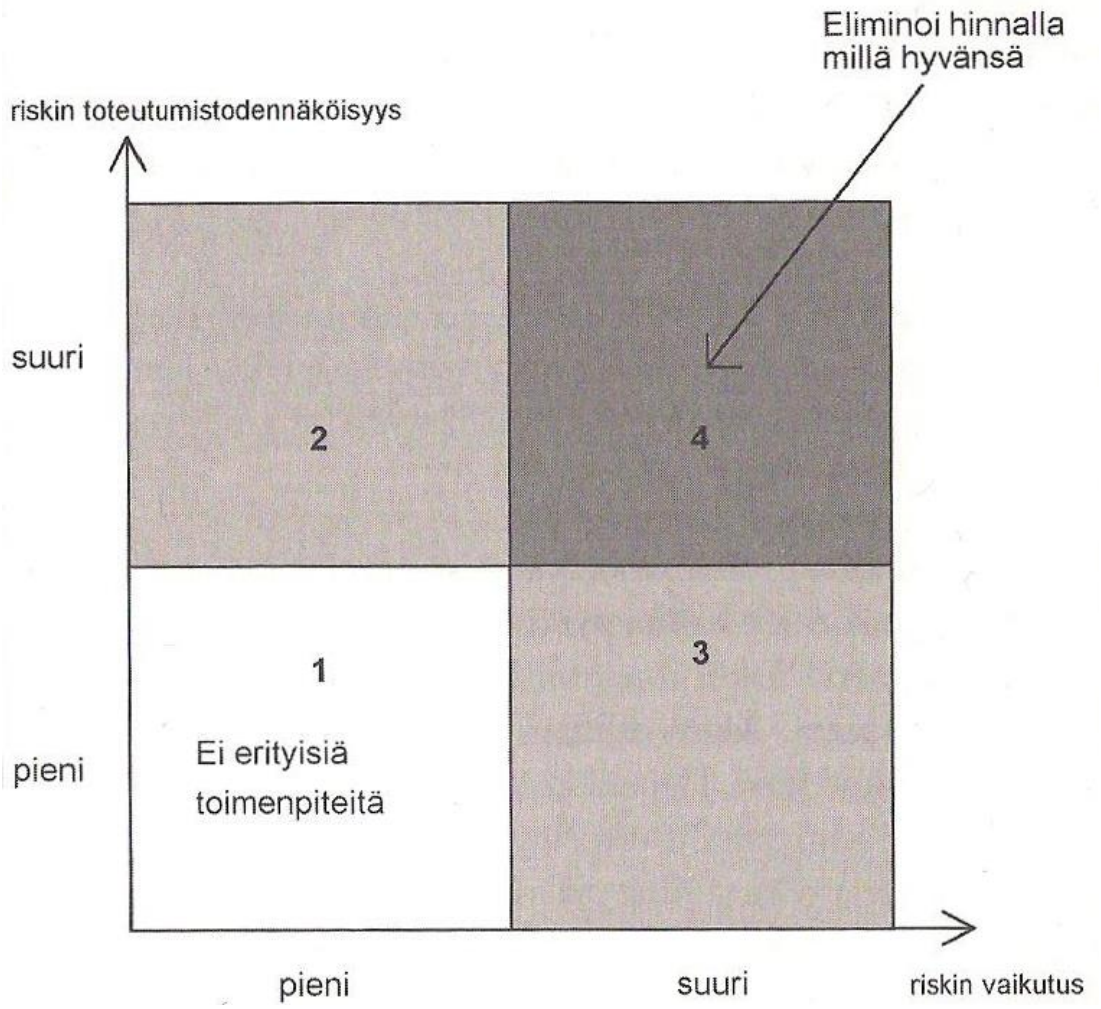
Sosiaalinen media on teoriassa organisaatiolle vähintäänkin yhtä vaarallinen kuin muukin internet. Sosiaalisesta mediasta tekee kuitenkin muuta internetiä vaarallisemman sen käyttäjien luottamus kontakteihinsa tai ystäviinsä. Sosiaalisen median uhat ja riskit voi jaotella monella tapaa. Esimerkiksi Centre for the Protection of National Infrastructure (CPNI) jakaa julkaisussaan (2014) sosiaalisen median riskit organisaatioille ja yksilöille karkeasti kolmeen kategoriaan: sosiaaliseen mediaan tuotetusta sisällöstä, sosiaalisesta kanssakäymisestä ja sosiaalisen median kautta leviävien haittaohjelmien, kalasteluiden ja roskapostin aiheuttamista riskeistä.

Sosiaalisen median tietoturvauhat saattavat elää suurestikin lyhyellä aikavälillä: eri huijauskeinot tai uhkatrendit ilmestyvät usein ”tyhjästä” ja ne hylätään sen jälkeen, kun niistä on tullut yleistiedossa tunnettuja. Internetin turvallisuusuhkia käsittelevän raportin mukaan (Symantec 2016, 30) uhrien erilaisia käyttäjä- tai henkilötietoja kalasteluun käytettyjen valetarjousten määrä romahti vuoden 2013 81 prosentista 23 prosenttiin. Vuonna 2015 kyseinen osuus oli enää 17 %. Kyseinen esimerkki osoittaa kuinka kerta-luonteinen ohjeistus yrityksessä ei takaa työntekijöiden tuntevan sen hetkisiä sosiaalisen median tietoturvauhkia: trendejä tulee seurata ja työntekijöiden ohjeistusta pitää ajan tasalla.

3 SOSIAALISEN MEDIAN UHAT YRITYKSEN NÄKÖKULMASTA

3.1 Riskienhallinta

Käsitteellä riski tarkoitetaan epävarmuustekijää, joka vaikuttaa tiettyyn tavoitteeseen pääsemistä. Riski yleensä toteutuu lukuisista tekijöistä muodostuvan tapahtumaketjun lopputuloksena (Ruuska 2007, 248). Riskienhallintasuunnitelma on suunnitelma, jossa organisaatio määrittelee riskien hallintaan käyttämäänsä toimintamallia ja niiden hallintaan käytettävät resurssit sekä vaikuttavat osatekijät (Andreasson & Koivisto 2013, 40). Hyvin tehty riskienhallintasuunnitelma auttaa yrityksen työntekijöitä päätöksenteossa ja resurssien kohdentamisessa projektiin liittyen (Mennie 2015, 13). Osana toimintasuunnitelmaa projektiin osallistuvat osapuolet suorittavat riskien tunnistamisen, johon sisältyy niiden havaitseminen sekä kuvaaminen. Tämän jälkeen riskeille tehdään riskianalyysi, jossa pyritään ymmärtämään riskien tyypit ja määrittämään niiden riskitaso. Edellä mainittua prosessia kutsutaan käsitteellä riskien arviointi. Riskilistan tekeminen edellyttää, että riskejä voidaan vertailla keskenään ja asettaa ne järjestykseen suuruusluokkansa perusteella. Täten riskit tulee kvantifioida eli arvottaa, jonka jälkeen ne voidaan asettaa riskiruudukkoon (Kuva 4). Ruudukko muodostuu kahdesta janasta, joista toinen kuvaa riskin toteutumistodennäköisyyttä ja toinen riskin vaikutussuuruutta. Ruudukon tarkoituksena on auttaa riskin suuruuden hahmottamisessa ja siinä minkä mittaluokan toimenpiteitä se projektia suunnittelevilta osapuolilta (Ruuska 2007, 252-253).



Kuva 4: Riskiruudukko auttaa riskien niiden vaikutusten arvottamisessa ja vertailemisessa (Ruuska 2007, 225).

Riskien hallitseminen ja niihin varautuminen vaatii yritykseltä luonnollisesti rahaa ja muita resursseja suojauksen, yleisen teknisen varmuuden ja henkilökunnan toimintatason ylläpitämiseen (Kuusela, Ollikainen 2005, 35). Tästä syystä riskien tasojen kartoittaminen onkin tärkeää, jotta yritys voi kohdentaa resurssinsa juuri ”oikeiden” riskien välttämiseen. Tietoturvallisuuden mittaaminen on oleellinen osa organisaation yleistä tietoturvallisuutta: sen avulla saadaan kerättyä tärkeää, onnistuessaan objektiivista tietoa yrityksen onnistumisesta sekä yleisestä tietoturvallisuuden tasosta. Mittaamisella pyritään myös löytämään heikkouksia yrityksen tietoturvasta. Objektiivisen mittaamisen lisäksi voidaan suorittaa myös subjektiivista mittaamista, eli arviointia, joka nähdäänkin usein luonteeltaan jatkuvana toimintona. Arviointia

voidaan käyttää esimerkiksi tietoturvallisuuden laadun parantamiseen ja kehittämiseen. (Laaksonen, Nevasalo, Tomula, 2006, 265-269).

Riskienhallinnan pääsäännön tulisi olla, ettei organisaatiossa oleteta ennaltaehkäisevien proseduurien, turvatoimien ja käytäntöjen toimivan uhan torjumisessa. Porvarin (2012, 103) mukaan riskienhallinnan tehtävät voikin jakaa kahteen osaan: sen avulla pyritään turvaamaan organisaation omaisuus ja muut voimavarat tunnistamalla, analysoimalla sekä priorisoimalla riskit. Riskienhallinnan toiseksi osa-alueeksi Porvari määrittelee varautumis- ja toipumissuunnittelun katastrofitilanteiden varalta.

Riskien hallinnassa on kyse varautumisesta odottamattomiin tilanteisiin. Riskien analysoinnissa ja hallinnassa on syytä muistaa, että teoriapohjalla pieniltä ja mitättömiltäkin tuntuvat potentiaaliset ongelmat voivat eskaloituessaan johtaa merkittäviinkin seurauksiin, kuten esimerkiksi lisä-kustannuksiin. Riskien hallinta koostuu neljästä osa-alueesta, joita ovat riskien analysointi, riskilistan laatiminen, toimenpiteistä sopiminen ja viimeisenä seuranta sekä riskilistan ylläpitäminen. (Ruuska 2007, 248.)

3.2 Tietovuodot

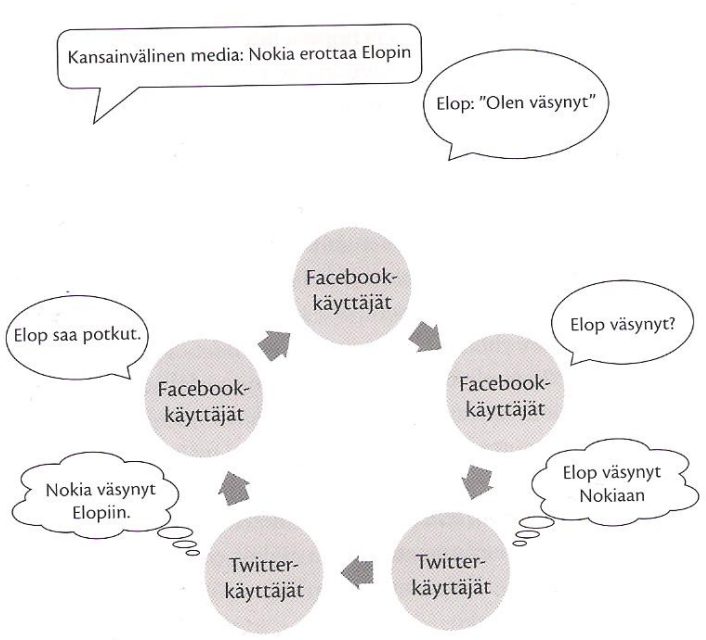
Käsitteellä tietovuoto tarkoitetaan tilannetta, jolloin salassa pidettäväksi tarkoitettu tieto päätyy taholle, jolla ei siihen ole käyttöoikeutta (Rousku 2014, 59-60).

Sosiaaliset mediat ovat muokanneet vapaa-ajan lisäksi myös ihmisten työtapaa, päätösten tekoa ja ongelmanratkontaa. Ongelmatilanteissa päädytään entistä useammin sosiaalisen median puoleen, josta yksittäinen henkilö saa mielipiteensä niin kollegoilta kuin muidenkin alojen edustajilta ja asiantuntijoilta. Työntekijät keskustelevat mielellään kollegoiden, ystävien ja tuttujensa kanssa avoimesti työasioistaan, usein ajatusten vaihto johtaakin innovaatioihin tai ratkenneisiin ongelmiin. Työnantajan näkökulmasta asia on haastava, sillä yritykset haluavat pitää yrityssalaisuutensa ja muut kriittiset

tiedot seiniensä sisällä. Sosiaalisen median arkipäiväistymisen ja ”avoimen maailman” vallankumouksen myötä kyseisten tietojen vuotamista on entistäkin haastavampaa estää (Lacey 2009, 3, 18).

Esimerkiksi mikroblogipalvelu Twitter perustuu vahvasti lyhyen elinkaaren omaaviin, maksimissaan 140 merkin päivityksiin. Vaikka suurelle yleisölle suosituksi kasvanut ilmiö onkin usein elinkaareltaan lyhyt (Nurminen 2013), päivitykset pysyvät palvelussa oletuksena ikuisesti. Vaikka käyttäjä poistaisikin yritykselle haitallisen päivityksen jälkikäteen, on siitä voitu jo ottaa esimerkiksi kuvakaappaus todisteeksi tai se voi levitä jo joitakin muita väyliä pitkin. Markkinoinnissa yritykset luonnollisesti pyrkivät nopeasti leviävään tietoon, ”someilmiöön”, mutta yritykselle kiusallisen tiedon leviämistä on varsin hankalaa hallita jälkikäteen. Joskus vasta yhtiön toimet kiusallisen materiaalin leviämisen estämiseksi tai poistamiseksi aiheuttavat tapaukselle suuremman näkyvyyden, jolloin voidaan puhua nk. Streisandin ilmiöstä.

Streisandin ilmiö (”Streisand effect”) tuli tunnetuksi, kun vuonna 2003 Kenneth Adelman julkaisi osana Kalifornian rannikon eroosiota tutkivaa valokuvaus-hanketta verkkosivuillaan ilmakuvan. Kuvassa näkyi laulaja-näyttelijä Barbra Streisandin omistama rantatalo, jonka johdosta Streisand haastoi valo-kuvaajan oikeuteen painostaakseen tätä poistamaan kuvan verkkosivuiltaan. Oikeus hylkäsi Streisandin vaateet ja oikeuskäsittelyn herättämän uteliaisuuden myötä Adelmanin projektin kotisivuilla vieraili valtaisa määrä uusia kävijöitä sekä kuva julkaistiin usean eri median kautta (Hiles 2011, 108).



Kuva 4. Esimerkki tiedon leviämisestä sosiaalisessa mediassa (Pesonen 2013, 40).

Työntekijä voi aiheuttaa yritykselle tietämättään tietovuodon esimerkiksi liittämällä LinkedIn-profiiliinsa tietoja projektista, jonka parissa hän on työskennellyt, mutta jota ei ole toistaiseksi julkistettu. Esimerkiksi peli- ja viihdealalla uusien projektien julkistaminen on usein suuri osa tuotteen markkinointia ja esilletuomista, joten työntekijä voi aiheuttaa odotettua suurempaa haittaa kyseiselle projektille (Livegamersin www-sivut 2013).

Yksi uhka organisaatiolle on sosiaalisen median alhainen julkaisukynnys yhdistettynä päihtyneeseen työntekijään (Andreasson, Koivisto 2013, 163). Vaikka työntekijällä onkin oikeus sosiaalisen median käyttöön vapaa-aikanaan, voi tämä rikkoa esimerkiksi lojaliteettivelvollisuuttaan tai salassapitovelvollisuuttaan (Pesonen 2013, 193, 194, 206). Esimerkiksi asiakkaita tai projektiin liittyvää luottamuksellista tietoa voi sosiaalisen median kautta vuotaa julki ilman, että työntekijä on julkaissut kyseistä informaatiota julkisesti mihinkään. Sosiaalisen median toinen käyttäjä voi esimerkiksi viestin, kuvan tai videon muodossa paljastaa työntekijästä tai hänen edustamastaan yrityksestä luottamuksellisia tietoja (Valtiovarainministeriö 2010). Erilaisten sosiaalisten medioiden sisältämien pikaviestimien yleistyminen työelämässä

(Suutarinen & Vesterinen 2011, 39) saattaa helpottaa työpaikalla viestimistä, mutta ne tuovat mukanaan myös riskejä yritykselle. Luottamukselliseksi tarkoitettu viesti tai keskustelu voi päätyä tarkoitettua suuremmalle yleisölle esimerkiksi tietomurron myötä (Andersson, Koivisto & Ylipartanen 2013, 55). Pikaviestit voivat myös vuotaa julkisuuteen ilman työntekijän tai organisaation virhettä: esimerkiksi sosiaalisen median työntekijän suorittama tietovuoto voi aiheuttaa tietovuodon lukemattomille muille yrityksille, jotka ovat käyttäneet kyseistä mediaa toiminta-alustanaan. Erityisesti tietovuodoissa organisaation tietoturvan kannalta heikoin lenkki on ihminen (Natri 2015).

Sosiaalisen median kautta tapahtuva tietovuoto voi yksittäisen selvän tapauksen lisäksi tapahtua myös tipoittain. Vaikka työntekijän yksittäiset viestit eivät välttämättä muodostaisikaan uhkaa työnantajalleen, voi kolmas osapuoli vähitellen kerätä yrityksen yhden tai useamman työntekijän julkaisemista tiedoista yhden kokonaisuuden, joka voi vaarantaa yrityksen tietoturvan (Valtiovarainministeriö 2010). Käyttäjä voi vuotaa myös omia tai kontakti-listansa profiilitietoja esimerkiksi Facebookissa toimivien testien ja pelien välityksellä (Kuva 5). Palvelut ovat ilmaisia ja niiden ansaintalogiikka perustuu siihen, että ne keräävät sovellusten käyttäjiltä ja näiden kontaktilistojen henkilöiltä tiettyjä profiilitietoja ja myyvät niitä edelleen kolmansille osapuolille, esimerkiksi mainostajille (Kähkönen 2016). Mikäli tietoja keräävän sovelluksen kehittäjän kohdalla tapahtuu tietovuoto, voivat esimerkiksi yrityksen työn-tekijöiden yhteystiedot tai muut tämän luovuttamat tiedot levitä hallitsemattomasti ja epätoivotusti.

Kuva 5: Erilaiset kolmansien osapuolien ilmaiset ”testit” ja ihmisistä ”kertovat” palvelut keräävät Facebookissa niihin osallistuvien yhteystietoja myyden niitä edelleen (Facebookin www-sivut 2016).

Yhtenä sosiaalisen median uusimpana osa-alueena ovat niin sanotut suoratoistopalvelut, kuten Twitterin maaliskuussa 2015 perustama Periscope (Periscopen www-sivut 2015). Palveluiden ideana on tehdä suorien lähetysten tekemisestä, eli niin sanotusta ”striimaamisesta” käyttäjälle mahdollisimman helppoa. Lähetyksen lähettäminen tapahtuu Android- tai iOS-älypuhelimella, mutta lähetyksiä voi katsella myös esimerkiksi PC:llä. Suoratoistopalvelut luovat yritysten tietoturvalle myös omat lisähaasteensa, vaikka yritys ei olisikaan virallisesti osallisena kyseisissä palveluissa. Livelähetysten helppo ja huomaamaton tekeminen madaltaa organisaatioon liittyvien tietovuotojen tapahtumista. Lisäksi livelähetysten välityksellä saatetaan levittää sellaista tekijänoikeuksien alaista materiaalia, jota ei ole tarkoitettu levitettäväksi (Vatanen, 2016). Myös erilaiset opetus- ja koulutustilaisuudet saattavat päätyä sellaisenaan julkisuuteen livelähetysten muodossa, jolla voi olla negatiivisia vaikutuksia esimerkiksi maksullisen kurssin osallistujamäärään. Suorien lähetysten kuvaamien salaa esimerkiksi oppitunneilta onkin yleistynyt vuoden

2016 aikana (Kivioja K-M, 2016) ja siinä salaa kuvaavat henkilöt rikkovat tekijänoikeuksia, sillä oppitunnit ja luennot ovat esittäjänsä ”teoksia” ja täten niiden salaa levittäminen on kiellettyä. Sovellukset saattavat aiheuttaa tietoturvaan ja tarkemmin tietovuotoihin liittyviä ongelmia myös turvallisuus- ja maanpuolustusorganisaatioille (Tolvanen 2016). Livelähetyksiä mahdollistavat sosiaalisen median palvelut ovatkin hyvä esimerkki sosiaalisen median uhkista sellaisen organisaation tietoturvalle, joka ei välttämättä itse aktiivisesti ja virallisesti olisi missään sosiaalisessa mediassa.

Tietyillä aloilla ammatinharjoittaja on sitoutunut keskivertoa tiukempaan linjaan työasioiden ja muun informaation jakamisen suhteen. Esimerkiksi pappeja, sotilaita, opettajia ja terveydenalan työntekijöitä velvoittaa ehdoton vaitiolo-velvollisuus asiakkaistaan ja näihin liittyvistä tiedoista. Lisäksi yleisesti työ-elämässä erilainen työelämän lainsäädäntö rajoittaa muun muassa sosiaalisen median kautta toteutettavaa yksilön sananvapautta. Työntekijää koskee muun muassa lojaliteettivelvollisuus, joka tarkoittaa käytännössä sitä, että kyseinen yksilö ei saa työsuhteensa aikana aiheuttaa tarkoituksellista vahinkoa työnantajalleen. Vaikenemisvelvollisuus kattaa puolestaan asiakas-tietojen lisäksi myös yrityssalaisuudet ja kyseisten tietojen levittäminen on yleensä kiellettyä työsopimuksessa myös työsuhteen päätyttyä (Järvinen 2012, 318).

3.3 Käyttäjätunnusvarkaudet

Erilaisissa tietomurroissa tai huijauksilla käsiin saatujen tilien tai profiilien luvaton käyttö voi täyttää useamman rikoksen tunnusmerkistön, vaikka kaapatuilla tileillä ei suoritettaisi mitään aktiivista toimintaa (Forss 2015, 93). Käyttäjätunnusvarkauksissa kaappaaja voi esimerkiksi julkaista kaapatun yksilön tai yrityksen nimissä erilaista materiaalia, varastaa henkilötietoja tai levittää erilaisia haittaohjelmia (Valtiovarainministeriö 2010). Lisäksi henkilöltä tai yritykseltä voidaan kiristää lunnaita tunnusta vastaan tai some-tilin salasanan avulla pyritään murtautumaan siihen liitettyyn sähköpostitiliin (Kyberturvakeskus 2014, 4). Yksittäistä kaapattua tiliä voidaan myös käyttää

yksittäisen henkilön tai organisaation muiden tunnustietojen hankkimiseen (Andreasson, Koivisto 2013, 165).

Käyttäjätunnusten salasanoja voidaan kalastella myös huijaussivustoilla, jotka muistuttavat sisällöltään, ulkonäöltään sekä verkkotunnukseltaan aitoa sivustoa. Sivujen tarkoituksena on kerätä uhrien käyttäjätunnukset sekä salasanat ja näin päästä käsiksi näiden käyttäjätunnuksiin (Korpela 2005, 118). Kirjautumistietoja voidaan kalastella myös sähköposteilla, jotka on naamioitu näyttämään erehdyttävästi kyseisen palvelun virallisilta sähköposteilta. Huijauspostissa saatetaan vaatia käyttäjältä pikaista kirjautumista esimerkiksi sääntörikkeiden tai keksityn arvonnan nimissä (Facebookin www-sivut 2016).

Usein käyttäjätunnusvarkauksia tehdään erilaisten aggressiivisesti sosiaalisten medioiden pikaviestimien kautta leviävien huijausten avulla. Ketjuviesti ohjaa yleensä vastaanottajansa sosiaalisen median ulkopuoliselle huijaussivustolle, joka puolestaan jäljittelee jotain muuta tunnettua verkkopalvelua. Uhria houkutellaan eri tavoin esimerkiksi asentamaan käyttämäänsä selainohjelmaan tietty laajennus, jonka avulla rikolliset saavat käsiinsä uhrin käyttäjätunnuksen sekä salasanan. Varastetun tilin lisäksi haitallinen selainlaajennus saa käyttöoikeudet uhrin tiliin ja näin haitallinen viesti leviää automaattisesti uhrin kontaktilistoille (Valtonen 2016).

Käyttäjätunnus – myös sosiaalisen median – voidaan kaapata erilaisten palveluiden unohtuneen salasanan palautusmekanismia hyödyntäen. Joissakin palveluissa käyttäjä voi turvakysymykseen oikein vastaten tilata uuden salasanan unohtuneen tilalle. Hakupalveluiden ja sosiaalisten medioiden tarjoaman informaation takia turvakysymyksissä tulisikin välttää helposti selvitettävissä olevaa vastausta. Esimerkiksi käyttäjän äidin tyttönimen tai ensimmäisen lemmikin nimen selvittäminen ei kyseisten palveluiden ansiosta välttämättä ole kovin vaivalloista. Tilien salasanat voidaan kaapata myös erilaisilla näppäimistökaappareilla. Kaapparit asennetaan uhrin tietokoneelle tämän huomaamatta ja se tallentaa taustalla kaikki laitteella tehdyt näppäilyt. Käyttäjän lisäksi kaikki virustentorjunta-

ohjelmatkaan eivät välttämättä havaitse kyseisiä haittaohjelmia. Kaappari voidaan asentaa myös muistisirun muodossa uhrin tietokoneen näppäimistön ja tietokoneen väliin, jossa se tallentaa kaikki näppäilyt suoraan laitteen kaapelista. Tällaisen, laitepohjaisen kaapparin havaitseminen on etsintä-ohjelmalle mahdottomuus. (Järvinen 2012, 128-129).

Tietoturva-asiantuntija Petteri Järvinen arvioi, että suomalaisella on keskimääräisesti muistettavanaan 10 - 20 erilaista tunnusta tai salasanaa (Savon Sanomat 2016). Aktiivisimmilla henkilöillä salasanoja kertyy suurempikin määrä, jolloin tunnusten ja salasanojen muistamisesta tulee hankalaa ja uusien salasanojen keksiminen hankaloituu. Yleisimpiä heikkoja salasanoja Suomessa ja ulkomailla ovat ”123456”, ”password/salasana”, ”qwerty” (SplashData 2015) sekä lemmikkien tai perheenjäsenten nimet ja syntymäajat (Talouselämä 2013). Ihmiset saattavat myös joko tietämättömyyttään tai välinpitämättömyyttään käyttää samaa, mahdollisesti heikkoa, salasanaa useassa verkkopalvelussa samanaikaisesti, joka aiheuttaa henkilölle jo suuren riskin tunnustensa turvallisuuden suhteen. Vahva salasana puolestaan on pitkä, se sisältää erikoismerkkejä, ei ole yksittäinen sanakirjasta löytyvä sana, sitä ei käytetä muiden palveluiden salasanana ja se ei ole arvattavissa eikä sitä ole tallennettu tietokoneelle tekstitiedostona. Salasana voi toisaalta olla esimerkiksi lause tai epämääräinen lista useita sanoja, joiden sekaan on upotettu erikoismerkkejä tai numeroita (Krebs 2014, 237-238).

Yhtenä motivaationa käyttäjätunnusvarkaudelle voi urkinnan ja kiusanteon lisäksi olla rahan tienaaminen. Esimerkiksi vuonna 2010 julkisuuteen nousi tapaus, jossa krakkeri kaupitteli eteenpäin 1,5 miljoonaa kaapattua Facebook-tunnusta 0,025 dollarin kappalehintaan. Tavallisesti varastettuja käyttäjä-tunnuksia kaupitellaan 1-20 dollarin kappalehintaan (Linja-Aho 2010).

3.4 Identiteettivarkaudet

Vuonna 2015, 4. syyskuuta Suomen rikoslakiin muutettiin seuraava pykälä:

”Joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee, on tuomittava identiteettivarkaudesta sakkoon” (368/2015 9 b §).

Identiteettivarkaudessa hyödynnetään jo olemassa olevia tietoja esimerkiksi keräämällä niitä eri lähteistä. Teollisuusvakoilun lisäksi motiivina voi toimia kohteen mustamaalaaminen, ihmissuhteiden vahingoittaminen tai väärän tiedon levittäminen (Pesonen 2013, 146). Myös yritysten nimissä voidaan avata profiili tai sivu sosiaaliseen mediaan, jonka tarkoituksena on vaikuttaa organisaation toimintaan tai imagoon tavalla tai toisella (Valtiovarainministeriö 2010).

Sosiaaliset mediat mahdollistavat useiden erityyppisten identiteetti-varkauksien toteuttamisen, joiden päätarkoituksena on yritysvakoilu tai muu yritykselle haitallinen toiminta. Yksittäisen henkilön tietoja voidaan kalastella yhdistellen eri nettipalveluiden profiileja ja tiedonjyväsiä yhdeksi kokonaisuudeksi, joka mahdollistaa ulospäin uskottavalta näyttävän valeprofiilin luomisen. Yritykselle valeprofiilit voivat olla kahdella tapaa uhka. Esimerkiksi kyseisen yrityksen edustajan nimissä tehdään uskottavalta vaikuttava valeprofiili, joka pyrkii verkostoitumaan esimerkiksi Facebookissa yhteistyökumppaneiden ja yrityksen muiden työntekijöiden kanssa. Toinen uhkatekijä on, että yhteistyökumppanin nimissä luotu valeprofiili ottaa yrityksen työntekijöihin yhteyttä yrittäen kalastella arkaluontoista tietoa. Koska molempia skenaarioita on yrityksen kannalta mahdotonta täysin ennalta-ehkäistä ja huijaamistavat vaihtelevat jatkuvasti, on työntekijöiden kouluttaminen erilaisten huijausyritysten tunnistamiseen ennakkoon tärkeää (Viestintävirasto 2010).

Joissakin tapauksissa yrityksen työntekijöiden profiilien sijaan identiteetti-varkaus voi kohdistua yritykseen itseensä, esimerkiksi sosiaalisessa mediassa voidaan luoda valesivu, joka vaikuttaa olevan yrityksen virallinen julkaisu-kanava. Yrityksiin kohdistuvan identiteetin varastaminen on helppoa ja varsin yleistä, myös Suomessa (Norppa, Peltomäki 2015, 101).

Joissakin tapauksissa väärennetyn profiilin luomisen taustalla saattaa olla ainoastaan halu päästä lähemmäksi tietyn työntekijän henkilökohtaista Facebook-aikajanaa, jonka kautta vihamieliset tahot pyrkivät keräämään tarvittavia tietoja yksilöstä tai yrityksestä (Tranberg, Heuer, 2012, 97). Yrityksen yksittäisten työntekijöiden kirjautumistietoja erilaisiin verkko-palveluihin voidaan kalastella erilaisin huijauskeinoin, joita käydään työn myöhemmässä vaiheessa tarkemmin läpi.

3.5 Tietojen kalastelu ja vakoilu

Yrityksessä voidaan teknisesti varautua erilaisiin tietoteknisiin uhkiin ylläpitämällä ajantasaista virustorjuntaa, varautumalla esimerkiksi palvelintiloja uhkaaviin riskeihin tai suodattamalla www-liikennettä yrityksen palomuurin avulla, mutta sosiaalisen median kautta tapahtuvaan suoraan tai epäsuoraan tietojen kalasteluun yrityksen ei ole juurikaan mahdollista teknisesti varautua. Tästä huolimatta tietojen kalastelu aiheuttaa organisaation tietoturvalle omat uhkansa.

Sosiaaliset mediat mahdollistavat kahdentyyppisen tietojen kalastelun: aktiivisen tietojen kalastelun (phishing) sekä passiivisemman, julkisuudessa olevan tietojen keruun (pharming). Kuitenkin molemmat tavat kalastella tietoja voivat aiheuttaa uhrilleen, tässä tapauksessa yksittäiselle työntekijälle tai organisaatiolle, vakavia seurauksia (Andreasson, Koivisto 2013, 169).

Erilaiset kalastelu- ja huijaussähköpostit ovat varmasti monelle yritykselle ja työntekijöille tuttu näky. Tietojen kalastelu on kuitenkin Symantecin mukaan (2015, 55) vähentynyt reilusti viimeisten vuosien aikana. Yhtiön keräämien

tilastojen mukaan vuonna 2013 sähköpostien osuus kalasteluista oli 1/392. Vuotta myöhemmin sähköpostien osuus oli jo huomattavasti pienempi: 1/965. Tietojen kalastelu, roskaposti ja vastaava onkin siirtynyt sähköposteista vaihe vaiheelta enemmän ja enemmän sosiaalisen median puolelle. (Symantec 2015, 55-58).

Sosiaaliset mediat palveluina nojaavat usein avoimeen sekä helposti yksilöä lähestyttävään toimintaan, joka tekee erilaisen informaation kalastelusta ja eriasteisesta vakoilusta aiempaa helpompaa (Valtiovarainministeriö 2010). Sosiaalista mediaa voidaan käyttää myös tietolähteenä muita väyliä tapahtuvaa petosta auttamaan. Esimerkiksi työntekijän lomatilapäivityksiä voidaan hyödyntää eri tietojen kalastelussa lähestyttäessä toista yrityksen työntekijää vaikkapa sähköpostitse. Muiden viestintävälineiden ohella myös sosiaalisen median kautta tapahtuva viattomalta vaikuttava tiedustelu tai tietojen urkinta saattaa usein olla vasta esivaihe itse petokselle tai muulle isommalle rikokselle (Viestintävirasto 2010).

Kuten aiemmassa kappaleessa mainittiin, voidaan yrityksen salaisia tietoja pyrkiä hankkimaan esimerkiksi erilaisten valeprofiilien avulla. Muun muassa vuonna 2011 nähtiin aiheeseen liittyvä kuuluisa tapaus, kun yhdysvaltalaisen laivaston amiraali James Stavridiksen nimissä tehtailtiin valeprofiili verkko-palvelu Facebookiin. Stavridiksen nimissä tehdyn valeprofiilin onnistui hankkia lähikontakteikseen (”kaverit”) muun muassa useita korkea-arvoisia brittien valtion virkahenkilöiden puolustusministeriöstä sekä armeijasta. Ennen paljastumistaan kiinalaisina vakoojina pidettyjen hyökkääjien onnistui hankkia itselleen virkahenkilöiden puhelinnumeroita, sähköpostiosoitteita, kuvia sekä näiden perheiden henkilötietoja (Forss 2014, 100). Vastaavalla periaatteella toimivia hyökkäyksiä on tehty myös eri yhtiöiden vastaavien henkilöiden nimissä tavoitteena urkkia erilaisia yrityssalaisuuksia (Hopkins 2012).

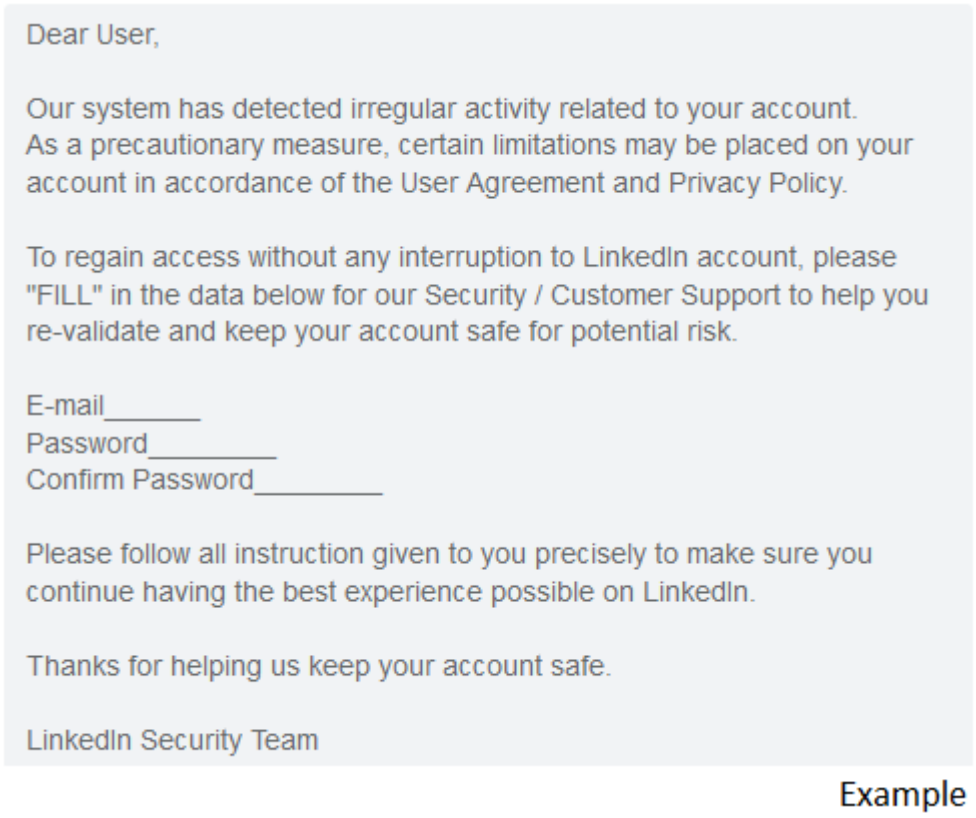
Eri sosiaaliset mediat mahdollistavat myös yksityishenkilöiden henkilötietojen keräämisen entistä tehokkaammin. Erilaisissa alkuun aidoilta vaikuttavissa kampanjoissa tai kilpailuissa on usein mukana jonkinlainen lomake, jossa henkilöltä pyydetään erilaisia tietoja hänestä itsestään ja mahdollisesti myös

työnantajasta. Keräysvaiheen jälkeen huijauksen suorittaneella toimijalla on käytössään valmis lista kontakteista, joihin osoittaa jatkossa uudet roskaposti-hyökkäykset tai vastaavia kampanjoita (Valtiovarainministeriö 2010). Myös aiemmin mainitut testisovellukset tai sivut keräävät käyttäjistään tietoja, joita myydään edelleen käyttäjän välttämättä ymmärtämättä tätä. Yleisesti sovelluksen tai palvelun ”ilmaisuus” tarkoittaakin sitä, että kyseisen palvelun kehittäjän ansaintatapa on käyttäjiensä tietojen keruu ja edelleen myyminen vaihtelevalla tasolla (Korhonen 2014).

Erilaiset sosiaaliset verkostot saattavat myös olla rikolliselle taholle arvokasta tietoa. Sosiaalisten verkostojen avulla esimerkiksi valtiolliset tiedustelupalvelut voivat päästä muiden rikosten jäljille. Sosiaaliset verkostot voivatkin paljastaa käyttäjästä jotain sellaista, mitä tämä ei itse olisi tarkoituksella profiilissaan kertonut. Jos henkilöllä on merkittävä määrä kaverilistallaan yrityksen X työntekijöitä, on hän itsekin luultavasti ainakin työskennellyt kyseisessä yrityksessä (Järvinen 2010, 235-236).

Tietojen kalastelu on Suomessa yleistä niin sähköpostitse kuin sosiaalisen mediankin välityksellä (Andreasson, Koivisto, Ylipartanen 2014, 28), mutta sosiaalisen median kautta tapahtuvien kalasteluyritysten suhteen ihmiset ovat usein varomattomampia. Henkilöstö voi osata yrityksessä toteutetun koulutuksen ja ohjeistuksen avulla varoa sähköpostien välityksellä tapahtuvia kalasteluyrityksiä, mutta sosiaalisessa mediassa samat työntekijät voivat käyttäytyä huomattavasti varomattomammin. Esimerkiksi, jos työntekijälle tuttu henkilö pyytää tätä tulemaan mukaan uuteen toiminnallisuuteen tai asentamaan uuden palveluun liittyvän lisäosan, voi tämä avata saapuneen linkin huomattavasti luottavaisempana (Puolustusvoimat 2013, 2). Vuoden 2016 marraskuussa 42 prosenttia Slush-yritystapahtumaan osallistuneista startup-yrityksistä kertoi joutuneensa jonkinlaisen phishingin, eli huijausviestien tai muunlaisen tietojen kalastelun kohteeksi (OSG Viestintä 2016), joten esimerkiksi tietojen kalastelun voidaankin sanoa koskettavan hyvin eri kokoisia ja tyyppisiä organisaatioita.

Tietojen kalasteluun liittyy usein niin sanottua sosiaalista manipulointia, jolla uhri saadaan vakuutettua kyseisen huijauksen luotettavuudesta. Huijausten onnistuminen onkin usein kiinni kyseisen manipuloinnin vakuuttavuudesta, jonka myötä huijaustavat ovat muuttuneet entistä monimutkaisemmiksi ja kekseliäimmiksi (Symantec 2016, 29). Kalasteluhuijausten lisäksi esimerkiksi erilaisten roskaposti- ja linkkispämmin ympärille saatetaan luoda kattavia ja monikerroksisia bottitiliverkostoja, jotta verkoston tietyt tilit saadaan näyttämään suosituilta, uskottavilta ja aktiivisilta (Symantec 2016, 29). Sosiaalisen median tietoja voidaan kalastella myös sähköpostitse erilaisten käyttäjäehtorikkomusten tai muiden kuvitteellisten palvelurikkeiden varjolla (Kuva 6).



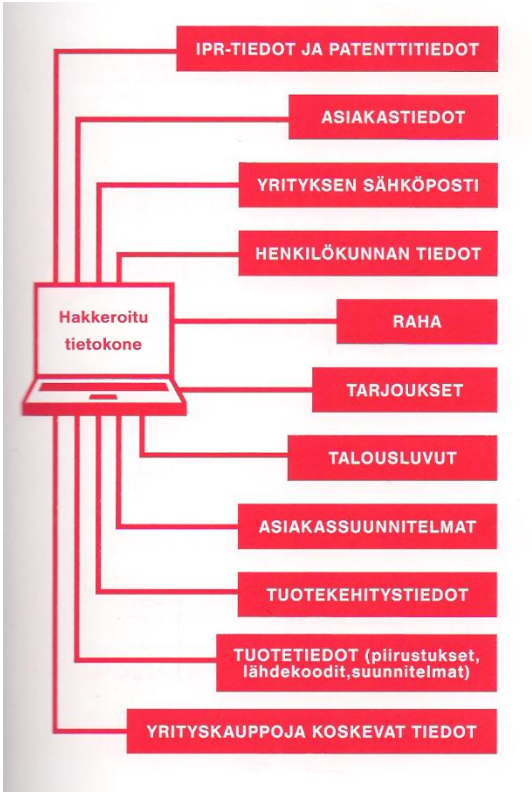
Kuva 6: Verkkorikolliset voivat kalastella sosiaalisen median tunnuksia esimerkiksi lähestymällä uhria sähköpostitse palveluntarjoajaksi tekeytymällä (LinkedInin www-sivut 2016).

3.6 Haittaohjelmat ja sovellushaavoittuvuudet

Sosiaalisen median välityksellä leviävä haittaohjelma käyttää yleensä tavalla tai toisella hyödyksi kyseisen alustan näkyvyyteen ja sisällön jakamiseen liittyviä ominaisuuksia. Esimerkiksi Facebookin tilapäivitysten jakamiseen tai massoittain kontakteille leviävät yksityisviestit ovat usein internetrikollisten suosimia tapoja levittää haittaohjelmaansa (Andreasson, Koivisto 2013, 16). Sosiaalisen median pikaviestimien välityksellä leviääkin usein automaatti-viestejä, jotka yrittävät saada uhreja asentamaan esimerkiksi haitallisen laajennuksen käyttämäänsä verkkoselaimeen. Haitalliset selainlaajennukset voivat esimerkiksi urkkia uhriensa luottokortti- tai salasanatietoja. Lisäksi ne leviävät lyhyessä ajassa nopeasti, sillä niitä levittävät ketjuviestit leviävät automatisoidusti uhrin kontaktilistalle (Valtonen 2016). Vuoden 2016 lopulla tunnistettiin uusi, Facebookin sekä LinkedInin välityksellä leviävä kiristys-haittaohjelma, joka hyödynsi tiedostojen liittämistä palveluiden pika-viestimissä. Kiristysohjelma levisi kuvatiedostoksi naamioituneena siten, että haittaohjelman uhrin hallinnoima tili lähetti kuvatiedostoksi naamioituneen asennustiedoston edelleen tämän kontaktilistalla oleville henkilöille (Check Point 2016)

Haittaohjelma on ohjelma, joka suorittaa käyttäjän kannalta ei-toivottuja toimintoja tämän laitteella. Ohjelman avulla voidaan esimerkiksi ohittaa some-palvelun turva-asetuksia tai vallata uhrin käyttäjätili kokonaan. Haittaohjelma voi myös toimia passiivisesti keräten käyttäjästä tietoja tai käyttää henkilön käyttäjätiliä roskaviestien lähettämiseen edelleen. Haittaohjelmia voidaan myös levittää sosiaalisessa mediassa esimerkiksi shokeeraavien valeuutis-juttujen, huijaussivujen tai selainlaajennuksien avulla (Facebookin www-sivut 2016). Yksi keino levittää haittaohjelmia on ohjata uhri sosiaalisen median ulkopuoliselle sivustolle ja huijata tätä klikkaamaan näkymätöntä kehystä, jonka klikkaaminen suorittaa halutun toiminnon (esimerkiksi mainoksen jakaminen sosiaalisessa mediassa, jonne uhri on kirjautuneena). Lopulta uhri saatetaan johdattaa luvattuun, usein esimerkiksi suoraan YouTubesta löytyvään, videon luo, jotta uhri ei kokisi tulleensa huijatuksi (Andreasson, Koivisto 2013, 166-167).

Työkäytössä olevista tietokoneista verkkorikolliset voivat sosiaalisessa mediassakin leviävien haittaohjelmien avulla havitella esimerkiksi organisaation IPR- ja patenttitietoja, henkilökunnan tietoja tai muita yrityksen toimintaan liittyviä arkaluonteisia asioita (Kuva 7).



Kuva 7. Esimerkki työkäytössä olevan tietokoneen tiedoista, joita vihamieliset tahot havittelevat (Norppa, Peltomäki 2015, 63)

Kuten muissakin tapauksissa, myös haittaohjelmien levityksessä tekijät nojaavat ihmisten luottamukseen kontakteihinsa. Ihmisten luottamus yhdistettynä varsinkin sosiaalisessa mediassa käytettyihin url-osoitteiden lyhenteisiin, kuten bit.ly tai tinyurl.com takaa erilaisille haittaohjelmille oman levitysväylänsä. Esimerkiksi mikroblogipalvelu Twitterin rajoitettu merkkimäärä totuttaa käyttäjänsä usein avaamaan erilaisia lyhennettyjä osoitteita, jolloin käyttäjä ei enää kiinnitä suurta huomiota lyhytlinkkien avaamiseen. Lyhennettyjen osoitteiden haittapuolena käyttäjä ei etukäteen tiedä mihin osoitteeseen lopulta itsensä klikkaa (Valtiovarainministeriö 2010, 2.2).

Joissakin tapauksissa käyttäjä voidaan huijata klikkaamaan kohdetta, joka ei todellisuudessa tarjoa klikkaajalle haluttua toimenpidettä. Esimerkiksi vuonna 2010 noin 100 000 suomalaista oli klikannut repäisevällä otsikolla varustettua ketjupäivitystä. Ensimmäisessä suomenkielisessä klikkauskaappauksessa käyttäjä ohjattiin erilliselle sivulle, jossa klikkaajaa pyydettiin klikkaamaan numeroita 1, 2 ja 3, jonka johdosta ”mato” alkoi levitä edelleen asianomaisen tietämättä tämän Facebook-profiilin kautta. Huijauksen toisella sivulla käyttäjältä pyydettiin tämän puhelinnumeroa, jotta henkilö voisi osallistua älypuhelinarvontaan. Todellisuudessa numeron antaja sitoutui mobiilipalvelun kestotilaajaksi 19 euron kuukausihintaan, joka peritään puhelinlaskun yhteydessä. Lopulta käyttäjä pääsi mainostetun videon luo, joka olisi tosin ollut normaalisti löydettävissä YouTube-videopalvelusta (Forss 2011, 120). Vastaavanlaisella periaatteella toimivan ”tykkäyskaappauksen” uhriksi joutui myös vuonna 2013 Suomen ulkoministeri Erkki Tuomiojan Facebook-profiili (Forss 2011, 120). Edellä mainitunlaisten esimerkkien tapaukset eivät välttämättä aiheuta suurta uhkaa työnantajan tietoturvalle, mutta ne saattavat olla hyvinkin kiusallisia tapauksia työnantajan tietoturvan ja yleisen imagon kannalta.

Muita haittaohjelmien tyyppejä on muun muassa niin sanotut kiristysohjelmat (”ransomware”), jotka leviävät erilaisten saastuneiden verkkosivujen välityksellä. Ne eivät välttämättä kosketa suoranaisesti sosiaalista mediaa, mutta niiden yleistyminen näkyy myös sosiaalisessa mediassa. Käyttäjä voidaan sosiaalisesta mediasta houkutella huijaussivustolle, jonka kautta asianomainen huijataan lataamaan haittaohjelma tietokoneelle. Ohjelmat ”lukitsevat” tietokoneen, jonka jälkeen ohjelma kiristää käyttäjältä esimerkiksi sakkomaksua tai vastaavaa tietokoneen avaamiseksi. Sähköisesti vaadittavaa maksua pyritään usein tehostamaan esimerkiksi viranomaisiin liittyvin kuvin, eikä maksun suorittaminen lopulta vaikuta tietokoneen toiminnallisuuteen millään tapaa. Kiristysohjelmat on usein räätälöity eri maiden mukaan, Suomessa viesteissä käytetään suomalaisten viranomaisten logoja ja kuvia, englantilaisissa esimerkiksi FBI:n (Federal Bureau of Investigation). Yleisiä kiristyshaittaohjelmia ovat muun muassa Browlock, Cryptolock ja Reveton (Andreasson ym. 2014, 27).

Niin sanotun BYOD-kulttuurin (bring your own device) yleistymisen myötä työntekijä voikin tuoda myös viihdekäytössä olevan laitteen mukana sosiaalisesta mediasta hankkimansa haittaohjelmat yrityksen verkkoon (Norppa, Peltomäki 2015, 106). Vaikka hakkeroitu tietokone olisikin työntekijän itsensä hankkima ja omistama, voi se sisältää henkilön edustaman organisaation kannalta kriittistä dataa (Kuva 8) tai rikollinen voi ainakin käyttää sitä tunkeutuakseen henkilön työsähköpostiin tai tämän hallinnoimiin organisaation virallisiin sosiaalisen median tunnuksiin.

Kuva 8. Esimerkki ”tavallisen” tietokoneen sisältämistä tiedoista (Norppa, Peltomäki 2015, 62).

Sovellushaavoittuvuuksissa ulkopuoliset tahot hyödyntävät tietystä ohjelmasta, lisäohjelmistosta tai käyttöjärjestelmästä löytyvää tietoturva-aukkoa. Yksi tunnetuin esimerkki viime aikoina oli Heartbleed-haavoittuvuus, joka mahdollisti monen eri nettipalvelun tunnusten urkkimisen. Heartbleedille altistui suurista sosiaalisista medioista muun muassa Facebook, Instagram, Googlen eri palvelut ja Dropbox (Viestintävirasto 2014). Myös kolmannen osapuolen sovellukset ja lisäosat voivat sisältää joko haavoittuvuuksia tai uhkia yrityksen tietosuojalle (Järvinen 2012, 309). Esimerkiksi Facebookissa

erilaisia kolmannen osapuolen piensovelluksia on saatavilla ainakin yli 10 miljoonaa, joiden seassa on käyttäjälleen suoraan haitallisia, tai ainakin arveluttavia toimijoita ja sovelluksia (Rousku 2014, 207).

3.7 Roskaposti

Roskaposti, joissakin tapauksissa spam tai ”spämmi”, on Jukka Korpelan (2005, 149) määritelmän mukaan sähköpostia, joka on kerralla lähetetty hyvin suurelle määrälle henkilöitä, ei ole vastaanottajien tilaama tai näiden suostumuksella lähetettyä liikennettä tai sisältää yleensä mainoksen tai jonkin tyyppisen huijausyrityksen. Kyseistä edellä mainittua määritelmää voi soveltaa myös nykypäivänä sosiaalisessa mediassa leviävään roskapostiin eli spämmiin.

Työn aiemmissa alaotsikoissa on jo sivuttu joitakin kertoja erilaista roskapostia ja sen leviämistapoja sosiaalisessa mediassa. Roskapostia pyritään sosiaalisessa mediassa levittämään erilaisten huijausuutisten tai vastaavien ajankohtaisten ja raflaavien otsikoiden avulla (Symantec 2015, 54). Roskaposteissa lukijalle voidaan myös luvata houkuttelevaa pelastusta raha- tai työongelmiin. Yleisen heikon taloustilanteen todettiinkin jo vuoden 2009 alussa näkyvän suoraan roskapostien levikissä (Symantec 2009).

Kuten moni muukin huijaustapa sosiaalisessa mediassa, myös roskapostin levityksessä hyödynnetään ihmisten luottamusta palvelun ”lähikontakteihin” (”kaverit”). Tietojen kalastelun lisäksi myös roskapostin levityksessä sähköpostin osuus on viimeisten muutaman vuoden aikana pienentynyt huomattavasti, muun muassa yritysten kehittyneiden roskapostisuodattimien ja suojausten ansiosta (Mashable 2013). Symantecin tutkimuksissa sähköpostin osuus roskapostin levityskanavista oli vuonna 2012 69 prosenttia, vuonna 2014 luku oli laskenut 60 prosentin tasolle ja sen uskotaan jatkavan laskua tulevinakin vuosina (Symantec 2015, 59). Roskapostin määrä kokonaisuudessaan ei yhtiön tutkimusten mukaan ole samojen vuosien aikana juurikaan muuttunut.

Eri sosiaalisen median palvelut käyttävät erilaisia työkaluja kitkeäkseen roskapostia palveluistaan, mutta ne ovat usein kierrettävissä ja askeleen jäljessä niin sanottua suorittavaa osapuolta. Spämmitilit kiertävät usein työkaluja siten, että alkuperäisten tilapäivitysten julkaisevat tilit poistavat päivitykset esimerkiksi 4-12 tuntia julkaisun jälkeen. Tässä ajassa ns. ”papukaija-tilit” ovat ehtineet jakaa kyseistä tilapäivitystä, joka mahdollisesti sisältää esimerkiksi saastuneen linkin. Kyseiset ”papukaijat” jakavat edellä mainittujen haitallisten linkkien lisäksi myös, usein kopioitua, muuta sisältöä, jotta tilit vaikuttaisivat autenttisilta (Symantec 2016, 29).

Yrityksen työntekijöiden lisäksi sosiaalisen median roskaposti voi vaikuttaa myös suoraan itse yritykseen tai sen brändiin. Nykypäivänä moni yritys haluaa toimia aktiivisesti sosiaalisessa mediassa, esimerkiksi pitäen yhteyttä asiakkaisiinsa tai suorittaen erilaista markkinointia. Mitä suositummaksi ja suuremmaksi yhtiö tai sen brändi sosiaalisessa mediassa kasvaa, sitä suuremman ongelman erilainen spämmi eli roskaposti yhtiölle muodostaa. Nexgaten vuonna 2013 teettämässä tutkimuksessa (Nexgate 2013) sosiaalisen median spämmistä asia käy ilmi erään anonyymin esimerkin muodossa. Yhtiöllä oli oma sivunsa Facebookissa, jonka tilapäivitysten kommenteista joka seitsemäs oli jonkinlaista spämmiä. Sivun roskapostista 3 % sisälsi jonkinlaisen spämmilinkin, 1,5 % linkkien sivuista sisälsi jonkinlaisen haittaohjelman. Merkittävä yrityksen sosiaalisen median tiliin tai lanseeraamaan tunnisteeseen (”hashtag”) kohdistuva roskaposti voi vaikeuttaa esimerkiksi kanssakäymistä asiakkaiden kanssa tai karkottaa asiakkaat.

Linkkispämmin motiivina voi olla mainostulojen kerääminen, haittaohjelman levittäminen tai niin kutsuttu spamdexing, jossa kyseistä sivustoa pyritään saamaan Internetin hakukoneissa korkeammille sijoille (Nexgate 2013, 6-7).

Yllä mainitun, haittaohjelmia sekä affiliatelinkkejä levittävän roskapostin ja spämmin lisäksi yritystä voi koskettaa myös toisenlainen spämmäys, yrityksen oma roskaposti. Joidenkin yritysten asiakasmarkkinointi sosiaalisessa

mediassa voi keskittyä voimakkaasti yrityksen tilapäivitysten, kuvien tai muun vastaavan median edelleen jakamiseen. Edellä mainitussa kampanjatyylissä yritys julkaisee sosiaaliseen mediaan esimerkiksi kuvan ja rohkaisee seuraajiaan jakamaan kyseistä kuvaa esimerkiksi arvonnan avulla. Kyseinen kampanjointi saattaakin kääntyä yritykselle imagotappioksi, sillä yksittäisten ihmisten mainosten jakamista pidetään epämiellyttävänä ilmiönä (Leino 2011, 263).

3.8 Paikantamiseen liittyvät uhat

Nykypäivän matkapuhelin kyetään paikantamaan esimerkiksi hätätilanteissa alle kymmenessä sekunnissa hätäkeskuksen toimesta. Hätäpaikannus voidaan tehdä sellaisessa tapauksessa, jossa hätäkeskukseen soittaneen henkilön uskotaan olevan välittömässä vaarassa. Paikannuksen tarkkuus vaihtelee henkilön sijainnista riippuen 50 metristä 1-5 kilometriin (Hätäkeskuslaitos 112.fi). Paikantaminen voidaan suorittaa joko GPS-, a-GPS- tai WLAN-paikannuksella (Koivunen 2010).

Älypuhelimet mahdollistavat siis tarvittaessa nopean sekä ainakin kaupunkialueella hyvinkin tarkan paikantamisen. Puhelin on nykypäivänä laitteena käyttäjälle niin henkilökohtainen, ettei sitä juuri luovuteta muiden käyttöön. Täten puhelimen paikantamisessa voidaankin olettaa laitteen omistajan löytyvän sieltä missä laite sillä hetkellä sijaitsee (Järvinen 2010, 129). Monet sosiaaliset mediat mahdollistavat paikkatietojen liittämisen esimerkiksi kuva-, video- tai tekstimuotoisiin tilapäivityksiin. Myös suorien verkkolähetysten tekemisen mahdollistava Periscope mahdollistaa lähetyksentekijän sijainnin jakamisen, joka yhdistettynä videon sisältöön voi aiheuttaa erityyppisiä tietoturvauhkia yksittäiselle työntekijälle tai tämän edustamalle organisaatiolle. Kyseisen palvelun paikannusominaisuus oli ennen ohjelmapäivitystä niin tarkka, että se mahdollisti videon lähettäjän yhdistämisen esimerkiksi tiettyyn asuinrakennukseen. Vuonna 2015 julkaistun ohjelmapäivityksen myötä paikannusjärjestelmää heikennettiin (Engadget 2015). Päivityksestä huolimatta esimerkiksi Suomen puolustusvoimat on

kieltänyt sosiaalisen median ohjeistuksessaan Periscope-lähetysten tekemisen kokonaan (Tolvanen 2016). Vastaavia käyttäjän paikantamiseen liittyviä uhkia on olemassa kuitenkin myös muissa palveluissa, kuten kuvapalvelu Instagramissa (Helsingin Sanomat 2016). Joissakin tapauksissa tulisi huomioida, että työntekijän jakama yksittäinen sijaintitieto ilman muuta informaatiotakin voi olla työnantajan näkökulmasta liian paljastava (Järvinen 2012, 310).

3.9 Sopimusehtoihin, lainsäädäntöön ja toimintoihin liittyvät epäselvyydet

Sosiaaliseen mediaan rekisteröidyttäessä tilin luojan tulee pyydettyjen käyttäjätietojen lisäksi sitoutua noudattamaan palvelua tarjoavan osapuolen laatimia sopimusehtoja, jotka hyväksytään sellaisinaan (Pesonen 2013, 134) ja palvelun käytön jatkaminen tulkitaan ehtojen hyväksymiseksi (Järvinen 2010, 245). Palvelun käyttöehdot voivat myös muuttua käytännössä milloin tahansa ja näin myös hyvin usein tapahtuu esimerkiksi Facebookin kohdalla (Järvinen 2010, 246). Käyttäjä ei myöskään rekisteröitymisensä jälkeen voi itse vaikuttaa ehtoihin esimerkiksi julkisella tilapäivityksellä, sillä käyttöehtojen muuttaminen vaatii aina sekä käyttäjän että palveluntarjoajan suostumuksen. Yksittäiselle käyttäjälle ainut tapa irtisanoutua palvelun käyttöehdoista on tilin sulkeminen ja kyseisen palvelun käytön lopettaminen (Toivanen 2012).

Sosiaalisen median palveluehdoissa käsitellään muun muassa palveluntarjoajan oikeuksista käyttäjiensä luomaan sisältöön, esimerkiksi kuviin, tekstiin tai profiilitietoihin (Koivunen 2010). Joissakin tapauksissa palveluun rekisteröityvä käyttäjä voi pahimmillaan antaa palveluntarjoajalle esimerkiksi rajattomat käyttöoikeudet kyseiseen palveluun ladattuihin valokuviin ja videoihin (Rousku 2014, 207).

Monet sosiaaliset mediat on ainakin alkujaan suunniteltu usein yksityishenkilöiden käyttöön, joten niiden sopimus- ja palveluehdot voivat olla ristiriidassa organisaation oman säännöstön kanssa (Koivunen 2010). Ongelmatilanteita voi syntyä myös silloin, kun käyttäjä tai tämän edustama

organisaatio haluaa lopettaa käyttäjätilin kyseisestä palvelusta tai kun tilin haltija menehtyy. (Pesonen 2013, 230).

Työntekijän työsuhteen päättyminen voi muodostaa ongelmia sekä työntekijälle itselleen että tämän edustamalle organisaatiolle. Työsuhteen osapuolilla saattaa olla esimerkiksi eri käsitys oikeuksista tiettyyn sosiaaliseen mediaan tai medioihin luotuun tiliin. Työnantajan mielestä tili asiakkaineen (seuraajat) voi kuulua työsuhteen päättymisenkin jälkeen organisaation alaisuuteen, koska sitä on käytetty työaikana työkäyttöön hyödyntäen työntekijän virallista työsähköpostia ja työntekijä on tiliä hallinnoidessaan esiintynyt selkeästi edustamansa yrityksen edustajana. Irtisanoutuva työntekijä puolestaan voi nähdä tilin kuuluvan hänelle, jos hän on esiintynyt palvelussa omalla nimellään. Mikäli työntekijällä ei ole etukäteen tehtyä sopimusta työnantajansa kanssa, voi tämä irtisanoutuessaan muokata tilin tiedot täysin henkilökohtaiseksi säilyttäen asiakaskuntansa eli seuraajat (Pesonen 2013, 191).

Sopimusehtojen lisäksi eri sosiaalisten medioiden palveluiden toiminnot ja palvelut muuttuvat ja kehittyvät alinomaa. Eri palveluihin lisätään uusia ominaisuuksia, jotka voivat tuoda mukanaan uusia, esimerkiksi yrityksen tietosuojaan, liittyviä uhkatekijöitä mukanaan (Järvinen 2012, 305). Uudet ominaisuudet voivat tavalliselle palvelun käyttäjälle ilmestyä päivityksen mukana kaikessa hiljaisuudessa.

Palvelinvirtualisoinnin ja erilaisten hajautettujen pilvipalveluiden hyödyntäminen on yleistynyt erilaisia Internet-palveluita tarjoavien organisaatioiden keskuudessa. Kyseiseen ilmiöön lukeutuvat muun muassa sosiaaliset mediat. Jaettuun kapasiteettiin liittyviä ongelmia palvelun käyttäjän näkökulmasta ovat esimerkiksi palvelun tietoaineistojen todelliseen sijaintiin liittyvät kysymykset ja siitä ilmenevät lainsäädäntöön liittyvät konfliktit: eri maiden tietoturvaan ja tietosuojaan liittyvä lainsäädäntö voi poiketa toisistaan merkittävästi. Lisäksi yrityksen on käytännössä mahdotonta auditoida kyseisen, ulkomailla sijaitsevan palveluntarjoajan tietoturvallisuutta (Koivunen 2010, 20).

4 OPAS SOSIAALISEN MEDIAN UHKILTA VARAUTUMISEEN

Tämän otsikon alla käydään aiemmin luetellut uhat yrityksen tietoturvalle uudelleen läpi ja esitellään erilaisia tapoja sosiaalisen median riskien minimoimiseen yrityksen tietoturvan kannalta. Otsikon alla käsitellään myös eri strategioita, kuinka organisaatiossa tulisi reagoida realisoituneeseen riskiin. Lisäksi otsikon alla esitellään organisaatiolle erilaisia tapoja riskienhallintaan ja miten työntekijöitä voidaan aiheesta opastaa.

4.1 Sosiaalisen median tietoturvaohjeen valmistelu

4.1.1 Ideaalitilanne

Yrityksen tietoturvasta huolehtiminen on yleistä tasapainoilua käyttö-mukavuuden ja tietoturvallisuuden välillä. Organisaation tietoturvapolitiikan tulisi luonnollisesti olla ennaltaehkäisevää ja turvallisuuteen pyrkivää, mutta se ei saa haitata yrityksen ydintoimintaa tai työntekijöiden tehokkuutta. Tietoturvallisuus on yrityksessä pieniä tekoja osana työntekijöiden jokapäiväistä toimintaa. Hyvä tietoturvallisuus osa organisaatiokulttuuria, jolloin kaikki työntekijät ymmärtävät tietoturvallisuuden merkityksen ja työskentelevät sen saavuttamiseksi (Laaksonen, Nevasalo, Tomula 2006, 17).

Sekä Suomen että EU:n lainsäädäntö asettaa yrityksille erilaisia suoria ja epäsuoria velvoitteita liittyen kyseisen toimijan tietoturvasta huolehtimiseen. Lainsäädäntöä ei tulisi kuitenkaan pitää miniminä yrityksen tietoturvaa kehitettäessä, sillä lainsäädäntö on usein varsin yleistä ja tulkinnanvaraista – tekninen tietoturva on luonteeltaan taas melko eksaktia (Laaksonen, Nevasalo, Tomula 2006, 18). Yrityksen tietoturva tulisikin nähdä muunakin kuin ainoastaan tiettyjen minimivaatimusten ja standardien noudattamisena sekä seuraamisena. Jo pelkästään yrityksen uskottavuuden ja luottamuksellisen kuvan luomisen kannalta tietoturvallisuudesta tulisi tehdä fiksu ja mielekäs osa työntekijöiden toimintaa. Kuten työssä aiemmin mainittiin, on esimerkiksi tietovuodon aiheuttamaa imagotappiota ongelmallista korjata.

Rousku (2014, 162) mainitsee työpaikan tietoturvalinjauksista tärkeimpänä sen, että työpaikalla on kaikkeen työntekoon liittyvistä asioista sekä ohjeistus että perustelu kyseiselle ohjeistamiselle. Tällöin kaikki ohjeistamattomat tehtävät ovat oletuksena työntekijöiltä kiellettyjä ilman esimiehen tai tietoturvavastaavan lupaa. Näin vältytään epävarmoilta tilanteilta, joissa vaillinaisella tietopohjalla toimiva työntekijä aiheuttaa edustamalleen yritykselle tietoturvauhan.

Ennen sosiaalisen median tietoturvaohjeistuksen luomista yrityksen tulisi asettaa jo itse ohjeistukselle selkeät tavoitteet ja päämäärät. Eri alojen ja kokoisten yritysten ohjeistukset poikkeavat väkisin toisistaan aivan kuten tietoturvaohjeistukset yleisestikin. Yrityksen koosta tai toimialasta huolimatta ohjeistuksen tulisi kuitenkin alkaa jo tilin luomisen suunnittelusta ja päättyä tilin sulkemiseen tai poistamiseen palvelusta, sillä kuten työstä on käynyt ilmi, sosiaalisen median uhat yrityksen tietoturvalle kattavat kaikki tilin luomiseen liittyvät vaiheet.

Aiemmin käsitellyn riskikartoituksen avulla yrityksessä ollaan selvillä sitä kohtaavien sosiaalisen median tietoturvauhkien eri tyypeistä ja niiden vakavuudesta: vakavimmat riskit pyritään luonnollisesti ennaltaehkäisemään täysin ja vähemmän vakaviin luodaan toimintasuunnitelma tilanteen purkamiselle.

Sosiaalisen median käyttäjältä saattaa unohtua tavallinen varovaisuus, mikäli hänelle tuttu henkilö suosittelee esimerkiksi linkkiä (Järvinen 2012, 302). Todellisuudessa viesti on roskapostia ja viestin linkki saastunut, mutta tilanteen uhri on varomattomuuttaan klikannut linkin auki ja refleksinä sulkenut ponnahdusikkunan klikkaamalla ”Ok”. Sosiaalisen median tietoturvauhkiin liittyy hyvin monessa tapauksessa edellä mainitun esimerkkitapauksen tapainen tapahtumasarja, jossa uhri joko tietämättään tai huolimattomuuttaan tekee pienen vaaditun virheen. Yrityksen toimialasta ja koosta riippumatta ohjeista tulisikin selvitä itse riskin ja ennaltaehkäisykeinojen lisäksi myös mahdolliset ”worst case scenario” -seuraukset, joiden avulla tietoturvalinjaukset saadaan perusteltua fiksusti. Virheiden seuraukset

ymmärtäessään työntekijää toivottavasti kiinnittää entistä enemmän huomiota omaan jokapäiväiseen, tässä tapauksessa sosiaalisessa mediassa, toimimiseen. Lisäksi työntekijän ymmärtäessä verkkorikollisen motiivit ja yleiset toimintatavat hän oppii tunnistamaan muuttuvat hyökkäykset aiempaa tehokkaammin sekä ottaa kyseiset uhkatekijät mahdollisesti aiempaa vakavammin huomioon toiminnassaan. Työntekijän ollessa itse suurin tietoturvauhkien ennaltaehkäisijä, on edellä mainitut työntekijän arkitoiminnan muutokset yksi päätavoite ja ideaalitilanne, johon ohjeistuksella tulisi yrityksessä pyrkiä.

Tiivistettynä ideaalitilanteessa yrityksessä tunnetaan etukäteen sosiaalisen median uhat sen tietoturvalle ja uhat on luokiteltu niiden seurausten perusteella. Organisaatiossa on myös tiedossa tavat, joilla uhkien ennaltaehkäisy maksimoidaan, palveluiden rooli yritykselle tunnetaan ja opastuksen, uhkien seurannan ja tietojen päivittämisen suhteen on tehty jonkinlainen kirjattu työnjako. Lisäksi yrityksessä työntekijät tietävät kuinka toimia mahdollisen tietoturvauhan konkretisoituessa.

4.1.2 Sosiaalisen median tietoturvaohjeen valmistelu yrityksessä

Järvinen (2014, 24) esittää tietoturvan periaatteista väitteen, jossa tietoturva on tekniikan sijaan enemmänkin psykologiaa. Hänen mukaansa tietoturvassa on 80 prosenttisesti kyse psykologiasta ja ainoastaan 20 prosenttia aiheesta on tekniikkaa. Ajatusmallia on hyvä hyödyntää luodessa yrityksen sosiaalisen median tietoturvaohjetta – kuten aiemmin mainittua, sosiaalisen median haitoista selkeä enemmistö leviää uhrien oman toiminnan avulla (Symantec 2016, 30). Ohjeistuksessa tulisikin painottaa työntekijän osuuden suuruutta yrityksen tietoturvan ylläpitämiselle: tietoturvaa ei voi ulkoistaa suoja-ohjelmistoille tai -laitteille.

Organisaation tietoturvallisuus ja työntekijän käyttömukavuus ovat käytännössä aina keskenään ristiriidassa: jokin asia on harvoin yrityksen kannalta tietoturvallinen ja työntekijän kannalta helppokäyttöinen (Järvinen

2014, 2). Tietoturvaohjetta valmistellessa suunnitteluprosessiin tulisikin ottaa mukaan yrityksen tietohallinnon edustajan lisäksi myös asianomaisia työkaluja, tässä tapauksessa sosiaalisen median, käyttävän ryhmän tai tiimin edustaja. Ohjeistuksessa voidaan antaa painoarvoa eri huomioille riippuen yrityksen yleisestä tietoturvapolitiikasta. Siinä tulisi myös huomioida palveluiden erilaiset, jo aiemmin käsitellyt, uhkia ennaltaehkäisevät toimet ja työkalut, jotka eivät kuitenkaan vaikuta työntekijän työtehokkuuteen tai yleiseen käyttömukavuuteen. Eri osapuolien välinen suunnittelu mahdollistaa myös potentiaalisten tietoturvauhkien vertailun sosiaaliseen mediaan avattavan tilin hyötyihin: mihin tarpeisiin tilin avaaminen vastaa ja onko sille kenties olemassa tietoturvan ja käyttömukavuuden kannalta tehokkaampaa alustaa tai palvelua?

Ennen ohjeen luomista yrityksessä tulisi selvittää sosiaalisen median nykyinen ja tuleva rooli työntekijöiden työ- ja vapaa-ajan käytössä. Ohjeistukseen vaikuttaa luonnollisesti muun muassa se, onko tulevaisuudessa tarkoituksena luoda virallisia tilejä yritykselle sosiaaliseen mediaan, toimiiko yrityksen tietyt edustajat henkilökohtaisilla tileillään yrityksen virallisina edustajina vai toimivatko yrityksen työntekijät sosiaalisessa mediassa mahdollisesti yritykseen yhdistettävinä yksityishenkilöinä. Mikäli sosiaalista mediaa käytetään merkittävästi osana jokapäiväistä työtä, on luonnollisesti myös tietoturvaohjeistuksen oltava tuolloin tavallista kattavampi. Ohjeistuksen luomista suunnitellessa tulisi myös huomioida organisaation koko ja sen muut, aiemmin tehdyt tietoturvaohjeistukset ja -politiikka.

Vaikka jokainen yritys varmasti mielellään ennaltaehkäisisi kaikki tietoturvariskit, ei realistisessa tietoturvasuunnitelmassa ja työntekijöiden ohjeistamisessa oleteta ennaltaehkäisyn toimivan sataprosenttisesti. Tästä syystä yrityksessä tulisikin olla toimintasuunnitelmat myös tilanteille, joissa jokin tietoturvauhka on konkretisoitunut: kun uhan havainnut työntekijä tietää kuinka toimia, voi hän toimillaan minimoida uhan aiheuttamat seuraukset.

Ohjeistuksen jakeluun tulisi myös kiinnittää huomiota, jotta keskiverto-työntekijä ei huku tietoturvainformaatioon ja niin sanottuun ”turhaan” tietoon.

Ohjeistus olisikin hyvä jakaa osiin sen valmistuttua siten, että oleellinen informaatio tavoittaa juuri ne työntekijät, jotka tietoa kaipaavat. Täten myös mahdolliset lisätiedotteet ja ajankohtaiset opastukset tavoittavat oikeat työntekijät, eikä ajankohtaisia tietoturvatiedotteita pidetä itselle kuulumattomina. Organisaation yleiseen tietoturvapolitiikkaan ja sosiaalisen median ”fiksuun” käyttämiseen liittyviä linjauksia ja ohjeistuksia voidaan jaella koko organisaatiolle yleislinjan selkeyden ylläpitämiseksi. Uhkien seuranta tulisi ohjeistusta luodessa asettaa tietyn työntekijän tai työntekijöiden vastuulle, jotta uhkien seuranta ja niistä tiedottaminen ei lopu ohjeistuksen julkaisuhetkeen. Yleispätevän ja muuttumattomana pysyvän ohjeistuksen, kuten muun muassa salasanaohjeet, sosiaalisen median keskustelusäännöt ja etätyöohjeet voi kuitenkin sisällyttää organisaation yleiseen tietoturvaohjeistukseen.

4.1.3 Työntekijöiden opastaminen

Yrityksen on laadittava työntekijöilleen asiaan kuuluva ohjeistus ennen minkään sosiaalisen median käyttöönottoa työelämässä siitäkin huolimatta, että palvelua käyttää ainoastaan sen työntekijät eikä kyseinen yritys itse esiinny virallisesti verkkopalvelussa. Organisaatio ei voi edellyttää työntekijöidensä ymmärtävän sosiaalisen median käyttöön liittyviä vastuita ennen työpaikalle tehtyä, aihetta kattavaa ohjeistusta. Ohjeiden tekemiseen velvoittaa Suomen työelämän tietosuojalaki (Pesonen 2013, 154).

Oppaan, ohjeistuksen tai organisaation tietoturvapolitiikan suunnittelijan tulee muistaa, että tietoturvapolitiikkaan liittyvissä linjauksissa, toimenpiteissä tai ohjeissa ei ole olemassa yhtä absoluuttista oikeaa tyyliä (Ruuska 2014, 162). Jokainen yritys ja organisaatio ovat erilaisia ja niissä käytetään erilaisia verkkopalveluita, sovelluksia, rautaa ja erilaista henkilöstöä, joten tällöin luonnollisesti myös tietoturvasuunnitelmat toteutetaan eri ympäristöissä eri tavoin.

Sosiaalinen media on ilmiönä varsinkin Suomessa melko nuori. Esimerkiksi tänä päivänä käytetyin sosiaalinen media, Facebook, on ollut Suomessa

yleisessä tietoudessa vajaat kymmenen vuotta. Erilaiset sosiaalisten medioiden ilmiöt haittoineen elävät myös suuresti erilaisissa tilastoissa, mikä vaikeuttaa yritysten varautumista ennakkoon erilaisiin sosiaalisen median kautta leviäviin uhkiin. Joissakin tapauksissa jopa edellisvuoden tilastot voivat olla vanhentuneita. Hyvänä esimerkkinä vuosittaisesta tilastopiikistä on aiemmin tekstissä mainittu Symantecin ylläpitämä tilasto, jossa loppukäyttäjien avulla leviäviä uhkia oli kaikista uhista ensin kaksi prosenttia ja vuotta myöhemmin luku oli huimat 70 %. Jatkuvasti muuttuvat sosiaalisten medioiden uhkatekijät vaativatkin yrityksen IT-asiantuntijalta jatkuvaa aiheen seurantaa ja työntekijöiden opastamista. Yhtenä haasteena muuttuvien trendien lisäksi organisaation IT-vastaavalle on aiheesta tiedottaminen siten, että työntekijät saavat aiheesta juuri heitä koskevaa informaatiota ja että käsiteltävä informaatio pysyy määrällisesti inhimillisenä.

Sosiaalisen median tietoturvaan liittyviin uhkiin kannattaa varautua organisaatiossa samalla periaatteella, mitä Andreasson & Koivisto käyttää yrityksen tietoturvasta yleisestikin: sen tulee olla luonteva osa organisaation muuta toimintaa ja varsinkin osa sen kokonaisvaltaista riskienhallintaa (Andreasson, Koivisto 2013, 32). Kuten tekstissä on aiemmin käynyt ilmi, on sosiaalisen median uhat yrityksen tietoturvalle sekä nopealla tahdilla muuttuvia että moniosaisia: tietojen kalastelua saatetaan käyttää käyttäjätunnusvarkauksiin, haittaohjelmia tietojen kalasteluun, käyttäjätunnusvarkauksia teollisuusvakoiluun ja niin edelleen. Tästä syystä yrityksen onkin erityisen tärkeää keskittyä luomaan puolustusverkostaan mahdollisimman moniosainen ja -kerroksinen.

Perehdytystä on työpaikalla annettava työntekijöille aloitus-, muutos- ja käyttöönottotilanteissa. Hyvä perehdyttäminen saa työntekijän ymmärtämään osuutensa eri työtehtävissä ja kyseisten tehtävien merkityksen organisaation toiminnassa. Yrityksen tulisikin panostaa omaan perehdytysprosessiinsa ja sen kehittämiseen jatkuvasti esimerkiksi keräämällä palautetta siitä (Andreasson, Koivisto, Ylipartanen 2014, 115).

Työntekijöiden tietämättömyys sekä joissakin tapauksissa tarkoituksellinen toiminta yritystä vastaan muodostavat yrityksille merkittävän turvallisuusriskin. Tästä syystä henkilöstön opastaminen kaikissa yrityksen tietoturvaan liittyvissä asioissa on ensisijaisen tärkeää (Norppa, Peltomäki 2015, 108-109). Kuten yrityksen tietoturvan hallitsemisessa yleisestikin, myös sosiaalisen median suhteen on tärkeää tehdä työntekijälle selkeät ja käytännölliset ohjeet. Sosiaalisen median suhteen ohjeistus riippuu hyvin paljon sekä yrityksen viestintätyylistä että sosiaalisen median roolista yrityksen toiminnassa. Perusohjeistuksen olisi oltava pituudeltaan alle kaksi sivua ja siinä voidaan käsitellä esimerkiksi sitä, onko sopivaa mainita työnantaja työntekijän henkilökohtaisissa sosiaalisen median profiileissa tai miten paljon työntehtävistä on hyväksyttävää kertoa LinkedInissä. Ohjeistuksessa tulisi ottaa huomioon työntekijän oikeus mielipiteidensä ilmaisuun sekä työlainsäädäntö. (Leino 2011, 162,163).

Yrityksen tietoturva on kokonaisuutena tekniikan ja ihmisten jokapäiväisen toiminnan summa. Paras tapa työnantajalle on rakentaa tietoturva selkeästi yrityksen toimintaan sisään (Kurki 2010, 97). Yrityksen kriittisten tietojen suojelemisessa ja yrityksen tietoturva-asioista huolehtimisessa jokaisella työntekijällä on oma roolinsa, osalla kyseinen rooli on luonnollisesti tavallista kriittisempi. Työntekijän kannalta onkin ensiarvoisen tärkeää, että työntekijä on tietoinen roolistaan työnantajansa tietoturva-asioissa ja kykeneväinen suoriutumaan roolistaan (Purser 2004, 215).

Selkeästi rakennettu tietoturvaohjelma on organisaation yleisen tieto-turvallisuuden tärkeimpiä osa-alueita. Siihen sisältyy muun muassa koko yhtiön toimintojen kattava politiikka ja aiheeseen liittyvä ohjeisto, joka sisältää spesifimmät ohjeet tietyistä osa-alueista, kuten tässä tapauksessa sosiaalisen median tietoturvasta.

Organisaation tietoturva-linjauksia – tässä tapauksessa sosiaaliseen mediaan liittyviä – tehtäessä on syytä muistaa, että henkilöstölle suunnattu ohjeistus kattaa myös yhtiön johdon, esimiestason sekä ICT-henkilöstön (Rousku 2014, 162).

Hyvä sosiaalisen median opas tai ohjeistus työnantajalta työntekijöilleen on selkeä kokonaisuus, josta selviää heti mitä vastuita ja velvollisuuksia työntekijää aiheesta kohtaa. Organisaation ohjeistuksen jälkeen työntekijän tulisi tietää mistä asioista hänen on sopivaa julkisesti kommentoida, mistä aiheista voi tarkemmin kirjoittaa, missä sosiaalisessa mediassa ja kenen suulla on sopivaa esiintyä sekä millä tyylillä työntekijöiden on sopivaa kirjoittaa sosiaalisiin medioihin (Isokangas, Vassinen, 2010, 151). Tietoturvaan liittyvä ohjeistus olisi hyvä yhdistää yleisen sosiaalisen median ohjeistukseen, jotta ohjeistuksen yleinen viesti työntekijälle on inspiroiva, rohkaiseva ja informatiivinen. Pahimmassa tapauksessa ohjeistuksen puuttuessa työntekijät eivät osallistu olenkaan yritystä tai yrityksen alaa koskevaan keskusteluun ja näin yritys menettää paljon hyviä uusia mahdollisuuksia ja sen näkyvyys jää haluttua pienemmäksi.

Alkuoppaiden lisäksi työntekijän perehdytyksessä tulisi ottaa huomioon myös ajankohtaisista tietoturvaan liittyvistä asioista tiedottaminen, perehdytyksen kontrollointi ja kehittäminen (Andreasson 2015, 97).

Viestintävirasto tiedottaa yleisimmistä haavoittuvuuksista, huijauksista, sosiaalisen median vuodoista ja alaan liittyvistä tapahtumista osoitteessa https://www.viestintavirasto.fi/kyberturvallisuus.html. Sosiaalisen median tietoturvaoppaasta vastaavan henkilön tulisikin seurata Viestintäviraston virallisia tiedotteita aktiivisesti ja tarvittaessa jakaa tietoa esimerkiksi yrityksessä käytetyn sosiaalisen median salasanavuodosta edelleen yrityksen työntekijöille.

4.1.4 Uhkien ennaltaehkäisyyn liittyviä ongelmia

Tietotyön yleistyminen on muuttanut työ- ja vapaa-ajan rajan huomattavasti aiempaa hämärämmäksi. Ennen esimerkiksi työpaikan pelisäännöistä oli huomattavasti helpompaa sopia työntekijän ja työantajan välillä, sillä työ oli aiemmin huomattavasti enemmän sidottua itse työpisteeseen tai työpaikkaan.

Työaikana ei hoidettu omia asioita, eikä vapaa-ajalla työasioita. Nykypäivänä kuitenkin esimerkiksi työpaikalta saatu puhelin tai kannettava tietokone kulkee työntekijän mukana tämän kotiin ja saattaa velvoittaa työntekijää olemaan tavoitettavana myös vapaa-aikana mukaan lukien loma-aikoina. Toisaalta sama työntekijä surffailee samalla laitteella YouTubessa, nettisivuilla ja päivittää tilapäivityksiä sosiaaliseen mediaan. Saman laitteen kautta työntekijä voi lähettää työsähköposteja ja päivittää sekä omaa että organisaation sosiaalista mediaa (Järvinen 2010, 279). Edellä mainittu asetelma tekeekin esimerkiksi työntekijöiden seurannasta kinkkisen: mitä ja miten työnantaja voi valvoa palkallistensa käyttäytymistä sosiaalisissa medioissa rikkomatta lakia ja toimimatta ylivalvovana isoveljenä?

Uusi tekniikka uusine palveluineen avaa työntekijöille myös uusia mahdollisuuksia erilaisten virheiden tekemiseen. Kiire tai uusien toimintojen vieraus voi johtaa väärän kuvan päätymisen väärälle henkilölle tai työntekijä voi julkaista isolle yleisölle sellaisen viestin, joka oli tarkoitettu vain pienelle ydinryhmälle (Järvinen 2012, 25). Matala kynnys virheiden tekemiseen yhdistettynä tiedon leviämisnopeuteen ja säilymisaikaan internetissä onkin sekä työnantajan että työntekijän kannalta uhkaava yhdistelmä.

Sähköpostiviestien ja erilaisten verkon ylitse kulkevien viestien ja sosiaalisen median palveluiden viestien saaminen sekä vastaanottaminen kuuluvat sananvapauteen, joten työnantaja ei voi ennaltaehkäisevästi kieltää kokonaan työntekijöitään käyttämästä kyseisiä palveluita työaikana ja -paikalla. Työntekijällä onkin oikeus seurata sosiaalisen median palveluita myös työaikana, mikäli sen ei katsota haittaavan työtehtäviä. Työaikana ja organisaation laitteilla tapahtuvaa viestintää voidaan kuitenkin työnantajan toimesta tietyissä määrin rajoittaa, jos esimerkiksi työpaikan toimintaympäristö tai työtehtävien laatu tätä edellyttää (Pesonen 2013, 151).

Lähtökohtaisesti työntekijällä on oikeus käyttää sananvapauttaan, mutta työnantajalla on myös oikeus reagoida, mikäli työntekijä loukkaa esimerkiksi muun henkilökunnan, yrityksen tai asiakkaiden oikeuksia. Työtilanteessa työsuhde, omistussuhde sekä viestintäsuhde ovat kaikki olemassa

samanaikaisesti luoden sekä oikeuksia että velvollisuuksia eri osapuolille. Tietyissä tilanteissa kaikki oikeudet eivät voi toteutua yhtäaikaisesti ilman, että jokin oikeus väistyy. (Pesonen 2013, 180-182). Organisaatio voi esimerkiksi estää työntekijää paljastamasta yritys- ja liikesalaisuuksia työsopimuslain nojalla (Työsopimuslaki 3:4§).

4.2 Sosiaalisen median tietoturvauhkien ennaltaehkäisy yrityksessä

4.2.1 Tietovuodot

Suomen valtion perustuslain nojalla työntekijällä on ”oikeus ilmaista, julkistaa ja vastaanottaa tietoja, mielipiteitä ja muita viestejä kenenkään ennakolta estämättä” (Perustuslaki 731/1999, 12 §). Työnantajalla on kuitenkin oikeus myös reagoida työntekijänsä viestimiseen, mikäli se loukkaa yrityksen, henkilökunnan tai asiakkaan oikeuksia. Lisäksi lojaliteettivelvollisuus sekä erilaiset sopimukset työnantajan kanssa rajoittavat työntekijän viestimis-oikeuksia sosiaalisessa mediassa, mikäli yrityksellä on omat profiilinsa sosiaalisessa mediassa, on sivuista vastaavien työntekijöiden noudatettava työnantajan ohjeistuksia tilien hallinnoinnista. Olipa kyse työntekijän henkilökohtaisesta tai työnantajan profiilista, on yrityksessä hyvä olla tietyt säännöt ja ohjeistukset, jotta niihin voidaan viitata esimerkiksi tarkoituksellisten tai tarkoituksettomien tietovuotojen tullessa julki (Pesonen 2013, 180, 182, 187). Työsopimuslain salassapitovelvoitteen mukaisesti työntekijän ei ole sallittua työsuhteen voimassaolon aikana käyttää omaksi tai muiden hyödyksi työnantajansa liike- tai ammattisalaisuuksia (Andreasson, Koivisto 2013, 17-19).

Yrityksessä tulisi myös varautua ennalta siihen, että yrityksen sosiaalisen median tileistä vastaava työntekijä tai työntekijät irtisanoutuvat. Pahimmassa tapauksessa yksittäinen työntekijä on avannut yrityksen viralliset sosiaalisen median tilit yhdistäen ne työsähköpostiinsa ja omaten näin valmiudet tilien muuttamiseen irtisanomistilanteessa. Tilejä avatessa tulisikin luoda peli-säännöt siitä kuka tilit omistaa ja miten niiden kanssa menetellään irtisanomis-

tilanteessa. Vastaavat pelisäännöt tulisi luoda ennakkoon myös työntekijöiden henkilökohtaisten, mutta työnantajansa nimissä luotujen profiilien suhteen (Pesonen 189, 190).

Työnantajan tulisi aina ennen organisaation tai työntekijöiden ”viemistä” sosiaalisen median palveluun ottaa muun valmistelun ohella selvää kyseisen palvelun tavoista kerätä ja käsitellä käyttäjiinsä liittyviä tietoja. Lisäksi etukäteen tulisi arvioida riskejä, joita palveluun liittyminen organisaationa tai yksittäisinä organisaation edustajina sisältää – kuinka ennaltaehkäistä arkaluonteisten asiakas- tai yritystietojen vuotamista julkisuuteen. Tietovuoto voi pahimmillaan aiheuttaa taloudellista vahinkoa, organisaation asiakkaalle kärsimystä ja se voi asettaa tietovuotoon liittyvän osapuolen vaaraan. Tietovuodon myötä organisaatio voi pahimmillaan menettää ammattimaisen uskottavuutensa sekä asiakkaidensa luottamuksen, jolla voi olla yrityksen taloudelle merkittävät, mutta vaikeasti mitattavat seuraukset. Työntekijöiden keskinäinen juoruilu ei sinänsä ole uusi ilmiö työpaikoilla, mutta sosiaalisessa mediassa tapahtuvassa viestinnässä lipsautettu yksityiskohta tai muu vahingossa julki tullut, tapaukseen tai ihmiseen yhdistettävissä oleva tieto leviää sellaisenaan internetin välityksellä kahvihuoneen lähipiiriä huomattavasti laajemmalle kuulijakunnalle. Juurikin tiedon hankalasti hallittavan leviämisen takia organisaatiossa tulisi olla selvät ohjeet siitä mitä työhön liittyviä asioita saa käsitellä sosiaalisessa mediassa ja mitkä asiat tulisi ehdottomasti jättää sosiaalisesta mediasta pois.

Sosiaalisen median uhat eivät kohdistu yritykseen ja sen työntekijöihin ainoastaan sähköisesti ja verkon ylitse. Monessa yrityksessä sekä työntekijöiden että organisaation virallisia sosiaalisen median tilejä hallinnoidaan niin sanotusti tien päällä kannettavalla tietokoneella, tabletilla tai älypuhelimella erilaisissa tapahtumissa, työmatkoilla ja muilla julkisilla paikoilla. Tämä tuo mukanaan omat uhkansa liittyen muun muassa sosiaalisen median kautta tapahtuviin tietovuotoihin. Työntekijä voi esimerkiksi unohtaa käyttämänsä laitteen julkiselle paikalle tai jättää huolimattomuuttaan jättää tilin kirjautuneeksi ja laitteen lukitsematta poistuessaan laitteen ääreltä lyhyeksi ajaksi. Tästä syystä työntekijöitä tulisikin ohjeistaa erityiseen

tarkkaavaisuuteen kaikkien mukana kulkevien laitteiden kanssa. Riskien minimoimiseksi tulisikin ehdottomasti välttää erilaisia automaattikirjautumisia, tilien yhdistämisiä ja laiskaa samojen salasanojen kierrättämistä eri palveluissa. Myös salasanojen tallentamista verkkoselaimiin tulisi työlaitteissa ja -tileissä välttää.

Muistilista tietovuotoihin valmistautumiselle:

- Ohjaa asiakas, yhteistyökumppani tai muu sosiaalisen median pikaviestimellä yhteyttä ottanut kontakti aina yrityksen asiakastuen sähköpostiin tai muuhun asiaan liittyvään sähköpostiosoitteeseen. Näin tilin pikaviestiarkisto pysyy mahdollisimman pienenä ja mahdollisen käyttäjätunnusvarkauden tapahtuessa se ei sisällä esimerkiksi luottamuksellista tietoa asiakkaista tai organisaation työntekijöistä.

- Sosiaalisen median tilejä on käytettävä ainoastaan ennalta määrättyyn tehtävään (asiakaspalvelu, mainonta tai muu). Esimerkiksi erilaisten Facebook-testien ja -pelien käyttämistä tulisi välttää työntekijöiden sekä yhtiön virallisilla tileillä, sillä ne voivat kerätä ja välittää edelleen muun muassa omia tai kontaktilistan profiilitietoja.

- Sosiaalisen median päivityksen (kuva, suora lähetys, video, teksti tmv.) sisältäessä informaatiota esimerkiksi yhteistyökumppanista, on asia varmistettava kyseisen yrityksen edustajalla. Yritysten tietoturvalinjaukset voivat poiketa toisistaan merkittävästi, jolloin toiselle tavallinen tilapäivitys voi olla toiselle yritykselle tietoturvalinjausten vastainen.

- Luo työntekijöille selkeä ohjeistus aiheista ja asioista joista ei ehdottomasti ole aiheellista, missään muodossa keskustella julkisesti tai yksityisesti pikaviestein sosiaalisessa mediassa. Linjaus olisi suotavaa tehdä yhdessä esimerkiksi organisaation viestinnästä vastaavan osaston kanssa. Opastukseen on hyvä sisällyttää myös esimerkkejä ns. ”hyvistä” ja positiivisista aiheista ja skenaarioista.

- Viestintävastaavan kanssa on luotava jo ennen yhtiön siirtymistä sosiaaliseen mediaan toimintastrategia mahdollisen tietovuodon varalta. Julkisuuteen välittyvä ripeä ja määrätietoinen toiminta minimoi vuodon seuraukset ja luo organisaatiosta uskottavamman.

- Ohjeistuksessa tulisi asettaa kaikkien kirjautumistietojen, kuten salasanojen, verkon yli tapahtuvalle jakamiselle ehdoton nollatoleranssi.

- Tapahtumissa tai luentotilaisuuksissa voidaan asettaa älypuhelimille ja sosiaalisille medioille nollatoleranssi esimerkiksi tiettyyn kellonaikaan tai hetkeen saakka, esimerkiksi tilaisuuden ”virallisen” osuuden ajan. Tilaisuudessa voidaan myös kerätä osallistujien älylaitteet säilöön, jotta vältytään esimerkiksi suorien lähetysten aiheuttamilta tietovuodoilta.

4.2.2 Identiteettivarkaudet

Sosiaalisen median kautta tapahtuviin identiteettivarkauksiin ja niiden kautta suoritettaviin petosyrityksiin voi varautua esimerkiksi soveltamalla Viestintäviraston ohjeita sähköpostitse tapahtuvien identiteettivarkauksien ja huijausyritysten tunnistamiseen. Sosiaalisessa mediassa lähestyvän yksilön tai yrityksen profiilin tietoihin ja identiteettiin ei tule sokeasti luottaa eikä vakuuttavista tiedoista tule hämääntyä. Yrityksen edustaja voi esimerkiksi yrittää lähestyä kontaktia puhelimitse tai etsiä hänestä lisätietoja eri väyliä hyödyntäen ja erilaisten käyttäjätunnusten ja salasanojen luovutusta tulee ehdottomasti välttää.

Kuten muissakin yritysmaailman tietoturva-asioissa, myös identiteetti-varkauksien ja niihin liittyvien huijausten tunnistaminen onnistuu parhaiten kouluttamalla työntekijöitä tunnistamaan erilaisia huijaustapoja ja variaatioita (Viestintävirasto 2010).

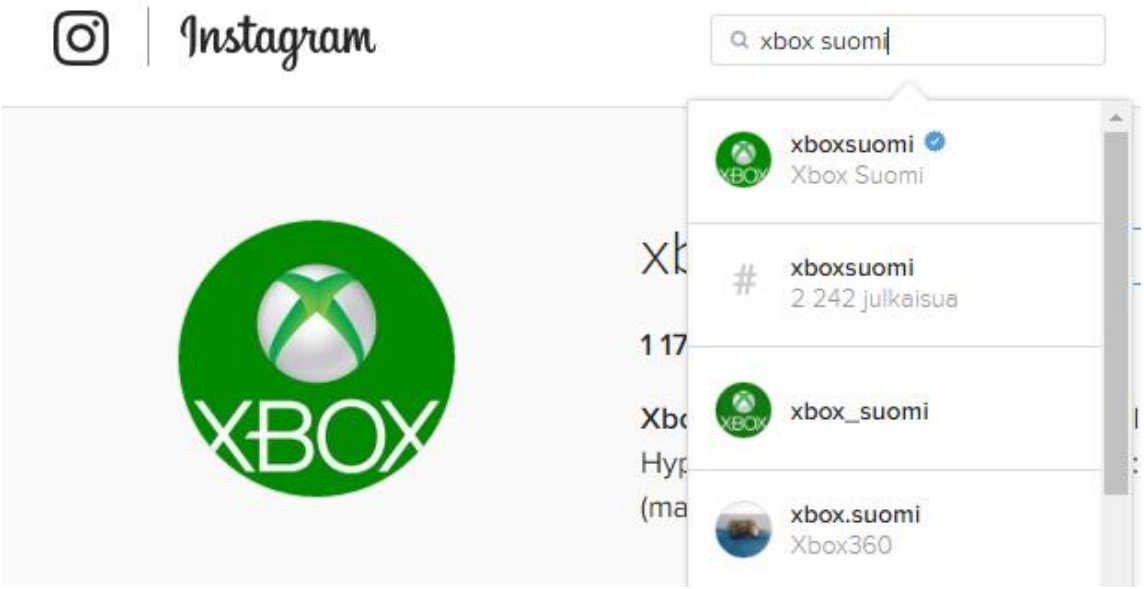
Valeprofiilin merkkejä voi olla esimerkiksi vähäisen jaettavan tiedon määrä, esimerkiksi esiintyminen ainoastaan nimellä. Myös netin hakukoneilla voi etsiä

tapauksen profiilista löytyviä yhteystietoja tai suorittaa tilin profiilikuvalla kuvahaku. Kuvahaun suorittamalla paljastuu, mikäli profiilikuva on otettu käyttöön esimerkiksi kuvapankista tai jostain toisesta, aidosta profiilista. Lisäksi profiilin edustaman yrityksen kotisivuilla voi olla linkkejä yrityksen tai yrityksen edustajien sosiaalisten medioiden profiileihin. Esimerkiksi Suomen nettipoliisien profiilit löytyvät poliisin verkkosivuilta (Forss 2015, 101-103). Muita valetilin merkkejä voi löytää tarkastelemalla tilin verkostoja: vaikuttavatko esimerkiksi tilin kontaktit aidoilta? Minkälaisia tilejä kyseisen tilin kontakteista löytyy? Esimerkiksi vuonna 2015 Suomen ulkoministeri Timo Soini ”liittyi” mikroblogipalvelu Twitteriin. Tilin kontaktilista muodostui kuitenkin pääasiassa turkkilaisista profiileista ja tili julkaisi kieliopillisesti kehnoa, englanninkielistä sisältöä. Tili paljastui valetiliksi Ulkoministeriön tiedotettua asiasta (Vehkoo 2016). Sosiaalisessa mediassa seuraajien määrä tai muu tilastollinen ”suosio” ei ole automaattinen merkki tilin aitoudesta. Käytännössä missä tahansa sosiaalisen median palvelussa on mahdollista lyhyessäkin ajassa ostaa erilaisten palveluiden kautta tilille valeseuraajia, eli botteja (Symantec 2016, 31).

Identiteettivarkaus voidaan suorittaa sosiaalisen median palveluissa esimerkiksi siten, että luotuun profiiliin tuodaan kohteesta julkisesti saatavilla olevia tietoja ja valokuva. Aidon tiedon sekaan upotetaan valheellista tai haitallista tietoa, jolla pyritään esimerkiksi levittämään disinformaatiota tai aiheuttamaan kohteelle ja tämän edustamalle organisaatiolle sosiaalista vahinkoa.

Yksi tapa ennaltaehkäistä valeprofiilien leviäminen on luoda henkilölle tai organisaatiolle aito tili ja verifioida kyseinen tili tai tilit. Suurimmat sosiaalisen median palvelut, kuten Facebook, Twitter ja Instagram mahdollistavat tilin ”varmentamisen”, jonka avulla voidaan vahvistaa kyseisen tilin olevan virallinen tuotemerkin, organisaation tai yksityisen henkilön tili. Tilin varmennuksen jälkeen palvelun käyttäjät näkevät kyseisen tilin nimen vieressä varmennusta kuvaavan merkin esimerkiksi hakutuloksissa ja profiilisivulla (Kuva 9). Tilin varmennusta voidaan anoa kyseisen palvelun valmiilla lomakepohjalla (Twitterin www-sivut, 2016).

Sosiaalisessa mediassa toimivien valeprofiilien tuntomerkkejä ovat muun muassa: geneerinen – mahdollisesti julkisesta kuvapankista haettu – profiilikuva, tilin historiasta (aikajana) ei löydy juurikaan itse tuotettua sisältöä, tilin kontaktilista on tuotetun sisällön määrään nähden silmiinpistävän laaja, profiili tuottaa kieliopillisesti huonoa ja luultavasti automaattikääntäjällä käännettyä tekstiä, tili levittää paljon lyhytosoitteisia linkkejä, joista ei selviä mihin se todellisuudessa ohjaa tai tili levittää esimerkiksi taloudellisesti tarjouksia, jotka yksinkertaisesti ovat liian hyviä ollakseen totta.



Kuva 9: Verifioitu tili erottuu jo hakutuloksessa mahdollisista vale-, tai jäljittelytileistä. Kuvassa kuvapalvelu Instagramin tilien profiilikuvat ja tilien nimet muistuttavat toisiaan, mutta sininen merkki erottaa virallisen Xbox Suomen tilin tätä jäljittelevästä valetilistä (Instagramin www-sivut 2016).

Mahdollisista vakavista huijausyrityksistä tulisi informoida työyhteisön lisäksi myös Kyberturvallisuuskeskusta. Valeprofiileista voi yleensä raportoida käytetyn sosiaalisen median omien työkalujen kautta.

Muistilista identiteettivarkauksilta valmistautumiselle:

- Sisällytä sosiaalisen median tietoturvaoppaaseen lyhyet ja yksinkertaiset ohjeet tekaistun profiilin tai ns. ”bottitilin” tunnistamiseen.

- Mikäli sosiaalisen median palvelu mahdollistaa, verifioi yhtiön virallinen tili, jotta se erotetaan mahdollisista matkija- ja huijariprofiileista.

- Määrittele esimerkiksi yhtiön sosiaalisen median parissa työskentelevä henkilö seuraamaan aktiivisesti mahdollisia yhtiöön tai sen avainhenkilöihin kohdistuvien huijaritilien ja -kampanjoiden ilmaantumista. Suomen laki ja virkavallan toimivaltuudet eivät yllä ulkomaisomisteisiin verkkopalveluihin, joten aktiivinen seuranta, omalle yhteisölle tiedottaminen ja palveluntarjoajalle raportoiminen ovat yhtiön työkaluja identiteettivarkauksiin.

4.2.3 Käyttäjätunnusvarkaudet

Organisaation työntekijä voi havaita käyttäjätunnuksensa joutuneen vääriin käsiin muun muassa seuraamalla käyttämiään sähköposteja aktiivisesti. Mikäli sähköpostiin alkaa tulla ilmoituksia esimerkiksi nettipalveluista, joihin ei ole itse liittynyt, voidaan alkaa epäillä jonkintasoista käyttäjätunnusvarkautta (Rousku 2014, 227).

Yksilön osalta salasana on tärkein yksittäinen tietoturvaan liittyvä asia, josta hänen on pidettävä huolta (Pönkä 2014, 63). Käyttäjän tulisi välttää verkkopalveluiden perinteistä salasanojen turvakysymysten käyttöä, sillä vastaus niihin saattaa pahimmassa tapauksessa löytyä kyseisen käyttäjän Facebook-profiilia tutkimalla. Lisäksi turvakysymyksissä vastaukset voivat olla hyvin helposti arvattavissa – jos kysymyksessä kysytään lempiruokaa, on englantia puhuvissa maissa 19,7 % todennäköisyydellä vastaus pizza (Bursztein & Caron 2015).

Aina yksilön tai koko yhtiön asiallinen salasanapolitiikkakaan ei riitä, silloin tällöin jokin tunnettu verkkopalvelu tiedottaakin mittavista salasanavuodoista. Esimerkiksi vuonna 2012 yli 6,4 miljoonan LinkedIn-salasanan kerrottiin vuotaneen vääriin käsiin (Whittaker 2012).

Käytännössä aina siellä missä on suosittu palvelu käyttäjätunnuksineen, siellä on myös tunnuksia havittelevia rikollisia. Usein muun muassa käyttäjä-tunnusvarkauksista puhuttaessa moni tuudittautuu siihen, ettei juuri hänen tunnuksestaan kukaan hyödy mitään. Työntekijöitä opastaessa olisikin tärkeää huomioida, että ns. henkilöön kohdennetut käyttäjätunnusvarkaudet ovat vain osa tapauksista, yleensä tunnusvarkaudet on automatisoitu esimerkiksi herkästi leviävän haittaohjelman avulla. Työntekijöille tulisikin selvittää sosiaalisen median tietoturvaoppaassa, että käyttäjätunnus-varkauden motiivina on lähes aina raha ja taustalla rikollista toimintaa: anastettu tili toimii kauppatavarana rikolliselle.

Usein yrityksissä on kiellettyä liittää henkilön työsähköpostia tämän sosiaalisen median profiiliin, jotta niitä kohtaan ei suoritettaisi ulkoa suuntautuvia hyökkäyksiä. Tilien yhteydessä käytettävien sähköpostien salasanoista on myös huolehdittava, jotta hyökkääjä ei voi tilata some-profiilille uutta salasanaa. On myös tärkeää, että henkilöt eivät käytä sähköpostinsa salasanaa sosiaalisten medioiden salasanoina. Työntekijöitä tulisi myös opastaa fiksuun salasanapolitiikkaan ja työssä aiemmin määriteltyjen vahvojen salasanojen käyttöön.

Muistilista käyttäjätunnusvarkauksien varalta valmistautumiselle:

- Tilien salasanoissa noudatettava yrityksen yleistä salasanapolitiikkaa. Tarvittaessa tehdään ohjeistus vahvasta salasanasta (numerot, erikoismerkit, merkkisarjat, minimipituus 10 merkkiä). Vahva ja uniikki salasana vaikeuttaa sen arvaamista ja laskennallista murtamista.

- Salasanat tulee uusia kolmen kuukauden välein, vanhoja salasanoja ei saa kierrättää. On vältettävä ehdottomasti käyttämästä samaa salasanaa tiliin yhdistetyn sähköpostin tai tiliä hallinnoivan salasanan kanssa. Jos sosiaalisen median tiliä hallinnoi useampi työntekijä, vastaa salasanojen vaihtamisesta kyseisestä tilistä vastuussa oleva henkilö, jotta salasanojen uusiminen todella toteutuu.

- Mikäli yrityksen virallista sosiaalisen median tiliä tai tilejä hallinnoinut henkilö irtisanoutuu, tai vaihtaa toimipaikkaa, on hänen hallinnoimien tilien salasanat vaihdettava

- Salasanoja ei tule tallentaa esimerkiksi www-selaimeen, eikä niitä tule säilyttää sellaisenaan tietokoneella

- Jos palvelu käyttää salasanojen palautuksissa turvakysymyksiä, on niihin luotava oma, arkistoitu, salasana, selkokielisen vastauksen sijaan.

- Työntekijöitä ohjeistettava julkisilla paikoilla työskentelemisen riskeistä. Tietokonetta, tablettia tai älypuhelinta ei saa jättää yksin valvomatta edes lyhyen vessareissun ajaksi, eteenkään sosiaalisen median palveluihin kirjautuneena.

- Ennalta määrätyn, esimerkiksi yrityksen tietoturvasta tai sosiaalisen median tileistä, vastaavan henkilön tulisi aktiivisesti seurata Viestintäviraston tiedotteita mahdollisista käyttäjätunnus- tai salasanavuodoista niistä palveluista, joihin yritys tai yrityksen työntekijät ovat rekisteröityneet.

- Salasanapolitiikkaa ei tule viedä liian ”äärimmäiseksi”. Ihmisen muisti on rajallinen ja liian tiukka ja työskentelyä huomattavasti haittaava salasanapolitiikka ajaa työntekijät suurella todennäköisyydellä kiertämään annettuja sääntöjä.

- Vältä eri sosiaalisen median tilien yhdistämistä toisiinsa. Yksi kaapattu tili mahdollistaa kaikkien siihen linkitettyjen tilien hallinnoimisen, jonka myötä seuraukset ovat huomattavasti suuremmat.

4.2.4 Tietojen kalastelu ja vakoilu

Tietojen kalastelulta suojautumiseen vaaditaan yksilöltä erityistä tarkkaavaisuutta eri palveluiden käytössä. Työntekijä voi huomaamattaan

menettää kirjautumistietonsa ilman, että on klikannut yhtäkään saastunutta linkkiä tai ladannut työpisteeseensä vakoiluohjelmia (Kyberturvakeskus 2014, 7). Yksilön on kriittisiä tietoja syöttäessään tarkkailtava muun muassa selaimen kohdeosoitetta sekä sitä, onko sivuston yhteys salattu. Kirjautumis-, luottokortti- tai muita kriittisiä tietoja ei tule lähettää missään palveluissa yksityisviestitse, vaikka käyttäjää niin vaadittaisiin tekemään (Facebookin www-sivut 2016).

Lähtökohtaisesti tuoreisiin, yhteyttä ottaneisiin, kontakteihin olisi syytä suhtautua vähintäänkin varauksellisesti. Työntekijän hälytyskellojen tulisi soida viimeistään silloin, jos tuore kontakti alkaa esittää kysymyksiä yritykselle arkaluontoisista aiheista ja ohjailee keskustelua kyseiseen suuntaan. Ei ole epäkohteliasta varmistaa kontaktin henkilöllisyyttä kasvotusten tai vaikka puhelimitse, tai pyytää lähestymään projektista virallisempaa väylää pitkin, esimerkiksi työsähköpostia käyttäen. Tietoja urkkivalla taholla saattaa olla jotain muita väyliä pitkin hankittua julkistamatonta faktatietoa, joita esittämällä hän luo uhrille itsestään uskottavampaa ja luotettavampaa kuvaa.

Tietyissä tapauksissa työntekijät luottavat liikaa vanhentuneeseen tietoon, jonka mukaan arkaluonteisia tietoja kalastelevat huijausviestit tai -kampanjat ovat aina englanninkielisiä. Nykypäivänä kuitenkin automatisoidut kääntäjät mahdollistavat kohdennettujen hyökkäysten tekemisen käytännössä millä kielellä tahansa. Yleisesti Internetissä, varsinkin sosiaalisessa mediassa, tulisikin unohtaa perinteiset ajatukset etäisyyksistä, rajoista ja ”turvallisista kolkista”.

Kuva 10. Tietoja voidaan kalastella sensaatiomaisen videon muodossa, jota ei todellisuudessa ole olemassa. Kuvan tapauksessa linkin klikanneilta kerätään erilaisia henkilötietoja (Digitoday.fi, 2014).

Muistilista tietojen kalastelun ja vakoilun varalta valmistautumiselle:

- Ohjeista työntekijöitä aina varmistamaan esimerkiksi yhteistyökumppanin, asiakkaan tai kollegan sosiaalisen median profiilin aitous.

- Kriittiset työhön, työpaikkaan tai tiettyyn projektiin liittyvät asiat tulisi hoitaa sosiaalisen median ulkopuolella.

- Virallista työsähköpostia tai sosiaalisen median tunnusta ei tule käyttää missään sosiaalisen median kautta tapahtuvassa arvonnassa, kilpailussa tai muissa osallistumistietoja vaativassa aktiviteetissa.

- Eri palveluiden kirjautumistietojen välittäminen sosiaalisen median pikaviestimissä tulisi kieltää ennakkoon, sillä kaappari saattaa kysyä tiettyä kriittistä tietoa kaapattua kollegan profiilia hyväksikäyttäen. Lisäksi pikaviestimellä lähetetyt, kriittistä tietoa sisältävät, viestit jäävät kyseisen

palvelun viestihistoriaan luettavaksi esimerkiksi mahdollisen käyttäjätunnus-varkauden tapahtuessa. Huijarit voivat käyttää myös työntekijän lomaan tai muuhun liikkumiseen liittyviä tilapäivityksiä hyväkseen esiintymällä kyseisenä henkilönä pyytäen unohtunutta salasanaa tai vastaavaa.

- Suunnittele millä alustalla ja miten työntekijät voivat varoittaa toisiaan tuoreista tietojen kalasteluista tai vakoiluyrityksistä. Usein sekä automatisoidut että manuaalisesti toimivat huijarit yrittävät samaa tai samantapaista huijausta useaan yksittäisen toimijaan samassa organisaatiossa, jolloin huijauksen tunnistaminen helpottuu.

- Huomioi organisaation tietoturvaohjeistus myös sosiaalisen median tiedusteluissa: mitä on sopivaa kertoa esimerkiksi lomailevasta työntekijästä.

4.2.5 Haittaohjelmat ja sovellushaavoittuvuudet

Paras tapa haittaohjelmilta ja haavoittuvuuksilta suojautumiseen yksilön kannalta on huolehtia päätelaitteilla olevien sovellusten päivityksistä ja asiaan kuuluvasta virustorjuntaohjelmistosta. Säännöllisten ohjelmapäivitysten lisäksi on hyvä huolehtia monikerroksisesta suojautumisesta. Säännöllisin väliajoin on myös hyvä tarkastaa asennetut ohjelmat ja poistaa sellaiset ohjelmat, joita ei enää käytä. Työntekijän olisi myös hyvä asentaa omille laitteilleen apu-ohjelma, joka tarkastaa tietokoneella olevien sovellusten tietoturvallisuuden. Ohjelma tarkastaa sovellusten haavoittuvuudet, ilmoittaa vanhentuneesta sovelluksen versiosta ja helpottaa saatavilla olevien sovelluspäivitysten lataamisessa (Rousku 2014, 221).

Kiristysohjelma saattaa lukita pahimmassa tapauksessa uhrin laitteen kokonaan vaatien tätä suorittamaan esimerkiksi lunnasmaksun. Olipa vaatimus mikä tahansa, ei uhrin tulisi missään tapauksessa suorittaa vaadittuja lunnasmaksuja tai -tekoja. Yrityksen työntekijöitä tulisikin opastaa jo yleisessä tietoturvaohjeistuksessa, että Suomen, tai minkään muun valtion, viranomaiset eivät lukitse kansalaisten laitteita laittoman materiaalin hallussa-

pidosta tai muustakaan syystä. Viranomaiset eivät myöskään pyydä kansalaisiaan maksamaan ikinä minkäänlaisia maksuja tai sakkoja hyvityksenä esimerkiksi laittoman materiaalin hallussapidosta laitteellaan. Huijauksiin ei tule ikinä lähteä mukaan, eikä uhkasakon maksaminen muuta tilannetta mitenkään (Andreasson, Koivisto, Ylipartanen 2014, 27).

Ohjelmien lisäksi myös itse käyttäjä toimineen on suuressa vastuussa päätelaitteen turvallisuudesta. Sosiaalisessa mediassa vastaan tulevien linkkien kautta ei kannata ladata mitään, vaan kaikki selainlaajennukset, ohjelmat ja vastaavat kannattaa ladata suoraan niiden kehittäjien kotisivuilta. Älä myöskään vastaa esimerkiksi Facebookin, LinkedInin tai Twitterin nimissä lähetettyihin sähköposteihin (Krebs 2014, 239-241). Yleisesti tiedostojen ja linkkien jakamisesta kannattaa tehdä organisaatiossa selkeä linjaus. Yhtenä esimerkkinä on ohjeistaa työntekijöitä jakamaan työhön liittyviä tiedostoja tai tiedostolinkkejä ainoastaan sähköpostitse, erilaisten pilvipalveluiden välityksellä tai muiden tiedostojen jakeluun erikoistuneita palveluita hyödyntäen.

Mikäli työntekijä havaitsee työnantajaltaan käyttöön saadulla laitteellaan sosiaalisen median kautta levinneen haittaohjelman, tulee hänen toimia organisaation yleisten tietoturvaohjeistusten mukaan. Työntekijä voi ensitöikseen ottaa tapahtuneesta haittaohjelmaan liittyvästä ilmoituksesta kuvakaappauksen tai kuvan ja tallentaa sen. Työntekijän ei tule yrittää haittaohjelman poistamista itse eikä sammuttaa virtaa työlaitteesta. Sen sijaan laitteen tietoliikenneyhteydet kannattaa IT-tukihenkilöä odotellessa katkaista (Rousku 2014, 216).

Muistilista haittaohjelmien ja sovellushaavoittuvuuksien varalta valmistautumiselle:

- Päätelaitteen käyttöjärjestelmän, sovellusten päivittäminen ja yleinen suojaus hoidetaan yrityksen tietoturvalinjauksen mukaan, mielellään keskitetysti sekä automatisoidusti.

- Erilaisten selainlaajennusten asentaminen työntekijöiden käyttämiin www-selaimiin työkäytössä oleviin laitteisiin tulisi kieltää.

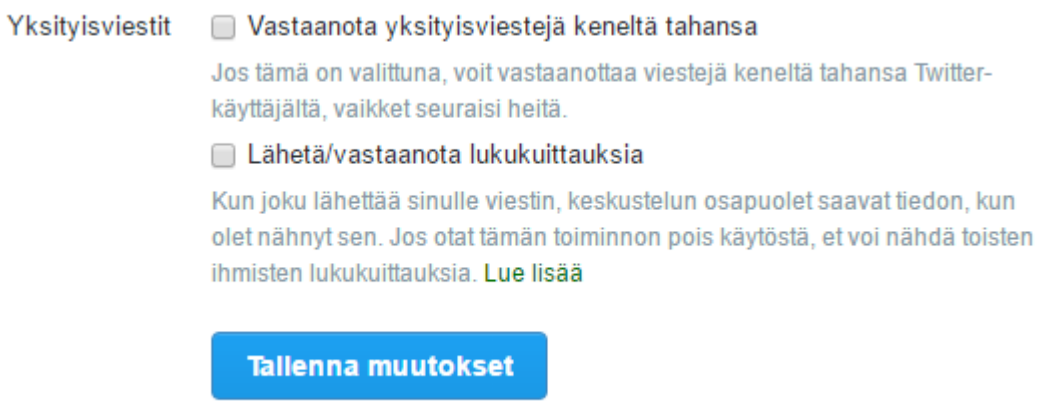
- Työntekijöitä tulisi ohjeistaa erityiseen varovaisuuteen sosiaalisten medioiden kautta levitettävien linkkien avaamiseen. Henkilön tulisi aina varmistua ennen klikkaamista mihin kyseinen linkki vie.

- Työntekijöitä tulee ohjeistaa tunnistamaan sosiaalisissa medioissa leviävät haittaohjelmat ja niiden seuraukset.

- Mikäli työntekijöiden päätelaitteilla (älypuhelin, tabletti) on asennettuna sosiaalisen median sovelluksia, on niiden päivittyminen asetettava automaattiseksi. Päivityksien sisältöä tulee seurata mahdollisten uusien ominaisuuksien ja niiden mukana tulevien tietoturvauhkien varalta.

4.2.6 Roskaposti

Sosiaalisessa mediassa esiintyvästä roskapostista työntekijä kykenee omilla teoillaan vaikuttamaan parhaiten niin sanotun linkkispämmin leviämättömyyteen omilla toimillaan. Työntekijän kannattaa jättää avaamatta linkit, joiden todellista osoitetta ei tiedä (URL-lyhenteet), jos se vaikuttaa vähänkään epäilyttävältä tai jos se vaikuttaa sensaatiomaiselta tai ”liian” lupaavalta. Skriptejä ei kannata koskaan kopioida selaimen osoiteriville ja sovelluksen lupapyynnöt kannattaa lukea aina tarkasti. Jos tutuilta kontakteilta tulee vieraskielinen viesti, jossa kehotetaan klikkaamaan linkkiä, on kyseessä melko varmasti roskaposti (Haasio 2013, 54-55). Eri sosiaalisen median palvelut mahdollistavat myös yksittäisen tilin hiljentämisen tai blokkaamisen, mikäli tietty tili kohdistaa käyttäjään tarpeettoman määrän roskapostia. Eri palvelut sisältävät myös erilaisia tapoja suojautua roskapostilta: esimerkiksi mikroblogipalvelu Twitter mahdollistaa pikaviestien vastaanottamisen rajoittamisen ainoastaan tilin sosiaaliseen verkostoon (Kuva 11). Tässä tapauksessa rajoittaminen tarkoittaa sitä, että asetuksia hallinnoivalle henkilölle voi lähettää pikaviestejä ainoastaan ne tilit, joita kyseinen henkilö tai organisaatio ”seuraa”.



Kuva 11: Kuvakaappaus mikroblogipalvelu Twitterin turva-asetuksista. Poistamalla valinnan ”vastaanota yksityisviestejä keneltä tahansa” tiliä hallinnoiva voi ennaltaehkäistä pikaviestimiä hyödyntävän roskapostin leviämistä (Twitterin www-sivut 2016).

Linkin ”puhtaus” tulisi aina varmistaa ennen sen jakamista yhtiön tai työntekijän virallisen sosiaalisen median tilin välityksellä. Sen lisäksi, että roskapostin jakaminen edesauttaa muille sosiaalisen median käyttäjille haitallisen materiaalin leviämistä, voi se näkyä myös yhtiön imagotappiona ja yhteisöllisen median markkinoiden pienentymisenä.

Useat sosiaalisen median palvelut mahdollistavat käyttäjäänsä määrittämään esimerkiksi sen kuka voi kontaktille lähettää kahdenvälisiä pikaviestejä ja liittää mukaan julkiseen tilapäivitykseen tai kuvaan. Näitä palveluiden työkaluja kannattaa hyödyntää, jotta roskapostibottien yhteydenotot voidaan ennalta estää mahdollisimman tehokkaasti. Esimerkiksi Facebookissa monet tekaistut, yksityishenkilöinä esiintyvät, tilit lähettävät ”oikeille” tileille ystäväpyyntöjä summittaisesti. Henkilön hyväksyessä vastaanotetun kaveripyynnön, lisätään tämä mukaan esimerkiksi huijausmainokseen tai tuotetarjoukseen, joka yleensä sisältää saastuneen tai yleisesti klikkejä kalastelevan linkin. Tilapäivitys, johon kaveripyynnön kutsunut henkilö on lisätty, näkyy eteenpäin hänen kontaktilistalla oleville henkilöille ja lisäksi automatisoitu tili lähettää automaattisesti kaveripyynnön edelleen uhrin kontaktilistan henkilöille ja näin roskaposti etenee jälleen uudelle yleisölle. Muun muassa tästä syystä kontaktiryhmiä sisältävissä palveluissa kuten Facebookissa tai LinkedInissä tulee varmistua esimerkiksi kaveripyynnön

lähettäneen henkilöllisyydestä ennen pyynnön hyväksymistä (Järvinen 2012, 309). Jos pyynnön lähettäjä on esimerkiksi työkollega, voi tilin aitouden varmistaa häneltä jotain muuta kautta. Työpaikan sosiaalisen median ohjeistuksessa olisikin hyvä olla jonkinasteinen linjaus esimerkiksi siitä ketä kollegoita on sopivaa lisätä kontaktilistalleen. Mikäli yritys tai organisaation osasto toimii aktiivisesti sosiaalisessa mediassa, voidaan avainhenkilöiden ja työntekijöiden viralliset, käytössä olevat sosiaalisen median tilit kerätä työntekijöiden saataville, jotta huijaustilit ja identiteettivarkaudet tunnistettaisiin virallisiin listoihin vertaamalla välittömästi.

Muistilista roskapostiin valmistautumiselle:

- Älä koskaan avaa suomenkieliseltä kontaktilta tullutta linkkiä, jonka saate-sanoina on vieraskielinen viesti.

- Kysy tutuiltakin kontakteilta lisätietoja jaetuista linkeistä tai tiedostoista.

- Voit saada roskapostia keneltä tahansa aina esimiehestä kollegoihin tai omiin vanhempiin. Henkilö harvoin tietää itse, että esimerkiksi hänen kauttaan leviää pikaviestien välityksellä haittaohjelma tai saastunut linkki.

- Lue aina ennen kuin klikkaat ”ok”.

- Vältä kaikkia Facebook-ohjelmia ja liitännäisiä, jotka vaativat käyttöoikeuksia seinällesi tai pikaviestimiin.

- Vältä erilaisia kilpailuja tai arvontoja, joissa vaaditaan esimeriksi tietyn linkin jakamista.

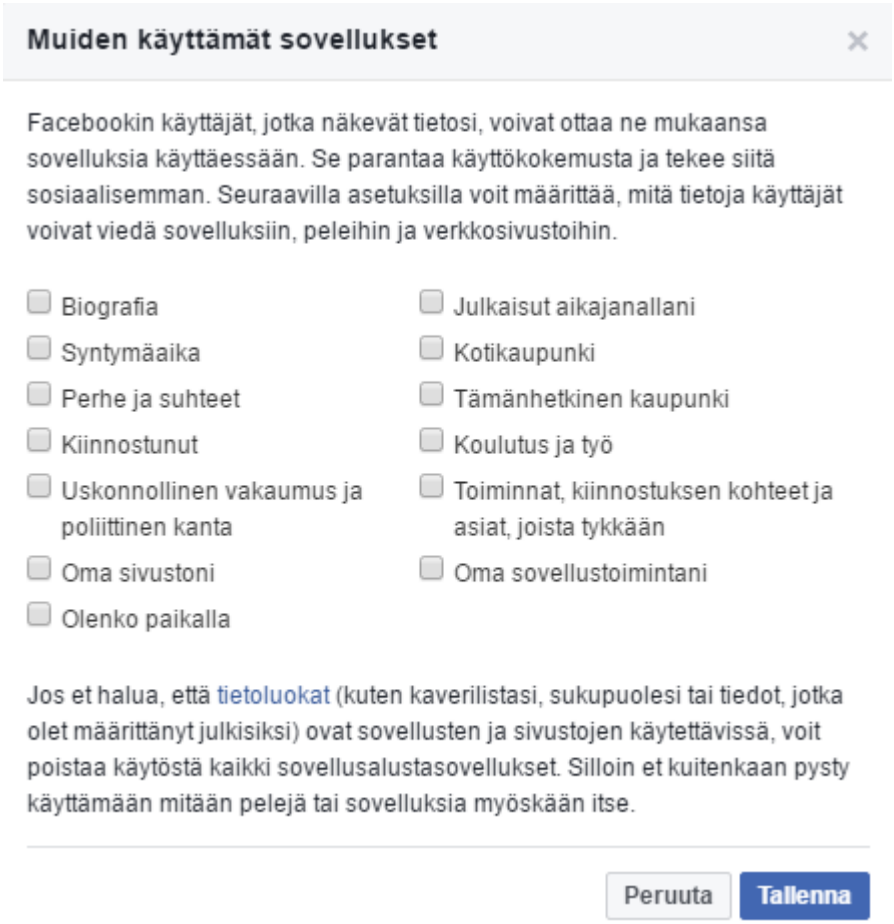
- Älä asenna vahvistamattomia selainlaajennuksia.

4.2.7 Palveluiden sopimusehtoihin liittyvät epäselvyydet

Yrityksessä tulisi paneutua ennen sosiaalisen median tilin luomista kyseisen palvelun sopimusehtojen avainkohtiin: onko kyseinen palvelu tarkoitettu organisaatioiden sijaan ainoastaan yksilöille, minkälaiset käyttöoikeudet palveluntarjoajalla on käyttäjiensä luomaan sisältöön ja missä määrin palveluun luotu tili sisältöineen on mahdollista poistaa.

Sosiaalisen median palveluehtojen suhteen yrityksellä ei juuri ole keinoja ennaltaehkäistä aiemmin mainittuja uhkia. Tilejä hallinnoivan tiimin tulisi aktiivisesti seurata niiden palveluiden sopimusehtojen muutoksia ja muun muassa muuttuvia tekijänoikeusehtoja. Yrityksessä tulisi selvittää muun muassa ovatko palvelun sopimus- ja tekijänoikeusehdot ristiriidassa kyseisen organisaation tai sen yhteistyökumppaneiden omien ehtojen ja sopimusten kanssa.

Useat kolmannen osapuolen piensovellukset esimerkiksi Facebookissa vaativat käyttäjältään usein laajojakin käyttöoikeuksia, mitkä voivat johtaa joko työntekijän tai yrityksen kannalta epämieluisiin yllätyksiin tai ainakin kiusallisiin tilanteisiin. Sovellukset saattavat käyttäjän ehtojen hyväksynnän jälkeen esimerkiksi lähettää henkilön kontakteille erilaisia automaattisia sovellusmainoksia tai -kutsuja, jotka eivät sinällään välttämättä aiheuta tietoturvan kannalta uhkaa, mutta saattavat olla työntekijän tai tämän edustaman yrityksen uskottavuuden kannalta kiusallisia. Facebook mahdollistaa nykyisin käyttäjäänsä estämään kaikkien kolmansien osapuolien sovellusten toiminnan (Kuva 12), jolla voidaan varmistaa käyttäjän profiilitietojen leviäminen erilaisten tietoja keräävien sovellusten kautta.



Kuva 12: Kuvakaappaus Facebookin sovellusasetuksista. Käyttäjän on mahdollista estää sovelluksia ja niiden käyttäjiä käyttämästä hänen profilointiin liittyviä tietoja (Facebookin www-sivut 2016).

Muistilista sopimusehtojen epäselvyyksiin valmistautumiselle:

- Tutustu aina sosiaalisen median palvelun käyttö- ja sopimusehtoihin ennen yrityksen virallisen tilin luomista. Palveluehdoissa ”ok”, ”jatka” tai vastaavan napin klikkaaminen vastaa sopimuksen allekirjoittamista.

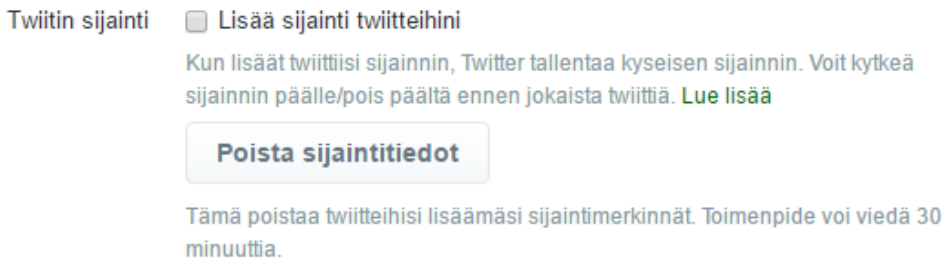
- Selvitä mahdolliset ristiriidat palvelun käyttöehtojen ja yrityksen omien sääntöjen välillä.

- Määritä tietty henkilö seuraamaan tietyin väliajoin palveluiden muuttuvia ehtoja ja mahdollisten uusien ominaisuuksien tuomia muutoksia ehtoihin.

- Kolmansien osapuolien piensovellusten ym. käyttö tulisi niiden usein laajojen käyttöoikeusvaatimusten ja epäselvien ehtojen vuoksi oletuksena kieltää yrityksen virallisilla tileillä.

4.2.8 Paikantamiseen liittyvät uhat

Useat sosiaalisen median palvelut mahdollistavat erilaisten sijaintitietojen liittämisen esimerkiksi kuva- tai tilapäivityksiin. Ominaisuus on kuitenkin lähes jokaisessa tunnetussa palvelussa joko otettava erikseen käyttöön tai kytkettävissä pois päältä. Esimerkiksi sekä Facebook että Twitter (Kuva 13) mahdollistaa paikannustietojen hallinnoinnin tilin asetuksista.



Kuva 13: Muun muassa Twitter mahdollistaa käyttäjää liittämään sijaintitiedot palveluun ladattuihin päivityksiin tai kuviin (Twitterin www-sivut 2016).

Esimerkiksi turvallisuusalalla työntekijöitä tulisi opastaa sijaintitietojen poistamisesta sosiaalisen median palveluiden tilapäivityksistä ja kuva-julkaisuista. Yksittäiset sijaintitiedot eivät välttämättä aiheuta yritykselle tietoturvauhkaa, mutta tipoittain kerätyt paikkatiedot yhdistettynä tiettyyn yksilöön voivat paljastaa esimerkiksi kaavan vartijan kiertotavoissa tai -ajoissa.

Muistilista paikantamiseen liittyviin uhkiin valmistautumiselle:

- Esittele työntekijöille paikannusominaisuuksiin liittyvät uhat kyseisessä yrityksessä.

- Opasta tarvittaessa työntekijöitä poistamaan paikannusominaisuudet palveluiden oletusasetuksista, mikäli kyseinen ominaisuus katsotaan yrityksessä ongelmaksi.

5 POHDINTA

Aloitin opinnäytetyön työstämisen käytännössä jo keväällä 2016 seminaarityön muodossa. Palasin aiheen pariin myöhemmin syksyllä, kun päätin työstää samasta aiheesta myös opinnäytetyön. Työ eteni sekä keväällä että kesällä varsin ripeällä tahdilla: vuosien aikana olin huomioinut erilaisia aiheeseen liittyviä epäkohtia ja esimerkkitapauksia, joiden avulla aihetta oli helppo lähestyä ja työstää eteenpäin. Aiemmin suorittamassani ammatti-korkeakoulun pakollisessa työharjoittelussa hallinnoin erään verkkojulkaisun sosiaalisen median tilejä sekä perehdytin julkaisun muuta henkilökuntaa tilien käyttämisen kanssa, joten osa-alue oli itselle tuttu mahdollisine uhkakuvineen.

Rakensin työn teoriapohjan yhdistelemällä yleistä tietoturva-alan kirjallisuutta erilaisiin verkkojulkaisuihin ja tutkimuksiin sekä viestinnän alan oppaisiin. Sosiaalisen median tietoturvauhat on aiheena melko spesifi ja rajattu, joten tietyissä tapauksissa hyödynsin yleistä tietoturva-alan kirjallisuutta opasta kasatessa. Esimerkiksi yleiset säännöt salasanojen kanssa tai haittaohjelmilta suojautumiseen pätevät yhtä lailla myös sosiaalisen median palveluiden kohdalla. Lisäksi aihealue on hyvin nopeasti kehittyvä ja muuttuva, joten tavoitteenani oli alusta alkaen luoda yleispätevä ohjeistus. Joissakin tapauksissa on mainittu tarkkojakin esimerkkejä tietyistä palveluista, mutta ne on pyritty pitämään ”ajattomina”, jotta materiaali pysyisi ajankohtaisena mahdollisimman pitkään.

Aihe tuntui itselleni hyvin mielenkiintoiselta muun muassa siksi, että sosiaalisen median uhat nähdään useissa tapauksissa enemmänkin viestinnällisinä ongelmina, ei niinkään tietoturvan kannalta. Lisäksi olen kohdannut aiheen parissa useista lähteistä joko tietämättömyyttä, välinpitämättömyyttä tai yllättyneisyyttä. Usein kyseisiä reaktioita on yhdistänyt joko juurikin tietämättömyys tai välinpitämättömyys: sosiaalinen media on ilmiönä melko nuori ja siihen ei välttämättä siitä syystä osata ”muun” verkon tapaan vielä yhdistää työssä ilmenneitä uhkia. Muun muassa näistä syistä halusinkin tehdä aiheesta yleispätevän oppaan, jonka lukemisen jälkeen

yrityksen edustaja tuntisi sosiaalisen median tietoturvauhkien eri tyypit pääpiirteittäin ja erilaisia tapoja tai vaihtoehtoja, kuinka ne voitaisiin huomioida ja mielellään ennaltaehkäistä yrityksen arjessa.

LÄHTEET

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2013. Tietosuojavastaavan käsikirja. Helsinki. Tietosanoma.

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2015. Tietosuojakäsikirja johdolle. Tallinna. Tietosanoma.

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2014. Tietosuojavastaavan käsikirja 2. Tallinna. Tietosanoma.

Andreasson, A., Koivisto, J. 2013. Tallinna: Tietosanoma.

Bursztein, E. & Caron, I. 2015. New Research: Some Tough Questions for 'Security Questions'. Google. Viitattu 12.3.2015. Saatavissa: https://security.googleblog.com/2015/05/new-research-some-tough-questions-for.html.

Cavazza, F. 2016. Social Media Landscape 2016. Viitattu 16.11.2016. Saatavissa: https://fredcavazza.net/2016/04/23/social-media-landscape-2016/.

Centre for the Protection of National Infrastructure. 2014. Good Practice Guide: Online Social Networking. Viitattu 10.1.2017. Saatavissa: https://www.cpni.gov.uk/system/files/documents/ce/fb/online-social-networking.pdf.

Digitoday. 2014. "Katso hirvittävä vuoristorataonnettomuus!" – Näin toimii Facebook-huijaus. Viitattu 16.3.2016. Saatavissa: http://www.digitoday.fi/tietoturva/2014/01/21/katso-hirvittava-vuoristorataonnettomuus--nain-toimii-facebook-huijaus/2014979/66.

Facebook. Ohje- ja tukikeskus. Viitattu 9.3.2016. Saatavissa: https://www.facebook.com/help/320234818071511/.

Facebook. Ohje- ja tukikeskus. Viitattu 12.12.2016. Saatavissa: https://www.facebook.com/help/1584206335211143/.

Forss, M. 2014. Fobban sosiaalisen median selviytymisopas. Helsinki. Crime time.

Franceschi-Bicchierail. 2013. Social Media Spam Increased 355% in First Half of 2013. Viitattu 12.3.2016. Saatavissa: http://mashable.com/2013/09/30/social-media-spam-study/.

Haasio, A. 2013. Netin pimeä puoli. Saarijärvi. Suomalaisen kirjallisuuden seura.

Hiles, A. 2011. Reputation Management: Building and Protecting Your Company's Profile in a Digital World. Bloomsbury Publishing.

Hinton, S. & Hjorth, L. 2013. Understanding social media. Lontoo: Sage Publications.

Hopkins, N. 2012. China suspected of Facebook attack on Nato's supreme allied commander. Washington. The Guardian. Viitattu 15.4.2016. Saatavissa: https://www.theguardian.com/world/2012/mar/11/china-spies-facebook-attack-nato.

Isokangas, A. & Vassinen, R. 2010. Digitaalinen jalanjälki. Hämeenlinna: Talentum.

Instagram. Viitattu 5.1.2016. http://www.instagram.com.

Järvinen, P. 2010. Yksityisyys: Turvaa digitaalinen kotirauhasi. Jyväskylä: Docendo.

Järvinen, P. 2014. Arjen tietoturva. Jyväskylä: Docendo.

Koivunen, E. 2010. Sosiaaliseen mediaan liittyvät tietoturvariskit. Viitattu 7.3.2016. Saatavissa: https://www.vahtiohje.fi/web/guest/2.-sosiaaliseen-mediaan-liittyvat-tietoturvariskit.

Kivioja, K-M. 2016. Oppilaat tekevät salaa suoraa Periscope-lähetystä tunneilta – hämmentyneet opettajat kysyvät apua OAJ:lta. Viitattu 21.11.2016. Saatavissa: http://yle.fi/uutiset/3-8596990.

Korhonen, S. 2014. F-Securen Hyppönen: Orwellin pahin pelko on jo toteutunut. Talouselämä. Viitattu 19.10.2016. Saatavissa: http://www.talouselama.fi/uutiset/f-securen-hypponen-orwellin-pahin-pelko-on-jo-toteutunut-3452012.

Korpela, J. 2005. Turvallisesti netissä. Jyväskylä: Docendo.

Korpimies, A. 2012. Verkkorikollisuus ei ole iso uhka, uskovat suomalaisjohtajat. Viitattu 8.3.2016. Saatavissa: http://www.tivi.fi/CIO/2012-05-04/Verkkorikollisuus-ei-ole-iso-uhka-uskovat-suomalaisjohtajat-3191896.html.

Krebs, B. 2014. Spam Nation. Naperville, Illinois: Sourcebooks.

Kurki, M. 2010. Pk-yrityksen tietotekniikka käytännönläheisesti. 1. painos. Jyväskylä: Helsingin seudun Kauppakamari.

Kuusela, H., Ollikainen, R. Riskit ja riskienhallinta. 2005. Tampere: Tampereen yliopistopaino.

Kähkönen, S. 2016. Facebook-testeistä voi olla vakavat seuraukset – myytkö tietosi ulkopuolisille?. Viitattu 25.11.2016. Saatavilla: http://yle.fi/uutiset/3-8765560

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita.

Lacey, D. 2009. Managing the Human Factor in Information Security. Chichester. John Wiley & Sons Inc.

Leino, A. 2012. Sosiaalinen netti ja menestyvän pk-yrityksen mahdollisuudet. Kopijyvä. Infor.

Linja-Aho, V. 2010. Krakkeri kaupustelee 1,5 miljoonaa varastettua Facebook-tunnusta. Tivi. Viitattu 23.11.2016. Saatavissa: http://www.tivi.fi/Arkisto/2010-04-23/Krakkeri-kaupustelee-15-miljoonaa-varastettua-Facebook-tunnusta-3178477.html.

LinkedIn.com. 2017. Phishing Emails. Viitattu 4.1.2017. Saatavissa: https://www.linkedin.com/help/linkedin/answer/5342?query=phishing.

Livegamers.fi. 2013. Dead Rising 3 bongattu työntekijän CV:stä. Viitattu 7.3.2016. Saatavissa: http://www.livegamers.fi/misc/news.php?shownum=7534.

Lyly-Yrjänäinen, M. 2016. Työolobarometri – syksy 2015. Työ- ja elinkeinoministeriö. Viitattu 25.10.2016. Saatavissa: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/74896/TEMjul_17_2016_28042016.pdf.

Mennie, P. 2015. Social Media Risk and Governance: Managing Enterprise Risk. Kogan Page Publishers. Viitattu 14.11.2016. Saatavissa: https://books.google.fi/books?id=Q82lCgAAQBAJ&dq=social+media+risk+analysis.

Natri, S. 2015. Tietovuoto Facebook-tileistä "vain ajan kysymys". Viitattu 4.12.2016. Saatavissa: http://yle.fi/uutiset/3-8413550.

Nexgate. 2013 State of Social Spam. Viitattu 10.3.2016. Saatavissa: https://docs.google.com/viewer?url=http%3A%2F%2Fnexgate.com%2Fwp-content%2Fuploads%2F2013%2F09%2FNexgate-2013-State-of-Social-Media-Spam-Research-Report.pdf.

Nurminen, J. 2013. Tutkimus: Sosiaalinen media tekee meistä syöksähteleviä sopuleita. Yleisradio. Viitattu 16.3.2016. Saatavissa: http://yle.fi/uutiset/tutkimus_sosiaalinen_media_tekee_meista_syoksahteleviä_sopuleita/6872750.

OSG Viestintä. 2016. Slush-kysely: Startupit tiedostavat tietoturvan tärkeyden, mutta mobiilitietoturvan taso on puutteellinen. Viitattu 25.12.2016. Saatavissa: http://www.epressi.com/media/userfiles/10873/1480403748/slush_mobiilitietoturvatutkimustiedote_291116_.pdf.

Peltomäki J. & Norppa, K. 2015. Rikos meni verkkoon. Helsinki. Talentum.

Periscopen www-sivut. 2017. Saatavilla: https://medium.com/periscope/up-periscope-f0b0a4d2e486#.t3ofao405.

Pesonen, P. 2013. Sosiaalisen median lait. Viro. Lakimiesliiton kustannus.

Porvari, P. 2012. Tietoturvallisuus liiketoiminnan johtamisessa, prosesseissa ja henkilöiden toiminnassa. Väitöskirja. Helsinki: Aalto-yliopisto. Sovellettu elektroniikka.

Purser, S. 2004. A Practical Guide to Managing Information Security. Norwood. Artech House.

Puolustusvoimat. Viitattu 10.3.2016. Saatavissa: http://www.puolustusvoimat.fi/wcm/69bec68041240579ae44ae1c0b52473c/TS_2013_verkkoversio_11.6.pdf?MOD=AJPERES.

Pönkä, H. 2014. Sosiaalisen median käsikirja. Jyväskylä. Docendo.

Rousku, K. 2014. Kyberturvaopas. Viro: Talentum.

Ruuska, K. 2007. Pidä projekti hallinnassa. Helsinki. Talentum.

Suominen, J., Saarikoski P., Turtiainen R. & Östman S. 2013. Sosiaalisen median lyhyt historia. Viro: Gaudeamus.

Suutarinen, M. & Vesterinen, P-L. 2011. Y-sukupolvi työ(elämä)ssä. Hansaprint. JTO.

Symantec Corporation. 2009. Symantec: Heikentyvä talous antaa lisäpuhtia roskapostittajille. Viitattu 16.3.2016. Saatavissa: http://www.symantec.com/fi/fi/about/news/release/article.jsp?prid=20090113_01.

Symantec Corporation. 2015. Internet Security Threat Report, Volume 20. Viitattu 16.3.2016. Saatavissa: https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347931_GA-internet-security-threat-report-volume-20-2015-appendices.pdf.

Symantec Corporation. 2016. Internet Security Threat Report, Volume 21. Viitattu 25.11.2016. Saatavissa: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

Savon Sanomat. Salasanojen määrä on monelle taakaksi. Viitattu 6.3.2016. Saatavissa: http://www.savonsanomat.fi/kotimaa/Salasanojen-m%C3%A4%C3%A4r%C3%A4-on-monelle-taakaksi/724351.

SplashData. 2015. “123456” Maintains the Top Spot on SplashData’s Annual “Worst Passwords” List. Viitattu 15.3.2016. Saatavissa: http://www.prweb.com/releases/2015/01/prweb12456779.htm.

Talouselämä. 2013. Näin helppoa on salasanan arvaaminen - Katso 10 yleisintä. Viitattu 15.3.2016. Saatavissa: http://www.talouselama.fi/uutiset/nain-helppoa-on-salasanan-arvaaminen-katso-10-yleisinta-3442375.

Taloustutkimus 2014. Suomalaiset vahvasti Facebook-kansaa – WhatsApp toiseksi suosituin. Yleisradio. Viitattu 16.3.2016. Saatavissa: http://www.yle.fi/tvuutiset/uutiset/upics/liitetiedostot/yle_somekysely.pdf.

Toivanen T. 2012. Facebook-päivityksellä ei voi muuttaa palvelun käyttöehtoja. Yleisradio. Viitattu 18.12.2016. Saatavissa: http://yle.fi/uutiset/3-6392894.

Tolonen, R. 2015. Jo toinen suomalaisyritys identiteetti-varkauden uhriksi – Affectolta vietiin lähes miljoona euroa. Helsingin Sanomat Viitattu 9.3.2016. Saatavissa: http://www.hs.fi/talous/a1440120852580.

Tolvanen, K. 2016. Varusmiehet koettelevat armeijan rajoja uusin keinoin: "Henkilö kieltäytyi ajamasta partaansa". Yleisradio. Viitattu 21.11.2016. Saatavissa: http://yle.fi/uutiset/3-8949285.

Tranberg, P. & Heuer, S. 2012. Älä kerro kaikkea! Liettua. Talentum.

Tuominen, P. 2013. Virtuaalimaine. Liettua. Talentum.

Twitter. 2013. Support. Saatavilla: https://support.twitter.com/articles/20174631.

Valtonen, R. 2016. Facebookissa leviää jälleen ärhäkkä haittaohjelma – näin tunnistat ja poistat sen. Yleisradio. Viitattu 3.1.2017. Saatavilla: http://yle.fi/uutiset/3-9306159.

Vatanen P. 2016. Keikoilla kuvaaminen on "räjähtänyt käsiin" – tekijänoikeusasioissa vielä avoimia kysymyksiä. Yleisradio. Viitattu 9.1.2017. Saatavissa: http://yle.fi/uutiset/3-8720774.

Vehkoo, J. 2015. Valheenpaljastaja: Näin tunnistat feikkiprofiilin. Yleisradio. Viitattu 18.10.2016. Saatavissa: http://yle.fi/aihe/artikkeli/2015/11/09/valheenpaljastaja-nain-tunnistat-feikkiprofiilin.

Viestintävirasto. 2014. Heartbleed-haavoittuvuus koskee useita suomalaisten käyttämiä palveluita. Viitattu 16.3.2016. Saatavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2014/04/ttn20140411500.html.

Viestintävirasto. 2015. Yrityksiin kohdistuu entistä uskottavampia huijauksia. Viitattu 10.3.2016. Saatavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/09/ttn20150909144 1.html.

Vilkka, H. & Airaksinen T. 2003. Toiminnallinen opinnäytetyö. Helsinki: Tammi.

Whittaker, Z. 2012. 6.46 million LinkedIn passwords leaked online. ZDNet. Viitattu 15.10.2016. Saatavissa: http://www.zdnet.com/article/6-46-million-linkedin-passwords-leaked-online/.

Zaikin, R & Barda, D. 2016. ImageGate: Check Point uncovers a new method for distributing malware through images. Viitattu 15.12.2016. Saatavissa: http://blog.checkpoint.com/2016/11/24/imagegate-check-point-uncovers-new-method-distributing-malware-images/.