Haaga-Helia
ammattikorkeakoulu Oy

Työntekijät – uhka yrityksen tietoturvalle

Nina Viskari

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
Kevät 2017

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Nina Viskari

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Raportin/Opinnäytetyön nimi
Työntekijät – uhka yrityksen tietoturvalle

Sivu- ja liitesivumäärä
24

Tämän tutkimuksen tarkoituksena oli selvittää työntekijöistä johtuvia tietoturvauhkia ja luoda maailmanlaajuinen katsaus nykytilasta. Lisäksi pohdittiin, onko uhka mahdollisesti nousussa vai laskussa sekä otettiin esille niitä seikkoja joihin yritysten kannattaisi kiinnittää enemmän huomiota. Lopuksi käytiin läpi niitä toimenpiteitä, joilla uhkaa voisi vähentää.

Tutkimus tehtiin systemaattisena kirjallisuuskatsauksena. Lähdeaineistona käytettiin mahdollisimman tuoreita, viime vuosina tehtyjä tutkimuksia ja kyselyitä. Lisäksi pyrittiin saamaan mukaan niin monta maata kuin mahdollista.

Tutkimus osoitti, että työntekijöistä johtuvia tietoturvauhkia tapahtuu edelleen kohtalaisessa määrin ja ne ovat myös hyvin monen tyyppisiä. Suurin osa uhista on edelleen niitä, joissa työntekijä joutuu tahtomattaan tai tietämättään hyökkäyksen kohteeksi ja näin edesauttaa yritykseen kohdistuvan tietomurron toteutumista. Varsinaisia työntekijän tekemiä tahallisia hyökkäyksiä tapahtuu myös, mutta ei hälyttävässä määrin.

Tutkimuksessa todetaan, että vaikka tietoturva-asioihin on alettu perehtyä enemmän, on niissä silti selkeitä puutteita tietyillä osa-alueilla. Yksi pahimmista ongelmista näyttää olevan työntekijöiden tietoturvakoulutuksen puute tai sen heikko taso. Myös johtotasolla on edelleen parantamisen varaa tietoturvan merkityksen ymmärtämisessä.

Asiasanat
Tietoturva, työntekijät, tietovuoto, tietotekniikkarikokset

Sisällys

1 Johdanto

Tietoturva ja sen tila puhuttaa meitä jatkuvasti. Tietomurrot, tietovuodot ja verkkohuijaukset ovat lisääntyneet viime vuosina eikä loppua valitettavasti ole näköpiirissä.

Työntekijöistä tietoturvauhkana on kirjoitettu lukuisia artikkeleita ja tehty useita tutkimuksia ja kyselyitä yrityksille. Tämä kaikki materiaali löytyy internetistä ja asiasta puhutaan jatkuvasti paljon. Kuitenkin konkreettista, koko maailmaa käsittävää yhteenvetoa ei ole saatavilla. Ei ole myöskään tietoa siitä, kuinka monia varsinaisia työntekijöiden tekemiä tietoturvarikoksia on tehty ja kuinka moni niistä on johtanut tuomioon asti. Paljon puhutaan, että yritykset eivät halua haastaa työntekijöitään oikeuteen kasvojen menetyksen vuoksi, joten on ollut mielenkiintoista selvittää, onko näitä tapauksia todella olemassa, millaisia ne ovat ja millaisia tuomioita niistä on langetettu.

Työ on toteutettu kirjallisuustutkimuksena ja sen tarkoituksena on ollut saada vastauksia seuraaviin kysymyksiin:

- Millaisilla eri tavoilla työntekijät voivat olla uhkana yrityksen tietoturvalle
- Millaisia tietoturvauhkia työntekijöiden taholta on erilaisten tutkimusten ja kyselyiden kautta raportoitu meillä ja muualla
- Onko uhka tulosten ja raporttien perusteella suurentunut vai pienentynyt viime vuosien aikana
- Millä tavalla yritykset voivat minimoida työntekijöiden taholta tulevat uhat

Opinnäytetyön tavoitteena on ollut luoda maailmanlaajuinen, kattava katsaus työntekijöiden taholta tulevaan tietoturvauhkaan ja koostaa tämä tieto yhdeksi kokonaisuudeksi. Työssä on käytetty hyväksi julkaistuja tutkimuksia ja kyselyitä, jotka on suunnattu pääosin yritysten it-asiantuntijoille tai tietoturvasta vastaaville henkilöille. Niiden pohjalta on voitu tehdä suhteellisen kattava yhteenveto siitä, kuinka suureksi uhaksi työntekijät ovat osoittautuneet yrityksille tietoturvallisuuden kannalta ja millä eri tavoilla nämä uhat ilmenevät. Lisäksi mukaan on poimittu sellaisia artikkeleita, jotka avaavat aihe-aluetta lukijalle tai tuovat uutta näkökulmaa tietoturvan nykytilanteeseen. Työn lopussa on käyty läpi tutkimustulosten perusteella niitä toimenpiteitä, joita yritykset voivat tehdä minimoidakseen uhkaa.

Olen pyrkinyt käsittelemään aihetta mahdollisimman kansantajuisesti ja välttämään turhan teknistä kirjoitustyyliä. Tämä siksi, että se olisi helppolukuisempi myös niille ihmisille, jotka eivät työskentele it-alalla.

Tietoturva on aihe-alueena todella laaja, joten työ on rajattu käsittelemään ainoastaan työntekijöistä johtuvia uhkia. Tilannetta käsitellessä on pyritty saamaan mukaan niin monta maata, kuin mahdollista. Hyväksi käytettävissä tutkimuksissa ja raporteissa on otettu huomioon mahdollisimman tuoreet eli viimeisimmät raportit.

1.1 Raportin rakenne

Raportin toisessa kappaleessa käsitellään valittua tutkimusmenetelmää sekä esitellään lähdemateriaalin hakuprosessi ja tutkimuksessa käytetyt, tärkeimmät lähteet.

Kolmannessa luvussa paneudutaan syvemmin itse aiheeseen eli esitellään lukijalle tyypillisimmät, työntekijöistä johtuvat tietoturvauhat ja käydään läpi viimeaikaisimpia ja suurimpia tutkimuksia, joista tähän raporttiin on poimittu lähinnä aihe-alueeseen liittyvä materiaali. Lisäksi käydään läpi tietoturvan nykytilaa yrityksissä sekä hallinnollisesta näkökulmasta että koulutuksen suhteen. Kappaleen lopussa luodaan yhteenveto kyseisten tutkimusten pohjalta.

Neljännessä luvussa käydään läpi niitä toimenpiteitä, joita yritykset voivat tehdä työntekijöistä johtuvan uhan minimoimiseksi.

Viides luku on kooste koko aihe-alueen pääkohdista sekä tuo esille myös omia pohdintoja aiheesta.

2 Tutkimusmenetelmä, lähteiden hakuprosessi ja tärkeimmät lähteet

Tässä luvussa on käyty ensin läpi tutkimuksessa käytetty menetelmä. Sen jälkeen on käyty läpi lähteiden hakuprosessi eli mistä tietoa on haettu ja mitä hakusanoja on käytetty. Lopuksi on esitelty työssä käytetyt, tärkeimmät lähteet.

2.1 Tutkimusmenetelmä

Tämä työ on tehty kirjallisuuskatsauksena ja menetelmäksi on valittu systemaattinen kirjallisuuskatsaus.

> Yleisen luonnehdinnan mukaan kirjallisuuskatsaus on metodi ja tutkimustekniikka, jossa tutkitaan tehtyä tutkimusta. Sen avulla tehdään ’tutkimusta tutkimuksesta’, eli kootaan tutkimuksien tuloksia, jotka ovat perustana uusille tutkimustuloksille. (Salminen 2011, 1.)

> Systemaattinen kirjallisuuskatsaus on tiivistelmä tietyn aihepiirin aiempien tutkimusten olennaisesta sisällöstä. Systemaattisella kirjallisuuskatsauksella kartoitetaan keskustelua ja seulotaan esiin tieteellisten tulosten kannalta mielenkiintoisia ja tärkeitä tutkimuksia. (Salminen 2011, 9.)

Työssä on käytetty Finkin mallia (Salminen 2011, 11.) eli ensin on asetettu tutkimuskysymykset, kartoitettu ja valittu lähteet ja valittu hakutermit. Sen jälkeen on asetettu aikaraja tutkimukseen otettaville lähteille. Lähteistä on tämän jälkeen poimittu aihealueeseen kuuluvat osuudet työhön. Lopuksi on tehty yhteenveto tämän hetkisestä tilanteesta ja analysoitu sitä.

2.2 Lähteiden hakuprosessi

Lähteitä on haettu käyttämällä Googlea ja Google scholaria. Hakusanoina on käytetty seuraavia:
insider threat survey, insider threat report, social engineering, access rights, priviledged users, cyber crimes, tietoturvaraportti ja käyttäjän manipulointi.

2.3 Tärkeimmät lähteet

Tässä osiossa esitellään ne tärkeimmät tutkimukset ja kyselyt, jotka on otettu mukaan tähän opinnäytetyöhön ja joiden pohjalta yhteenveto on tehty:

Verizon tietomurtojen tutkimusraportti vuodelta 2016. Verizon on yhdysvaltalainen tietotekniikkayhtiö, joka julkaisee vuosittain raporttinsa edellisen vuoden aikana tapahtuneista tietomurroista. Vuoden 2016 raporttiin on koottu yli 100 000 tapausta. (Verizon 2016.)

IBM:n vuonna 2016 teettämä maailmanlaajuinen tietoturvatutkimus. IBM:n tietoturvapalveluiden monitorointitulosten perusteella tehty yhteenveto kyberhyökkäyksistä ja erilaisista tietoturvaloukkauksista ajalta 1.1.2015 – 31.12.2015. (IBM 2016.)

CGI:n tukema, oppilasyhteistyönä toteutettu tutkimus, jossa selvitettiin kyberturvallisuuden tilaa suomalaisissa yrityksissä ja julkisen sektorin organisaatioissa. Aiheina olivat mm. kyberturvallisuuden johtaminen, varautuminen, riskienhallinta sekä organisaatioille tapahtuneet tietomurrot ja -vuodot. Vastaajia olivat liiketoiminta-, IT- ja tietoturvajohto sekä -asiantuntijat. Tutkimus suoritettiin sähköisenä kvantitatiivisena kyselynä ajalla 11/2015 – 3/2016. Vastaajia oli yhteensä 200. (CGI 2016.)

F-Securen kyberturvallisuuden tila 2017-raportti, johon on koottu yrityksen tutkijoiden kokemukset vuonna 2016 tapahtuneista haavoittuvuuksista, hyökkäyksistä sekä haittaohjelmista. Raportin tarkoituksena on auttaa yrityksiä selviämään asiantuntijoiden avustuksella alati kasvavista ja kehittyvistä tietoturvauhista. (F-Secure 2017.)

Viestintäviraston vuonna 2017 tammikuussa julkaisema raportti Tietoturvan vuosi 2016, johon on kerätty viime vuoden tärkeimpiä suomalaisia tietoturvailmiöitä. (Viestintävirasto 2017.)

ISACA & RSA Conference Survey 2014. State of Cybersecurity : Implications for 2015. RSA Konferenssin pitäjien ja ISACAN vuonna 2014 tekemän yhteistyön tuloksena syntynyt raportti, johon on kerätty tammikuussa ja helmikuussa 2015 lähetetyn kyselyn tulokset. Vastaajina ovat olleet ISACAN CISM-sertifioinnin omaavat tietoturva-ammattilaiset, RSA Conference Loyalty Plus-asiakkaat ja henkilöt, jotka ovat rekisteröityneet vuoden 2015 RSA konferenssin osallistujiksi. Vastaajia oli maailmanlaajuisesti 1500, joista 649 vastasivat kaikkiin kyselyssä esitettyihin kohtiin. (ISACA & RSA 2014.)

PWC 2015 Information Security Breaches Survey. Iso-Britanniaa käsittelevä, kansalliseen kyberturvallisuusohjelmaan pohjautuva ja PWC:n toteuttama tietoturvakysely maassa toimiville IT-ammattilaisille, liiketoimintajohtajille ja muissa päättävissä asemissa oleville henkilöille. Vastaajia oli 664 kappaletta. (PWC 2015.)

Alcosecin USA:ssa San Franciscossa helmikuussa 2014 järjestämän RSA-konferenssin yhteydessä tekemä kysely tietoverkkojen turvallisuudesta. Kyselyyn osallistui 142 tietoturva-, verkko- ja sovellusasiantuntijaa. (Alcosec 2014.)

Bluecoatin vuonna 2015 tekemä globaali tutkimus työntekijöiden osallisuudesta tietoturvauhkiin. Tiedot on poimittu Symantecin lehdistötiedotteesta, joka on ostanut Bluecoatin. Alkuperäistä tutkimusta ei ollut saatavilla. (Bluecoat 2015.)

CyberEdgeGroupin julkaisema Cyberthreat Defense-raportti koskien Pohjois-Amerikkaa ja Eurooppaa. Kyselyyn osallistui 814 tietoturvallisuudesta vastaavaa henkilöä ja ammattilaista, joista kaikki yli 500 henkilömäärän yrityksistä. He edustivat 7:ä eri maata Pohjois-Amerikassa ja Euroopassa. (CyberEdgeGroup 2015.)

Ryan Francisin artikkeli, johon on kerätty yhdeksän eri työntekijän tapaukset eli miten he ovat toteuttaneet tietoturvarikoksen työnantajaansa kohtaan. (Francis, 6.10.2014.)

Osterman Research-yhtiön julkaisu ” Best Practices for Protecting Your Data When Employees Leave Your Company” joulukuulta 2016, jossa käsitellään yleisesti työntekijöiden toimia suhteessa yrityksen tietoihin silloin kun hänen työsuhteensa päättyy. (Osterman Research 2016.)

Biscom on johtava turvattujen kommunikaatio-ohjelmien valmistaja, jonka tutkimuksessa Employee Departure Creates Gaping Security Hole on käsitelty työntekijöiden käyttäytymistä yrityksen tieto-omaisuuden suhteen työsuhteen päättyessä. (Biscom 23.12.2015.)

Eric Colen SANS-instituutin sivustolla julkaisema artikkeli Taking action against the insider threat tarkastellaan erilaisia sisäisen uhkan tyyppejä ja kerrotaan millaisella prosessilla uhka voidaan huomata ja poistaa. (Cole 2016.)

Angus McIllwraithin kirjassa Information security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness käsitellään miten työntekijöitä voidaan koulutuksen ja tiedottamisen avulla valistaa tietoturva-asioissa ja siten minimoida riskejä. (McIllwraith 2006.)

"Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin" on Ari Salmisen kirjoittama Vaasan yliopiston julkaisu vuodelta 2011. Teoksessa käydään läpi mistä kirjallisuuskatsauksissa on kysymys ja esitellään kirjallisuuskatsauksen eri tyypit. (Salminen 2011.)

3 Työntekijöistä johtuvat tietoturvauhat

> ”Seuraava hyökkääjä on todennäköisesti joku, johon uskoit luottavasi. Työntekijästä johtuvat tietoturvauhat ovat edelleen merkityksellisin uhka yrityksille kaikkialla maailmassa” (IBM 2016, 2).

Vaikea uskoa, että työntekijät muodostavat yhden suurimmista ja vaarallisimmista uhista yritykselle. Suurimman siksi, että hyvin monet yritykset eivät pidä asiaa tärkeänä ja sivuuttavat sen. Vaarallisimman taas sen vuoksi, että ulkopuoliseen hyökkääjään verrattuna he ovat jo sisällä yrityksessä ja heillä on myös jo pääsy sen resursseihin tavalla tai toisella.

Työntekijöistä johtuvia sisäisiä uhkatyyppejä ovat:

- Hyökkääjä, joka haluaa tahallisesti vahingoittaa yritystä
- Hyökkääjä, joka huijataan tai manipuloidaan tekemään jotain joka vahingoittaa yritystä (Cole 2016.)

> Suurin osa tietomurroista, vahingoista ja muista tapahtumista, jotka johtavat ongelmiin, on ollut käyttäjien avustamia. Lähes jokainen nykypäivän rikkomus on tapahtunut käyttäjän hyväksymänä, esimerkiksi avaamalla sähköpostin liitetiedoston, joka on sisältänyt saastuneita tiedostoja taikka käyttäjä asentanut koneelle epäilyttäviä haittaohjelmia. (Ikonen 2015.)

Suurin osa näistä edellä mainituista tapahtumista on täysin tahattomia eli työntekijät eivät yksinkertaisesti tajua tekevänsä mitään väärin. Tämä voi johtua kunnollisen ohjeistuksen puutteesta tai sen unohtamisesta. Lisäksi kaikki työntekijät eivät pidä tietoturvaa niin tärkeänä asiana tai tajua sen merkitystä yrityksen toiminnan turvaamiselle. On toki yrityksiä joissa tietojen turvaamiselle ei ole tarvetta tai joissa katsotaan, ettei heillä ole sellaista tietoa, jonka vuodosta aiheutuisi mittavia kustannuksia tai haittoja heidän toiminnalleen. Vain harvoissa tapauksissa on selkeästi kyse työntekijästä, joka haluaa tahallisesti vahingoittaa työnantajaansa. Oli niin tai näin, jokaisen yrityksen olisi syytä varautua näihin potentiaalisiin uhkatekijöihin ja ottaa tietoturva-asioita suunnitellessa ja toteuttaessa huomioon myös omat työntekijänsä.

Verizonin tutkimuksen mukaan tapauksia, joissa työntekijän tahaton toiminta on suoraan vaarantanut jonkun tieto-omaisuuden tietoturvan, on todettu 11347 tapausta, joista 197:ssä tapauksessa on vahvistettu tietovuoto. Näistä suurimmassa osassa (61 kpl) on ollut kyse työntekijän aiheuttamasta järjestelmän kuormittamisesta. Muita huomattavia virheitä ovat mm. dokumenttien ja sähköpostien lähettäminen vääriin osoitteisiin, tiedon julkaiseminen väärien ihmisten nähtäväksi, väärin konfiguroidut laitteet sekä tietojen vääränlainen hävittäminen. Suurin osa näistä tietovuodoista tulee ilmi ulkoisilta asiakkailta, joiden tietoja asia koskee. (Verizon 2016,40-41.)

ISACA:n ja RSA:n konferenssissa vuonna 2014 ilmoitettiin 636 vastauksen pohjalta sisäisiä tahallisia hyökkääjiä 182 kappaletta (28,62%) ja tahattomia 259 (40,72%). (ISACA & RSA Conference Survey 2014, 5.)

Isossa-Britanniassa 81% isoista yrityksistä mainitsi, että työntekijät olivat jollakin tasolla mukana niissä hyökkäyksissä, joita heillä on ollut. Tutkimuksessa mainitaan, että suurin osa näistä tapauksista käsittelee joko hyökkäystä järjestelmiin ja tietoihin ilman oikeuksia, hyökkäystä tietosuojalakeja ja säännöksiä vastaan tai luottamuksellisten tietojen vuotamista tai menetystä. Pienistä yrityksistä 27% kertoi kohdanneensa hyökkäyksen työntekijän taholta. (PWC 2015,13.)

Vuonna 2013 Alcosecin tutkimukseen osallistuneista yrityksistä 62% katsoi, että työntekijöiden kautta tulevat sisäiset uhat ja vahingolliset hyökkäykset olivat heidän suurin tietoturvariski. Vuonna 2014 luku oli jo 73%, tosin tähän saattoi vaikuttaa samana vuonna paljon julkisuutta saanut Edward Snowdenin tapaus. (Alcosec 2014, 6.)

IBM:n tutkimuksen mukaan työntekijät olivat vastuussa 60%:sta kaikista hyökkäyksistä. Näistä kuitenkin 1/3-osa oli sellaisia, joissa työntekijä on vahingossa ja hyvässä uskossa päästänyt ulkoisen hyökkääjän käsiksi yrityksen tietoihin tai ei ole kiinnittänyt huomiota yrityksen tietoturvaohjeistukseen. Tietojenkalastelu on yksi tällainen tyypillinen tilanne. Toisin sanoen, he eivät ole tahallaan toimineet väärin. (IBM 2016, 11.)

CGI:n tutkimuksen mukaan liiketoimintajohto ajattelee, että tietomurto johtui yhtä usein inhimillisestä virheestä (40%) kuin ulkoisesta kyberhyökkäyksestä (40%). Asiantuntijoiden mielestä syy on kuitenkin selkeästi enemmän (67%) ulkoisessa kyberhyökkäyksessä, eikä niinkään inhimillisessä virheessä (22%). (CGI 2016,12.)

PWC:n tutkimuksessa taas todetaan, että työntekijän inhimillinen virhe oli syynä puoleen kaikista hyökkäyksistä. Kaiken kaikkiaan työntekijöiden joko tahattomasti tai tahallisesti aiheuttamia hyökkäyksiä oli 21 tapausta 39:stä. (PWC 2015, 14.)

Työntekijän päivittäisen työpäivän aikana tapahtuu lukuisia tilanteita, joissa yrityksen tietoturva voi olla vaarassa, ainakin potentiaalisesti. Käyttäjän fyysinen toiminta jo itsessään voi olla haitallista. Yritykseen saatetaan samalla oven avauksella päästää sisään vakoilija, salasanoja jätetään esille ja siten väärien käsien saataville, puhelimessa saatetaan antaa huijauksen avulla arkaluontoista tietoa. Puhumattakaan sitten itse työhön liittyvistä uhista kuten esimerkiksi internet-käytön tai sähköpostin kautta tulevat hyökkäysmahdollisuudet. Nykyisessä mobiilimaailmassa oma lukunsa ovat myös työn liikkuvuudesta ja mobiilikeskeisestä toiminnasta johtuvat uhat eli lähinnä kannettavat ja kännykät. Nämä laitteet ovat usein täynnä työhön liittyvää materiaalia ja varkauden tai katoamisen sattuessa suuressa vaarassa joutua vääriin käsiin. Luonnollisesti tällöin myös yrityksen tietoturva on uhattuna. Seuraavana on käyty läpi tässä työssä käytettyjen tutkimusten esille tuomia yleisimpiä uhkia ja tietoturvaan liittyviä muita asioita, joihin yrityksien kannattaisi kiinnittää huomiota.

3.1 Käyttäjän manipulointi

Käyttäjän manipuloinnilla (eng. social engineering) tarkoitetaan toimintaa, jossa hyökkääjä käyttää hyväksi ihmisluonnetta manipuloimalla työntekijää luovuttamaan sellaista

tietoa, joka mahdollistaa hyökkääjän pääsyn käsiksi yrityksen tietojärjestelmään tai saada hänet toimimaan hyökkääjän toivomalla tavalla. Manipulointi voidaan jakaa joko passiiviseen tai aktiiviseen toimintaan.

Passiivisessa manipuloinnissa hyökkääjä tunkeutuu tavalla tai toisella fyysisesti suoraan yritykseen sisään ja kerää tietoa varastamalla esimerkiksi salasanoja tai mobiililaitteita, tonkimalla roskakoreja tai salakuuntelemalla työntekijöitä. Harva työntekijä tulee ajatelleeksi, että saapuessaan töihin, hän saattaa epähuomiossa päästää yrityksen tiloihin myös sinne kuulumattoman ja tietojen kalastelumielessä saapuvan vakoilijan. Valitettavasti tämä tilanne on kuitenkin tätä päivää. Mikäli yrityksellä on tarpeeksi kallisarvoista ja rikollista toimintaa hyödyttävää tietoa, käyttävät sitä havittelevat tahot kaikkia mahdollisia keinoja hyväkseen.

> Vuonna 2016 eräissä taidokkaimmissa kyberhyökkäyksissä käytettiin fyysistä tunkeutumista osana toimintaa. Se on erittäin tehokas tapa toteuttaa hyökkäys ja kohdentaa se johonkin tiettyyn yritykseen tai henkilöön. Koska ihmiset eivät tavallisesti kiinnitä huomiota mahdollisiin fyysisiin vakoiluyrityksiin, ne ovat vaarallisen helppoja toteuttaa ja jäävät usein paljastumatta pitkäksi aikaa. (F-Secure 2017, 12.)

Joidenkin yritysten toimitilojen valvonnassa on tänä päivänä edelleen huomattavia puutteita eikä kulunvalvontaan ole panostettu tarpeeksi. Henkilökortteja ei ole, ovikoodeja ei käytetä eikä kukaan ei ole valvomassa vieraiden tai yleensä sisään taloon tulevien henkilöiden identiteettiä ja tarkoitusperiä. Suurimmissa ja hyökkääjän kannalta usein myös tärkeimmissä kohteissa saattaa valvontaan olla satsattu huolella, mutta se ei kuitenkaan välttämättä estä luvatonta sisäänpääsyä. Taktiikkoina tällaisiin kohteisiin pääsyssä käytetään työntekijöiden huijausta ja hyväuskoisuutta esimerkiksi samalla oven avauksella sisäänpääsyä tai valehtelemalla, että oma kulkukortti on jäänyt kotiin.

> Hyökkäystä suunnitteleva saattaa myös hyödyntää erilaisia toimitilojen huolto- ja ylläpitotehtäviä tarjoavia yrityksiä, joiden työntekijöillä on sisäänpääsy johonkin tiettyyn yritykseen ja myös todennäköisesti tarvittavia kulkukortteja, ovikoodeja ja yrityksen karttoja. Hyökkääjä murtautuu ensin tällaisen yrityksen järjestelmiin ja kerää sieltä tarvittavaa materiaalia ennen varsinaista hyökkäystä itse kohteeseen. (F-secure 2017, 20.)

Aktiivinen manipulointi on toimintaa, jossa hyökkääjä on suoraan kontaktissa työntekijään ja manipuloi häntä paljastamaan haluamiaan tietoja tai toimimalla hyökkääjän haluamalla tavalla. Metodeina tässä hyökkäystavassa käytetään muun muassa esiintymistä yrityksen pomona tai muuna korkeammassa asemassa olevana henkilönä.

> Usein käyttäjän manipuloinnista johtuvia hyökkäyksiä on vaikea huomata tai ehkäistä, koska ongelmat ovat psykologisia eikä teknologisia. Näin ollen käyttäjän manipulointi on helppo tapa löytää aukkoja yrityksen tietoturvasta, kun taas yrityksen on erittäin vaikea löytää ja tukkia näitä aukkoja. (Ikonen I. 2015.)

> Vuoden 2016 aikana, ennen lähinnä satunnaiset ja loma-aikoihin keskittyvät, yritykset lypsää rahaa valelaskuilla ja toimitusjohtajahuijauksilla arkipäiväistyivät. Toimitusjohtajahuijauksessa rikollinen lähestyy uhriaan sähköpostitse tai puhelimitse, tekeytyy yrityksen johtajaksi ja koettaa saada talousosaston siirtämään rahaa tililleen. Apuna käytetään väärennettyjä sähköpostiosoitteita tai aidon näköisiä verkkotunnuksia. Uskottavalla huijauskampanjalla rikollisten saama hyöty voi nousta kymmeniin tuhansiin euroihin kerralla. Valelasku muistuttaa toimitusjohtajahuijausta, mutta on usein vain pelkkä lasku, joka koetetaan saada maksuprosesseista läpi vauhdikkaasti. Kertasummat ovat pienempiä kuin toimitusjohtajahuijauksissa. (Viestintävirasto 2017, 4.)

Verkkohuijauksista on lukuisia eri variaatioita. Seuraavassa on lueteltu muutamia:

Kaikki eivät hoksaa tarkistaa lähettäjän tietoja ja haksahtavat lähettämään sähköpostinsa kirjautumistunnukset rikollisille. Sen jälkeen huijari voi lähettää sähköpostitilin omistajan nimissä viestejä, joissa pyydetään esimerkiksi lomamatkalla sattuneen onnettomuuden verukkeella siirtämään rahaa ulkomaille.

Huijausmuodosta riippumatta rikolliset pyytävät usein siirtämään rahaa rahanvälityspalvelu Western Unionin kautta. Sen avulla raha siirtyy osapuolelta toiselle kansainvälisen toimipisteverkoston välityksellä.

Vuoden aikana ovat yleistyneet erilaiset kiristystroijalaiset. Ne lukitsevat käyttäjän tietokoneen tai tiedostot. Lukitsemisen jälkeen kiristäjät lähettävät koneen omistajalle viestin, jossa he maksua vastaan lupaavat avata koneen tai sen sisältämät tiedostot.

Facebook-mainoksessa tarjotaan merkkituotetta ilmaiseksi toimituskulujen hinnalla, kunhan vastaa nettikyselyyn. Kyselyyn päästäkseen joutuu hyväksymään sopimusehdot. Ehdoissa lukee pienellä, että lahjan tilaamalla sitoutuu maksulliseen jäsenyyteen. Huijarit luottavat siihen, että kaikki eivät lue sopimusehtoja riittävän tarkasti tai ollenkaan. Jäsenyys saattaa maksaa joitain kymmeniä euroja kuukaudessa.

Lomamatkalla vaikeuksiin joutunut ystävä lähettää sähköpostilla avunpyynnön. Selvitäkseen pulasta hän tarvitsee rahaa äkkiä.

Sähköpostiviestissä kerrotaan sinua kohdanneesta onnenpotkusta. Olet voittanut ulkomaisessa lotossa miljoonia euroja. Voittaja on seulottu arvonnassa, johon osallistujat on valittu sähköpostien perusteella. Kuulostaa liian hyvältä ollakseen totta – ja niin se onkin. Voittosumman saamiseksi sinun pitäisi nimittäin pulittaa pieni summa rahaa lottoarvonnan järjestäjille.

Jos tuntematon nettikauppa myy merkkiaurinkolaseja, -käsilaukkuja tai -untuvatakkeja pilkkahintaan, tuotteet voivat olla väärennettyjä. Epäuskottavan verkkokaupan tuotteet kannattaakin jättää tilaamatta. Kalliita luksustuotteita tuskin myydään sivustoilla, jotka näyttävät halvoilta. (Miettinen 2015.)

Aktiivisen manipuloinnin yleisin ilmentymä on tietojenkalastelu sähköpostin kautta. Tavallisessa tietojenkalastelussa ei ole ennalta määrättyä kohderyhmää vaan se suunnataan satunnaisille henkilöille. Tämän lisäksi on olemassa myös kaksi lähinnä kohdennettuihin hyökkäyksiin suuntautuvaa kalastelumuotoa. Toisessa uhrina on tarkkaan ennalta määrätty yritys tai joku tietty työntekijä, jonka kautta hyökkääjä olettaa pääsevänsä parhaiten käsiksi haluamiinsa tietoihin. Toisessa taas hyökkäys kohdistetaan yrityksen ylempiin toimihenkilöihin. Suurimmalla osalla yrityksistä on verkkosivuillaan lista, jossa on yhteystietoineen mainittu yrityksen tärkeimmät päättävät henkilöt. Mukana saattaa olla jopa kyseisen henkilön ammatillista tai muuta taustatietoa, jota hyökkääjä voi helposti käyttää hyväkseen hyökkäystä suunnitellessa.

> Hyökkääjät käyttävät paljon aikaa kerätäkseen tietoa yrityksistä ja heidän työntekijöistään. Tekniikoiden kuten phisingin, vishingin ja imitoinnin avulla kerätään henkilötietoja, valtakirjoja, käyttäjätunnuksia, pankkitietoja ja arkaluontoisia potilastietoja, kaiken muun mainitsemattoman tiedon lisäksi. (Ikonen 2015.)

Verizonin 2016 tutkimuksen mukaan jopa 30 % työntekijöistä avasi tietojenkalasteluviestin ja 12 % heistä klikkasi myös saastunutta liitetiedostoa tai linkkiä. Kuitenkin vain 3% heistä ilmoitti tietoturvahenkilöstölle mahdollisesta uhasta. (Verizon 2016, 18.)

Yleisen tietojenkalastelun ilmentymiä ja muotoja on lukuisia erilaisia, mutta päämäärä on aina sama. Nykypäivänä nämä viestit on tehty melko taidokkaasti ja valitettavasti hyvin moni niihin myös lankeaa. Ainoa asia, joka erottaa kalasteluviestin oikeasta, on osoiterivillä näkyvä, yleensä hyvin sekava sähköpostiosoite. Sitä ei välttämättä kuitenkaan tule tarkistettua. Esimerkiksi pankit joutuvat tänä päivänä käsittelemään paljon huijausviestejä koskevia yhteydenottoja, koska niiden nimissä lähetetään lukuisia erilaisia kalasteluviestejä. Niissä pyydetään käyttäjää klikkaamaan linkkiä ja antamaan omat verkkopankkitunnuksensa avautuvaan sisäänkirjautumisikkunaan. Kun kirjautuminen on tehty, sivusto ohjautuukin hyökkääjän tekemälle valesivustolle tai hänen jo murtamalle sivulle, josta on helppo poimia tiedot talteen varsinaista murtautumista varten.

Aktiivista manipulointia on myös sähköpostin välityksellä lähetettävät vakoiluohjelmat, joiden päämäärä on saada käyttäjä klikkaamaan linkkiä, josta ohjelma aktivoituu ja tätä kautta hyökkääjä pääsee sisään järjestelmään.

> Vuoden 2016 havaintojen perusteella vakoiluun räätälöidyn haittaohjelman saamiseksi kohdeverkkoon käytettiin kahta tyypillistä keinoa: joillekin verkon käyttäjille lähetetään sähköpostiviesti, joka sisältää joko haitallisen liitetiedoston tai linkin, joka johtaa haitalliselle verkkosivustolle. Itse sähköpostiviestit sisälsivät vastaanottajan työtehtävien kannalta mielenkiintoisia teemoja ja ne lähetettiin selkeästi ennalta huolellisesti valituille henkilöille. Verkkosivut, joihin linkit osoittivat, saattoivat olla tuttuja ja luotettuja työtehtävien tai arkisten asioiden hoitamisessa. Nämä sivustot kuitenkin

> oli murrettu ja valjastettu haitalliseen käyttöön. (Viestintävirasto 2017, 12.)

> Uutena ilmiönä havaittiin, että työsähköpostien lisäksi, haittaohjelmaa yritettiin levittää kohdehenkilöiden yksityissähköpostien ja esimerkiksi heidän perheenjäsentensä sähköpostiosoitteiden kautta. Yksityissähköpostin käytön havainnointimekanismit ja postin käyttötavat ovat löyhempiä työsähköpostiin verrattuna. Hyökkääjät pyrkivät jatkuvasti kehittämään uusia menetelmiä löytääkseen heikoimmalla suojauksella varustetun reitin kohdehenkilön tietoihin. (Viestintävirasto 2017, 12.)

Bluecoatin kyselyssä yksi kolmesta (29%) kiinalaisesta työntekijästä avasi liitetiedoston tuntemattomalta taholta vaikkakin kolme neljästä (72%) tiedosti sen olevan riskialtista. Yhdysvaltalaiset yritykset sen sijaan ottavat riskin vakavammin. Siellä 80% on tietoisia riskistä ja vain 17% avaa liitetiedoston. (Bluecoat 2015.)

Kysyttäessä työntekijöiltä kuinka hyvin yritys on valistanut heitä kalasteluun liittyvistä hyökkäyksistä, yli neljä kymmenestä oli sitä mieltä, että ei ole, toinen neljä kymmenestä vastasi ” jokseenkin valistettu” ja loput 20 % oli sitä mieltä, että valistusta on annettu. (CyberEdgeGroup 2015, 28.)

Voimme näiden edellä olevien perusteella arvailla, kuinka hyvin erilaiset käyttäjien manipulointikeinot ovat työntekijöiden tiedossa ja onko heitä neuvottu, miten toimia tällaisessa tilanteessa.

3.2 Oikeuksien väärinkäyttö

Yksi yleisimpiä tietoturvauhkia on työntekijän pääsy verkkolevyille ja tiedostoihin, joihin hänen ei pitäisi päästä. Tämä tietomurtotapa on myös ehdottomasti vaikeimpia huomata ja yleensä ne saadaan selville vasta paljon myöhemmin.

Järjestelmäasiantuntijoiden tehtävä on työntekijöiden käyttäjätunnusten hallinnointi. Kun työntekijä aloittaa työssään, hänelle määritellään käyttäjätilin yhteyteen ne verkkolevyt, kansiot tai tiedostot, joille hänellä on pääsy. Yleensä ne on määritelty työtehtävien mukaan ja näin ollen riittävät. Mutta mitä tapahtuu näille oikeuksille, jos kyseinen käyttäjä vaihtaakin myöhemmin toisiin tehtäviin talon sisällä? Mitä jos hän onkin määräaikainen työntekijä, joka on yrityksessä töissä vain pari kuukautta? Pääsääntöisesti järjestelmävastaavat poistavat vanhat oikeudet ja lisäävät uudet uuden tehtävän mukaisiksi sekä poistavat tai jäädyttävät tilin, jota ei enää käytetä. He ovat kuitenkin vain ihmisiä ja erehdyksen tai unohduksen riski on olemassa. Isoissa yrityksissä tämä korostuu entisestään. On todella suuri työ pysyä kaikkien työntekijöiden käyttäjätunnusten tasalla ja näin ollen joillakin työntekijöillä voi olla enemmän oikeuksia, kun olisi edes tarpeen. Saattaa myös olla, että

on olemassa tilejä, joita ei enää edes käytä kukaan. Nämä kaksi tekijää muodostavat tietoturvan kannalta huomattavan riskin ja väylän tietomurtoa suunnittelevalle tai muuten yritystä sisältä päin uhkaavalle tekijälle. Erityistä valvontaa kaipaavat varsinkin laajemmilla oikeuksilla olevat käyttäjät, joilla siis on tavallista työntekijää isommat valtuudet. Harva työntekijä ilmoittaa järjestelmänvalvojille omaavansa oikeuksia, joita hänellä ei pitäisi olla, pikemminkin päinvastoin. Kun puhutaan työntekijästä, joka haluaa tahallisesti käyttää hyväkseen tai hyödyntää rikosmielessä saatuja oikeuksia, on uhka tietomurrolle ja tietovuodolle tällaisessa tilanteessa jo melkoinen.

Verizonin tutkimuksen mukaan vuonna 2016 työntekijöistä johtuvia oikeuksien väärinkäyttöä oli 10 489 tapausta yli 100 000:sta. Väärinkäytöllä tässä tapauksessa tarkoitetaan mitä tahansa hyväksymätöntä tai vahingollista yrityksen resurssien käyttöä. Näistä 172:ssa tapauksessa vahvistettiin tietovuoto. (Verizon 2016, 35.)

Työntekijälle voidaan antaa myös työnkuvaan sopivat oikeudet, mutta rajoittaa niiden käyttöä muulla tavoin. Esimerkkinä uutinen, jossa Supon määräaikaisen työntekijän epäillään tehneen luvattomia tietohakuja salaisista ja arkaluontoisista kohteista. KRP:n mukaan vääriin käsiin joutuessaan tiedot olisivat voineet olla vahingollisia tai haitallisia valtion tai kansallisen turvallisuuden kannalta. (Iltalehti 13.4.2017.)

Tässä tapauksessa siis työntekijä on saanut oikeudet, jotka ovat työn kuvan mukaisia mutta sisäisillä säädöksillä on määrätty erikseen mitä hän voi tehdä ja mitä ei. Tällainen käytäntö on yleistä valtion laitoksissa, terveydenhoitoalalla ja korkeammissa johtotehtävissä toimivien henkilöiden toimenkuvassa tai kun ollaan yleisesti tekemisissä arkaluontoisen, salaisen tai henkilötietojen kanssa.

Oikeuksien väärinkäyttö ei rajoitu pelkästään käyttäjätileihin ja niiden oikeuksiin vaan se ilmenee myös muilla tavoin. Esimerkiksi kaikenlainen työntekijän hallussa olevan tiedon, oman ammattitaidon, yrityksen omaisuuden sekä sähköpostin väärinkäytön lisäksi myös standardien vastaisten laitteiden tai ohjelmien tuominen verkkoympäristöön katsotaan kuuluvan samaan kategoriaan.

Jokaisessa yrityksessä käytetään paljon käyttäjätilejä, joilla on muita suuremmat tai jopa rajoittamattomat oikeudet minne tahansa verkkoympäristössä.

> Nämä ns. etuoikeutetut tilit tekevät ulkopuolisesta hyökkääjästä sisäisen, jolloin he voivat liikkua verkossa vapaasti ilman paljastumista. Ne ovat todellinen uhka, joka vaanii yrityksen sisällä. Jos niitä ei tarkkailla, vihamielinen työntekijä käyttää niitä va-

hingoittaakseen yritystä ja ulkopuolinen hyökkääjä käyttää niitä kuin olisi sisällä yrityksessä. (Worrall 2014.)

Tällaisia kaikilla oikeuksilla varustettuja tilejä löytyy pääasiassa IT-järjestelmistä vastaavilla työntekijöillä, mutta vastaavilla oikeuksilla varustettuja tilejä on myös paljon erilaisissa ohjelmissa tai laitteissa. Internetistä löytyy monia sivustoja, joihin on kerätty useiden eri laitteiden oletus käyttäjätunnukset ja salasanat. Koska valitettavan monissa laitteissa näitä ei ole muutettu käyttöönoton yhteydessä, on niihin sisäänpääsy suhteellisen vaivatonta.

CyberEdgeGroupin kyselyssä tiedusteltiin kuinka paljon yritykset valvovat näiden etuoikeutettujen käyttäjien toimia, yksi kolmasosa epäili, ettei sitä tehdä ja hitusen alle puolet-kin olivat sitä mieltä, että valvonta on heikkoa. Käyttäjätunnusten varastaminen ja uudelleen käyttäminen ovat edelleen yksi suurimpia uhkia tämän päivän yrityksille. (CyberEdgeGroup 2015, 15-16.)

3.3 Sosiaalinen media

Elämme nykyään sosiaalisen median kultakautta. Meillä on käytössä lukusia erilaisia sosiaalisia ohjelmia, ei pelkästään tietokoneissa vaan myös älypuhelimissa. Tämä on helpottanut suunnattomasti ihmisten kanssakäymistä ja esimerkiksi työasioiden hoitoa, mutta samalla tuonut monia tietoturvaan liittyviä huolenaiheita mukanaan.
Yritysten sisällä käytävien tietojenkalasteluyritysten tai vakoiluohjelmien viljelyn lisäksi hyökkääjät käyttävät tänä päivänä hyvin paljon hyväksi myös erilaisten sosiaalisten medioiden kuten Facebookin, Twitterin ja LinkedIn:in kautta saatavaa tietoa henkilöistä, kun he suunnittelevat toimintaansa. Ihmiset saattavat latailla kuvia tai kertoa muuten työpaikastaan eivätkä tajua, että nämä voivat olla hyökkääjän kannalta erittäin hyödyllistä informaatiota.

Bluecoatin tutkimuksessa 1580 vastaajaa 11 eri maasta ottivat esille maailmanlaajuisen trendin eli työntekijät eivät edelleenkään ota huomioon internetin käyttöön liittyviä tietoturvariskejä työpaikallaan. Tutkimuksen tulokset kertoivat, että he käyvät sopimattomilla sivustoilla vaikka tietävät varsin hyvin millainen riski se on yritykselle.

Akuisviihdesivustot ovat suosituimpia väyliä piilotettujen haittaohjelmien levittämiseen. Vaikka työntekijöillä on tiedossa näiden sivustojen tietoturvariskit, he silti käyvät niissä. Kiinassa 19% työntekijöistä käyttää työkonetta tällaisten sivujen katsomiseen, Meksikossa luku on 10 % ja Iso-Britanniassa 9%. Vähiten vastauksia tuli Australiasta ja Saksasta,

kummastakin vain 2%. Melkein kaksi viidestä työntekijästä (41%) käyttää sosiaalisia mediasivustoja henkilökohtaisiin tarkoituksiin työpaikalla. (Bluecoat 2015.)

> Työntekijöiden verkkoselailusta eli ns. verkkosurffailusta muodostuvia tunnistamistietoja ei saa käyttää työnantajan työn johto- ja valvontaoikeuden eli direktio-oikeuden nojalla siten, että työntekijöitä valvotaan, seurataan ja tarkkaillaan keräämällä ja/tai katsomalla näitä tunnistamistietoja. Tunnistamistiedoista muodostunee myös henkilörekisteri siltä osin kuin niistä tallentuu tunnistettavia luonnollisia henkilöitä koskevia henkilötietolain 3 § 1 kohdan tarkoittamia henkilötietoja.
> Työnantaja voi kuitenkin direktio-oikeuden nojalla päättää tietoverkkojen käyttösäännöistä ja päättää siitä, saako työpaikalla verkkosurffailla ylipäätään tai vain tietyillä sivuilla. Työnantaja voinee myös estää joillekin sivuille pääsyn koko organisaatiossa tai tietyille tahoille organisaatiossa. Tältä osin työnantajan on kuitenkin huomioitava tasapuolinen kohtelu työpaikalla ja työsopimuslain (55/2001) 2 luvun 2 §:n tarkoittama syrjimättömyyden toteutuminen. Sääntöjen noudattamista voidaan valvoa myös perinteisin työnjohto-oikeudellisin keinoin siten, että työnantaja tai tätä edustava esimies huomatessaan työntekijän surffailevan kielletyillä sivuilla kieltää häntä näin tekemästä. (Tietosuojavaltuutetun toimisto 2014.)

Käyttäjien internetsivustojen käyttöä voidaan teknisesti rajoittaa, mutta harva yritys näin tekee ainakaan meillä Suomessa. Käytön valvomisessa sen sijaan on otettava huomioon lakiin perustuvat vaatimukset.

ISACAN & RSA:n tutkimuksen mukaan 57,66 % yrityksistä rajoittaa käyttäjien pääsyä sosiaalisiin medioihin ja 42,34% ei. (ISACA & RSA 2014, 14.)

CyberEdgeGroupin tutkimuksessa taas todetaan, että yritysten suojaustoimenpiteet koskien Facebookia ja Twitteriä ovat edelleen heikoin lenkki yritysten tietoturvatoimenpiteissä. (CyberEdgeGroup 2015, 10.)

3.4 Mobiililaitteet

Mobiililaitteet eli kannettavat, kännykät ja tabletit ovat arkipäivää nykyisessä yrityskulttuurissa ja ovat helpottaneet suunnattomasti sekä työelämää että ihmisten arkea. Kuitenkin näihin laitteisiin liittyy huomattavia tietoturvariskejä.
Ehdottomasti suurin riski on varkaudet ja katoamiset. Usein näissä laitteissa on paljon työhön liittyvää materiaalia ja mikäli ne sisältävät arkaluontoista tietoa, on edellä mainituissa tilanteissa suuri vaara, että tieto voi joutua vääriin käsiin. Vaikka yritykset ovatkin satsanneet niiden suojaukseen salasanojen, todennusmenetelmien ja kryptauksen avulla, ovat nekin murrettavissa taitavissa käsissä.

ISACAN & RSA:n tutkimuksessa kysyttiin yrityksiltä antavatko he mobiililaitteita työntekijöittensä käyttöön. Kyllä vastasi 82,57% ja ei vain 17,43%. Kun heiltä kysyttiin, onko heidän yrityksessään ollut laitteiden fyysisiä katoamisia, oli mobiililaitteiden osuus 91,40% kaikista laitteista. (ISACA & RSA 2014, 11.)

Samassa tutkimuksessa mobiililaitteiden katoamisten ja sisäisten varkauksien suhde oli 43,89% katoamisille ja 25,28% varkauksille. (ISACA & RSA 2014, 6.)

PWC:n tutkimuksessa 15% isoista yrityksistä koki tietoturvaloukkauksen tai tietovuodon, jossa oli mukana joko tabletti tai älypuhelin. Vuoden takaiseen tilanteeseen nousua on 7%. (PWC 2015, 9.)

Kun yrityksiltä kysyttiin kuinka paljon mobiililaitteisiin kohdistuvat uhat ovat muuttuneet viimeisen 12 kuukauden aikana, kuusi kymmenestä vastasi että luku on noussut. Tämä trendi ja alhainen mobiililaitteiden tietoturvakäytäntöjen haltuunotto selittää osaltaan sen miksi mobiililaitteet katsotaan heikoimmaksi lenkiksi suurimassa osassa yrityksien puolustusstrategiaa. Mitä tulee eri maanosiin, Eurooppalaiset vastaajat (64%) katsoivat mobiililaitteisiin kohdistuvan uhan kasvaneen esimerkiksi Pohjois-Amerikkalaisiin verrattuna (57%). (CyberEdgeGroup 2015, 18.)

Yksi suuri riski, jota ei tuoda esille näissä tutkimuksissa, mutta jota yritysten on mietittävä vakavasti, on työntekijöiden omien, suojaamattomien ja yrityksen standardien vastaisten mobiili- ja datalaitteiden tuominen sisäiseen verkkoon. Samaan kategoriaan voidaan laskea myös omat suojaamattomat ohjelmistot. Nämä kaikki ovat potentiaalisia haitta-, vakoilu- ja virusohjelmien välitysväyliä ja mikäli niihin ei puututa, ne voivat aiheuttaa yritykselle huomattavaa vahinkoa. Paras tapa tai toimivin, on yksinkertaisesti kieltää omien laitteiden ja ohjelmien tuonti ja asentaminen tai sitten varmistaa, että ne ovat tarkistettu ja asianmukaisesti suojattu ennen verkkoon liittämistä.

3.5 Työntekijöiden tekemät tietoturvarikokset

Tietoturvarikoksiksi lasketaan sellaiset hyökkäykset, joissa työntekijä on tarkoituksella saattanut työnantajansa tietoturvauhan uhriksi. Näitä ovat esimerkiksi petos, väärinkäytökset, tietojen tahallinen muuttaminen, varkaudet, järjestelmän tahallinen vahingoittaminen tai toimintakyvyttömäksi saattaminen, lahjonta ja vakoilu. Niiden motiiveina toimivat yleensä pettymys työnantajan toimintaan, irtisanominen tai taloudellisen hyödyn tavoittelu.

Kyseessä saattaa olla kaltoin kohdeltu ohjelmistokehittäjä, joka on turhautunut johdon toimintaan tai terveydenhoitotehtävissä toimiva työntekijä, joka on rekrytoitu organisoidun rikollisuuden palvelukseen. Ehkäpä jopa se kellarissa istuva kaveri, joka suree kadonnutta nitojaansa. Huolimatta siitä keitä he ovat, totuus on se, että he ovat tarkoin suunniteltujen turvatoimiemme sisäpuolella ja he aiheuttavat vahinkoa tiedoillemme. (Verizon 2016, 35.) Tahallisten hyökkäysten kirjo on mittava, tässä muutamia esimerkkejä työntekijöiden tekemistä tietoturvahyökkäyksistä sekä niiden seurauksista:

3.5.1 Iso-Britannia

> Ison Kaakkois-Englannissa sijaitsevan konsultointifirman työntekijä sai haltuunsa arkaluontoisia asiakastietoja ja käytti niitä liiketoiminnan kasvattamiseen ilman lupaa. Tapaus aiheutti yritykselle maineen menetystä, laillisia toimenpiteitä sekä 500 000 punnan menetyksen. Tapauksen jälkeen yritys otti käyttöönsä kohdennetun tietoturvakoulutuksen työntekijöilleen. (PWC 2015, 16.)
>
> Ison laitetuottajan it-osastolla työskennellyt henkilö varasti arkaluontoisia, yli 500 000 punnan arvoisia tietoja. Tapaus vaikeutti yrityksen liiketoimintaa huomattavasti ja aiheutti maineen menetystä. Liiketoiminnan palauttamiseen meni viikosta kuukauteen ja rahallinen, korjauksesta aiheutunut kulu oli 100 000 – 249 999 puntaa. (PWC 2015, 22.)

3.5.2 USA

Ryan Francis on koonnut artikkeliinsa yhdeksän eri USA:ssa tapahtunutta tapausta:

> Terry Childs, entinen San Franciscon verkkoasiantuntija, piti kaupungin järjestelmiä hallinnassaan jonkin aikaa. Hän ei suostunut antamaan salasanoja, koska väitti etteivät hänen pomonsa ole päteviä. Childs tuomittiin Kalifornian tietokonelakien rikkomisesta huhtikuussa 2010.
>
> Kesäkuussa 2012, öljy- ja kaasuyrityksen EnerVestin entinen verkkosuunnittelija Ricky Joe Mitchell Charlestonista tuomittiin vankeuteen yrityksen järjestelmien sabotoinnista. Hän sai tietää, että oli saamassa potkut ja päätti palauttaa yrityksen serverit tehdasasetuksille.
>
> Vuonna 2007 tuli ilmi, että tietokanta-asiantuntija William Sullivan oli varastanut 3.2 miljoonaa asiakastietoa, mukaan lukien luottokortti-, pankki- ja henkilötietoja Fidelity National Information Services-yritykseltä. Hän myönsi syyllisyytensä ja tuomittiin neljäksi vuodeksi ja yhdeksäksi kuukaudeksi vankeuteen ja määrättiin maksamaan 3.2 miljoonan USA:n dollarin korvaukset.
>
> Flowersin sairaalassa oli sisäinen vuoto kesäkuusta 2013 helmikuuhun 2014 kun eräs heidän työntekijöistään varasti lomakkeita, joissa oli potilastietoja, ja mahdollisesti käytti niitä hakeakseen valheellisia veronpalautuksia.
>
> Techworld.comin mukaan 34-vuotias Sam Chihlung Yin kehitti valheellisen VPN tokenin olemattoman henkilön nimissä, jonka hän huijasi Guccin it-osaston henkilöitä aktivoimaan sen jälkeen kun hän sai potkut toukokuussa 2010.

> Army Private First Classin työntekijä Bradley Manning vuoti arkaluontoisia, armeijan dokumentteja Wikileaksille vuonna 2009. Manning, joka myös tunnetaan nimellä Chelsea Manning, sai 35 vuoden vankeustuomion.
>
> Vuonna 2002, Timothy Lloyd tuomittiin 3,5:ksi vuodeksi vankeuteen ajastetun ohjelmistopommin asentamisesta sen jälkeen kun hän joutui riitoihin työnantajansa Omegan kanssa. Tästä ohjelmistosabotoinnista seurasi miljoonien dollareiden tappio yritykselle sekä 80:n työpaikan menetys.
>
> Alkuvuodesta 2014 NRAD Medical Associates huomasi, että radiologina toiminut työntekijä oli päässyt käsiksi ja saanut haltuunsa suojattuja terveystietoja yrityksen laskutusjärjestelmästä ilman lupaa. Vuoto koski noin 97 000 potilaiden nimi- ja osoitetietoja, syntymäaikoja, sosiaalitietoja, henkivakuutustietoja ja sairausdiagnooseja.
>
> Ja tietysti lopuksi on mainittava kaikkien aikojen kuuluisin tapaus: Edward Snowden. Ennen pakenemistaan maasta, hän vuoti arkaluontoisia NSA dokumentteja, jotka paljastivat tietoa valtionjohdon valvonnasta. (Francis 6.10.2014.)

Kuten voidaan todeta, tahallisista hyökkäyksistä koituu yrityksille usein mittavia rahallisia menetyksiä sekä mahdollisesti myös maineen ja asiakkaiden menetystä.

CGI:n tutkimuksessa todetaan, että julkisuuteen tulleiden tietomurtojen osuus on vain 31 prosenttia kaikista vastauksista. Niistä 7% :ssa syynä on se, etteivät he ole halunneet julkistaa tapahtunutta ja ovat tästä syystä jättäneet ilmoittamatta asiasta viranomaisille. Suurin osa organisaatioista ei tee rikosilmoitusta, koska ajattelee että siitä ei ole mitään hyötyä. Kuitenkin 62% vastaajista on ollut jälkikäteen ollut yhteydessä muihin viranomaisiin tai tietoturvatoimijoihin tietomurron takia. (CGI 2016, 13.)

Suomesta ja muualta on hyvin vaikea saada julkista tietoa tietoturvarikoksista, USA näyttää tässä asiassa olevan kärkimaita. Meillä julkisuuteen tulevien rikosten määrä tulee kasvamaan, kun uusi tietosuoja-asetus astuu voimaan vuonna 2018.

3.6 Tietoturvan yleisen hallinnan ja koulutuksen tila yrityksissä

Millainen tilanne yrityksissä on sitten yleisen tietoturvajohtamisen, työntekijöiden kouluttamisen ja tietoturva-asioista ja -käytännöistä valistamisen suhteen?

CGI:n tutkimuksen mukaan 34 prosentilla kaikkien vastaajien organisaatioista ei ole erikseen nimettyä tietoturvajohtajaa tai -osastoa. Pk-yrityksissä 54 prosenttia on ilman tietoturvasta vastaavaa henkilöä. Yksityisellä sektorilla luvut ovat vielä korkeammat eli 65 prosenttia on ilman yrityksen sisäistä tietoturvavastaavaa ja pk-yrityksissä 76 prosenttia. Kaikista vastaajista 54 prosenttia katsoo, ettei sellaiselle ole nähty tarvetta. Vaikka organi-

saatiot kokevat, ettei tietoturvaan erikoistuneelle henkilölle tai osastolle ole tarvetta, kokevat he silti samaan aikaan, että kyberhyökkäyksen kohteeksi joutumisen riski ja varautumisen tarve ovat kasvaneet. (CGI 2016, 4.)

Kysyttäessä yrityksiltä kuka heillä hoitaa tietoturvallisuusasioita, oli vastauksena toimitusjohtaja tai jokin muu johtaja (18%). Vastanneista 33% ilmoitti vastuussa olevan IT-johtaja, joka vastasi tietoturvallisuudesta oman työnsä ohella. Kaiken kaikkiaan noin 50 prosentissa organisaatioista tietoturvallisuutta hoitaa joku muu kuin siihen erikoistunut taho (CGI 2016, 5.)

PWC:n tutkimuksessa todetaan, että 28% vastaajista ilmoitti pahimpien hyökkäysten olevan seurausta ylimmän johdon riittämättömästä paneutumisesta tietoturvaan.(PWC 2015, 14.)
Samassa tutkimuksessa 14% vastaajista ilmoittaa, etteivät ole ilmoittaneet johdolle yrityksessä ilmenneistä tietoturvariskeistä. (PWC 2015, 7.)
Koulutuksen suhteen tutkimuksessa todetaan, että 72% isoista ja 63% pienistä yrityksistä tarjoavat työntekijöilleen jatkuvaa tietoturvavalistusta ja koulutusta. (PWC 2015, 7.)
Kuitenkin 72% yrityksistä, joissa tietoturvakäytännöt olivat huonosti ymmärrettyjä, oli myös työntekijöistä johtuvia hyökkäyksiä. (PWC 2015, 8.)
Ottaen huomioon työntekijöistä johtuvat hyökkäykset, on selvää, että koulutus on tärkeää. Yritysten olisi kuitenkin mietittävä kuinka tehokasta heidän nykyinen tarjontansa on kun kerran hyökkäysten määrä on selvässä nousussa. (PWC 2015, 15.)

CyberEdgeGroupin tutkimuksessa kysyttiin, mitkä seikat eniten rajoittavat yrityksen hyökkäyksiltä suojautumismahdollisuuksia. Alhainen tietoturvatietoisuus työntekijöiden keskuudessa oli ensimmäisenä ja rahoituksen puute toisena. Muita merkille pantavia rajoitteita olivat mm. liian suuri tietomäärä, tietoturvaosaamisen puute sekä johtotason tuen ja tiedostamisen puute tietoturva-asioissa. (CyberEdgeGroup 2015, 22.)

Yrityksen tietojen suojaaminen on yksi merkittävä osa-alue sisäisten hyökkäysten vastustamisessa.

Biscomin tutkimuksessa on paneuduttu tähän asiaan enemmän. Siinä todetaan, että yksi neljästä vastaajasta kertoi ottaneensa tietoja kun lähtivät yrityksestä. Vastaajista 15% sanoivat ottavansa tietoa mukaan mikäli heidät irtisanoutumisen sijaan irtisanotaan tai lomautetaan. Niistä, jotka ottavat tietoja mukaansa, 85% ilmoittivat, että ottamansa materiaali on heidän itsensä tekemää eivätkä he sen vuoksi näe siinä mitään väärää. Kun suurin osa työntekijöistä ottaa itse tekemää materiaalia, vain 25% ottaa mukaan sellaista joka on

jonkun muun tekemää. Vastaajista 95% toteaa, että tällainen toisten henkilöiden tekemän materiaalin mukaanotto on mahdollista, koska joko heidän yrityksessään ei ole toiminta-suunnitelmaa tai teknologiaa estää tietojen varastaminen. Tai jos sellaisia on ollut, yritys ei välitä niitä noudattaa.
Tutkimus osoitti myös, että niillä teknologioilla, jotka yrityksissä on käytössä, on myös merkitystä tietojen varastamisessa. Esimerkiksi Dropboxista, Google Drivesta ja sähköpostista tiedostojen noukkiminen on hyvin vaivatonta.
Tutkimustulokset paljastavat, että työntekijät ovat suuri tietoturvariski tässä asiassa. Yritykset voivat hyödyntää sen tuloksia ymmärtääkseen paremmin, kuinka he voivat turvata tietojaan. Oli se sitten koulutuksen päivittämistä, tiukempien toimintaperiaatteiden käyttöön ottoa tai tietojen turvaamiseen ja seuraamiseen liittyvien työkalujen hankintaa.
Vaikka tietojen varastaminen onkin suuri tietoturvariksi, suurin osa vastaajista ei nähnyt asiaa tällä tavalla. Työntekijät uskoivat, ettei heidän toimintansa ole vihamielistä vaikka ottivatkin arkaluontoista tietoa, yrityksen strategiaa käsitteleviä dokumentteja, asiakaslistoja sekä taloudellisia tietoja. Ehkä juuri tämän asenteen vuoksi toiminta onkin niin yleistä. (Biscom 2015.)

3.7 Yhteenveto

Kaiken kaikkiaan tähän työhön otetuissa tutkimuksissa osassa käsiteltiin samoja asioita ja sitten toisia, hyvin tärkeitä osa-alueita käsiteltiin yllättävän vähän.

Tietojen kalastelu ja verkkohuijaukset ovat yleisiä ja työntekijöitä näyttäisi olevan myös helppo edelleen huijata. Kalasteluviestejä ja saastuneita linkkejä avattiin, vaikka riskit ovatkin tiedossa. USA on tästä poikkeus, siellä suhtaudutaan näihin asioihin vakavasti. Todennäköisesti tämä johtuu siitä, että siellä tietoturva-asioissa ollaan muutenkin muita maita edellä.
Tietojenkalasteluun ja verkkohuijauksiin liittyy selkeästi valistuksen puute eli näistä asioista ei näytetä puhuttavan yrityksissä. Tämä liene suurin syy siihen, miksi työntekijät eivät tajua niihin liittyvää riskiä ja ovat edelleen huijattavissa.
Fyysisiä tunkeutumisia tapahtuu myös jonkin verran. Niitä tehdään luultavasti enenevässä määrin tulevaisuudessa, koska yritykset eivät osaa niihin varautua ja täten ne on helppo toteuttaa.

Vain yhdessä tutkimuksessa käsiteltiin oikeuksien väärinkäyttöä mutta uskoisin, että tilanne vastaa koko maailman tilannetta. Lisäksi käyttäjien toimien valvontaa käsiteltiin tutkimuksissa vähän. Vain yhdessä tutkimuksessa nousi esille niin sanotut etuoikeutetut

käyttäjät ja heidän toimiensa valvonta. Tässä ilmenee puutteita eli yrityksillä ei ole tarpeeksi selkeitä toimintaohjeita eikä myöskään työkaluja valvonnan järjestämiseen. Käyttäjätunnusten varastamiseen ja uudelleenkäyttöön ei myöskään oltu kiinnitetty tutkimuksissa niin paljon huomiota kuin ehkä pitäisi.

Sosiaalisissa medioissa ja sopimattomilla internetsivuilla surffaillaan tutkimusten mukaan työpaikoilla, riskit joko tiedostaen tai ei. Yhdessä tutkimuksessa kävi ilmi, että internetin käyttöä valvotaan kohtuullisesti, muissa asiaan ei oltu paneuduttu ollenkaan. Voidaan siis todeta, että internetkäytössä ja sen valvonnassa olisi parantamisen varaa.

Mobiililaitteiden käyttö on hyvin yleistä yrityksissä eri puolilla maailmaa. Niitä myös katoaa tai varastetaan kohtuullisesti. Tässä tilanteessa siis niiden antama hyöty katsotaan olevan selvästi suurempi kuin niihin liittyvät uhat. Tietovuotoja, joissa osallisena on mobiililaite, tapahtuu jonkin verran. Mobiililaitteisiin liittyvä uhka on myös joidenkin tutkimusten mukaan nousussa.
Toin itse esille myös omien, suojaamattomien ja yrityksen standardien vastaisten mobiili- ja datalaitteiden tuomisen yritysten sisäiseen verkkoon ja niihin liittyvät riskit, koska minua yllätti, ettei asiaan paneuduttu missään tutkimuksessa.

Tahallisia hyökkäyksiä tapahtuu maailmanlaajuisesti jonkin verran. Ongelmana on se, ettei niistä välttämättä raportoida viranomaisille. Yhdessä tutkimuksessa tosin ilmoitettiin, että viranomaisiin oltiin oltu yhteydessä viiveellä. Suomessa tilanne on se, että kynnys ilmoittamiselle on edelleen liian iso tai katsotaan, että asian selvittämiseen menee liikaa aikaa ja resursseja. USA:ssa sen sijaan on jo annettu melkoinen määrä tuomioita tietoturvarikoksista ja maa on muihin verrattuna selkeästi edelläkävijä tässä asiassa.

Ehkä huolestuttavin piirre tutkimuksissa oli se, kuinka vähän yrityksissä panostetaan kunnolliseen tietoturvaan erikoistuneen asiantuntijan tai asiantuntijaryhmän toimintaan. Edelleen katsotaan ettei sellaiselle ole tarvetta vaikka hyökkäykset ovat lisääntymässä koko maailmassa.
Lisäksi huolestuttavaa on myös se, että usein vastuu tietoturvallisuudesta on sellaisella henkilöllä, joka ei ole lainkaan perehtynyt asiaan tai yrittää hoitaa sitä oman toimen ohella. Ei siis ihme, että viimeisten vuosien aikana tietoturvapalveluita tarjoavien yritysten määrä on kasvanut huimasti. Näyttää siltä, etteivät yritykset eivät halua satsata rahallisesti omiin tietoturva-asiantuntijoihin vaan ostavat palvelun mieluummin muualta. Kuinka hyvä asia se on, sen tietysti päättää jokainen yritys itse.

Tietoturvaan liittyvää koulutusta tarjotaan yrityksissä jonkin verran. Toisaalta koulutuksen

sisältö ei välttämättä ole niin tehokasta kuin sen pitäisi olla. Tuntuu siltä, etteivät työntekijät siitä huolimatta osaa varautua tilanteisiin siten kun pitäisi. Tässäkin olisi yrityksillä parantamisen varaa.

Tietojen suojaamisessa työntekijän irtisanomistilanteissa oli yhden tutkimuksen mukaan puutteita. Heidän mukaansa lähtee kohtuullisesti työhön liittyvää materiaalia, pahimmassa tapauksessa arkaluontoista tietoa. Selkeät ohjeistukset ja käytännöt puuttuvat monilta yrityksiltä näiden tilanteiden osalta.

4 Uhan välttäminen ja siltä suojautuminen

Millaisia toimia yritykset voivat sitten tehdä ja millaisia työkaluja käyttää suojautuakseen työntekijöiden taholta tulevilta uhilta?

Jokaisen yrityksen kannattaisi kysyä itseltään seuraavat kysymykset:

- Millaiseen tietoon hyökkääjän toiminta yrityksessä kohdistuisi?
- Millaisiin, näitä tietoja sisältäviin järjestelmiin hyökkäys kohdistuisi?
- Kenellä on pääsy kriittisiin tietoihin?
- Mikä olisi helpoin tapa vahingoittaa työntekijää?
- Millaisia keinoja ja työkaluja tietotekniikasta vastaavat voivat hyödyntää ehkäistäkseen ja huomatakseen nämä hyökkäykset?
- Onko yrityksessä budjetoitu tarpeeksi sisäisten hyökkäysten vastustamiseen?
- Millaiselta tietoturvasuunnitelma, jossa on otettu mukaan myös sisäiset hyökkäykset, näyttäisi yrityksessä? (Cole 2015, 11.)

Tämän jälkeen määrätään tavoitetila, alkaa varsinainen tietoturvan suunnittelu ja määritellään ne keinot ja työkalut joilla tähän tilaan päästään.
Koska huomioitavia asioita on monia, olen keskittynyt niiltä uhilta suojautumiseen, joita tässä työssä on tullut esille.

Tietojenkalastelua vastaan parhain suojautumiskeino perinteisten, teknisten roskapostisuodattimien ja verkkovalvontatyökalujen lisäksi on ehdottomasti työntekijöiden koulutus. Kuten tässä tutkimuksessa on tullut esille, siinä on paljon parantamisen varaa sekä määrässä että laadussa. Koulutuksen pitää olla riittävää ja ennen kaikkea jatkuvaa, jotta asia ikään kuin pysyy koko ajan muistissa.

> Mitä tulee työntekijöihin, tarjoa heille vain sellaisia laitteita, jotka olet itse asentanut ja konfiguroinut. Anna heille pääsy vain sellaisiin järjestelmiin, jotka ovat työn kannalta välttämättömiä ja poista pääsy heti kun he ovat tehneet työnsä. Varmista, että heidän tietokoneen käytöstään ja muutoksistaan, joita he tekevät, jää talteen lokitietoja ja muista auditoida näitä. (F-Secure 2017, 23.)

Lokitietojen keräyksen ja niiden valvonnan lisäksi on syytä myös satsata varsinaisiin tunkeutumisen havainnointi- ja esto-ohjelmiin, joilla voidaan mahdollisesti estää hyökkäys jo varhaisessa vaiheessa tai selvittää tilanne nopeasti, mikäli se on jo päässyt tapahtumaan.

Salasanoihin ja niiden varastamiseen liittyviä riskejä voidaan minimoida esimerkiksi keskitetyillä identifiointihallintaratkaisuilla. Nämä ratkaisut ovat hyvä vaihtoehto myös käyttäjätilien resursseihin pääsyhallinnan kannalta, jolloin työntekijöillä on pääsy vain työn kannalta välttämättömimpiin resursseihin.

Käyttäjien internetin käytön valvominen olisi suotavaa ja sitä olisi lisättävä tai jopa rajoitettava kokonaan tietyille sivustoille pääsyä. Valvonnan suhteen kuitenkin muistettava lakiin perustuva yksityisyyden suoja eli jos käyttöä tarkkaillaan, on siitä kerrottava myös työntekijälle.

> Yrityksen tietojen lähtemistä työntekijöiden mukaan kun heidän työsuhteensa päättyy, voidaan estää luomalla niihin liittyviä käytäntöjä ja toimintoja keskittyen työntekijöiden toiminnan valvomiseen, rajaamalla heidän pääsyä tietoihin, vaatimalla arkaluontoisten tietojen kryptausta, hallinnoimalla laitteita oikeaoppisesti, varmistumalla, että tiedot on varmuuskopioitu ja arkistoitu oikein ja vaatimalla vain yrityksen vahvistamia sovelluksia, jotka voidaan etähallinnalla pyyhkiä tyhjäksi myös henkilökohtaisista laitteista. (Osterman Research 2016.)

Hallituilla henkilöstöprosesseilla eli työhöntuloon ja työsuhteen päättymiseen liittyvät ohjeistukset ja toimintaperiaatteet lisäävät työntekijöiden tietoisuutta siitä, mitä tietoturvaan liittyviä toimenpiteitä ja velvollisuuksia heiltä odotetaan. Tämä tietysti edellyttää, että yrityksessä on selvitetty ensin mitkä ovat yrityksen toimintaperiaatteet ja miten työtä toivotaan tehtävän. Esimerkiksi työhöntulotilanteessa voidaan työntekijälle antaa allekirjoitettavaksi ohjeet, joita hänen tulee noudattaa työsuhteen keston ajan. Jotkut yritykset liittävät tähän myös vaitiolovelvollisuuksiin ja yrityssalaisuuksiin liittyviä sopimuksia.

> ”Tarkkaavaiseksi koulutettu henkilökunta on paras suoja uhkia vastaan” (Viestintävirasto 2017, 4).

> Yrityksen johtoryhmien ja ylemmän johdon pitäisi pohtia, tekevätkö he riittävästi töitä tietoturvakulttuurin vahvistamiseksi yrityksessään tällaisena aikana jolloin sisäiset, vahingossa tapahtuvat tietovuodot on ehdottomasti suurin syy tietoturvaloukkauksille. Yritysten pitäisi tutkia kuinka tehokasta heidän koulutuksensa on, onko se pakollista, interaktiivista, testattua ja sitovaa vai onko se vapaaehtoista ja kärsii alhaisesta osanotosta. (PWC 2015, 15.)

> Kyberturvallisuuskoulutuksia tulisi pitää koko henkilöstölle ja näin antaa kaikille käsitys mahdollisista uhista. Koulutusten tulisi myös olla jatkuvia, koska rikolliset keksivät aina uusia keinoja hyökkäyksien toteuttamiseen. Hyvin päivitetyllä tietoturvatiedolla/tietoturvapolitiikalla voidaan säästää paljon yrityksen varoja sekä pystytään välttämään ikäviä tilanteita. (Ikonen 2015.)

Koulutukseen ja ennen kaikkea sen suunnitteluun liittyen on hyvä ottaa esille myös psykologinen puoli eli se, miten me ihmiset olemme rakentuneet ja miten me toimimme.

> Ihmiset tekevät virheitä ja voivat välillä olla tyhmiä. Tämä pitää tiedostaa pikemminkin kun teeskennellä ettei sitä tapahdu. Tämä väite ei ole vihamielinen eikä alentava, se on fakta joka tekee työn helpommaksi. Kun tiedostetaan, että me kaikki teemme virheitä, voimme helpommin yrittää auttaa yritystämme välttämään, vähentämään tai muuttamaan ikävien tilanteiden vaikutusta. (McIlwraith 2006, 21.)

Tambe Ebot kuvaa väitöskirjassaan miksi ihmiset joutuvat tietojenkalastelun uhreiksi. Tulosten mukaan uhriksi joutumiseen vaikuttavat sekä henkilökohtaiset tavat, että internetin käyttötottumukset. Vaikuttavana tekijänä on myös henkilön tietoisuus tietoturvallisuudesta ja internetin käyttöön liittyvistä riskeistä. Verkkoa vähemmän käyttävällä henkilöllä on vähemmän kokemusta tietoturvallisuusuhkista, ja hän saattaa tulkita huijausviestit aidoiksi. Kokeneempi käyttäjä taas päätyy uhriksi esimerkiksi yrittäessään suojella itseään mahdolliselta kiristykseltä. Aiemmat tutkimukset ovat niputtaneet tietojenkalastelun uhrit yhtenäiseksi joukoksi, mutta Tambe Ebotin mukaan huijauksen välttämiseksi annetut ohjeet on parasta yksilöidä käyttötottumusten perusteella. (Ebot 2017.)

5 Pohdinta

Tähän lukuun olen koonnut omia ajatuksia tutkimuksista, tietoturvan tilasta yleensä ja niistä seikoista, jotka tätä työtä tehdessä nousivat esille.

Ensinnäkin mitä tulee työhön otettuihin tutkimuksiin, useissa oli käyty läpi samoja asioita vain hieman eri tavalla kysyttynä. Huomiota herättävää ja ehkä huolestuttavaakin ole se, että joitakin hyvin tärkeitä tietoturvaan liittyviä asioita ei oltu käsitelty ollenkaan. Ehkä olisi syytä keskittyä enemmän tasapuolisesti kaikkiin osa-alueisiin sen sijaan, että tehdään useita kysymyksiä samasta asiasta.

Lisäksi minua henkilökohtaisesti häiritsee suunnattomasti se, että kaikki nämä tutkimukset on suunnattu aina it-alan toimihenkilöille tai johtotehtävissä toimiville henkilöille. Mitään tutkimusta ei ole suunnattu tavalliselle työntekijälle. Kun kerran heidän toivotaan toimivan toisin tietoturva-asioissa, olisi todellakin ehdottoman tärkeää kysyä heidän mielipidettään ja kuunnella heidän ehdotuksiaan enemmän, jotta esimerkiksi aiheeseen liittyvää koulutusta voisi suunnitella paremmin ja yritykset osaisivat valistaa heitä oikein.

Lopuksi totean, että tietoturvaan liittyvissä asioissa on edelleen puutteita eri osa-alueilla ja työtä riittää varmasti myös jatkossa. Varsinkin kun hyökkäystekniikat ja hyökkääjät muuttuvat päivä päivältä haastavimmiksi ja taitavimmiksi. Tämä vaatii satsausta yrityksiltä, niin rahallisesti kun resursseissa. Trendi näyttäisi kuitenkin olevan se, että yritykset alkavat hitaasti tiedostaa tietoturvan merkityksen ja tajuta ne ongelmat, joita sen puute saa aikaan yrityksen toiminnassa.

Lähteet

AlcoSec RSA Conference-survey. State of Network Security 2014. Luettavissa: https://www.algosec.com/wp-content/uploads/2016/03/Report_2014State-of-Network-Security_0401_2014.pdf. Luettu 27.3.2017.

Biscom 2015. Employee Departure Creates Gaping Security Hole. Luettavissa: https://www.biscom.com/employee-departure-creates-gaping-security-hole-says-new-data/. Luettu 1.4.2017.

Blue Coat 19.5.2015. Luettavissa: https://www.symantec.com/about/newsroom/press-releases/bc-2015/research-shows-workers-ignoring-known-cyber-risks-surfing-adult-content .Luettu 28.3.2017.

CGI 2016. Kyberturvallisuuden tila suomalaisissa organisaatioissa 2016- tutkimus. Luettavissa: https://www.cgi.fi/sites/default/files/files_fi/pdf/cgi_kyberturvallisuuden-tila_tutkimuraportti2016.pdf . Luettu: 6.3.2017.

Cole, E. 2016. Taking action against the insider threat. Luettavissa: https://www.sans.org/reading-room/whitepapers/analyst/action-insider-threat-37322. Luettu 1.4.2017.

CyberEdgeGroup 2015. Cyberthreat Defense-raportti Pohjois-Amerikka ja Eurooppa. Luettavissa: https://www.netiq.com/docrep/documents/xvbozdzzxj/CyberEdge_2015_CDR_Report.pdf. Luettu 29.3.2017.

Ebot, T. 26.1.2017. Explaining two forms of Internet crime from two perspectives: toward stage theories for phishing and Internet scamming. Luettavissa: https://www.jyu.fi/ajankohtaista/arkisto/2017/01/tiedote-2017-01-23-08-47-05-198328. Luettu 1.4.2017.

Francis, R. 6.10.2014. Nine employee insiders who breached security. Luettavissa: http://www.csoonline.com/article/2692072/data-protection/data-protection-165097-disgruntled-employees-lash-out.html. Luettu 30.3.2017.

F-secure 2017. State of Cyber Security- raportti. Luettavissa: https://fi.business.f-secure.com/kyberturvallisuuden-tila-2017/ . Luettu 7.3.2017.

Gutman, P. 2014. Security Engineering. Luettavissa: https://www.cs.auckland.ac.nz/~pgut001/pubs/book.pdf . Luettu: 1.4.2017.

IBM 2016. IBM Kyber-turvallisuustutkimus. Luettavissa: https://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03133usen/SEW03133USEN.PDF. Luettu: 16.2.2017.

Ikonen, I. 2.5.2015. Käyttäjien manipulointi. Luettavissa: http://www.hackingthroughcomplexity.fi/2015/09/kayttajien-manipulointi.html. Luettu 28.4.2017.

Iltalehti 12.4.2017. Supon asiantuntija urkintatapauksesta: Tekijä tiennyt, että väärinkäyttö on rikos. Luettavissa: http://www.iltalehti.fi/uutiset/201704122200102068_uu.shtml. Luettu 15.4.2017.

ISACA & RSA Conference Survey 2014. State of Cybersecurity: Implications for 2015. Luettavissa: http://www.isaca.org/cyber/documents/state-of-cybersecurity_res_eng_0415.pdf. Luettu 21.3.2017.

MCIllwright, A. 2006. Information Security and Employee Behaviour. Luettavissa: https://books.google.fi/books?id=XnBOhKHJKMQC&hl=fi . Luettu 1.4.2017.

Miettinen, J. 1.9.2015. Näin nettihuijari iskee – HS esittelee viisi tyypillistä petkutusta netissä. Luettavissa: http://www.hs.fi/talous/art-2000002849255.html. Luettu 28.4.2017.

Osterman Research 2016. Best Practices for Protecting Your Data When Employees Leave Your Company. Luettavissa: http://info.archive360.com/hubfs/Pdf/best-practices-for-protecting-data-when-employees-

leave.pdf?__hssc=67876814.1.1483474653805&__hstc=67876814.b99568fca2405fd6ae291040c76b596e.1483474653805.1483474653805.1483474653805.1&__hsfp=907893354&hsCtaTracking=ba1ca800-c2bd-4470-9655-f2b259120fae%7C5581f17e-5839-4874-a4b8-2e2539fce76b. Luettu 12.4.2017.

PWC 2015. Information Security Breaches Survey. Luettavissa: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf. Luettu 24.3.2017.

Salminen, A. 2011. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Luettavissa: http://www.uva.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf. Luettu 2.3.2017.

Tietosuojavaltuutetun toimisto 27.1.2014. Internetin käytön ja työntekijöiden verkkoselailun eli ns. verkkosurffailun valvonta työpaikalla. Luettavissa: http://www.tietosuoja.fi/fi/index/ratkaisut/internetinkaytonjatyontekijoidenverkkose.html. Luettu: 8.5.2017.

Verizon 2016. Data Breach Investigations report. Luettavissa: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/. Luettu: 12.1.2017.

Viestintävirasto 2017. Tietoturvan vuosi 2016. Luettavissa: https://www.viestintavirasto.fi/attachments/tietoturva/Tietoturvan-vuosi_2016_ViVi_29-11-2017_L.pdf. Luettu 14.3.2017.

Worrall, J. 14.10.2014. The insider threat is priviledged access, not a person. Cyber ark blog, security and risk-osio. Luettavissa: https://www.cyberark.com/blog/insider-threat-privileged-access-person/. Luettu 13.4.2017.