Haaga-Helia
ammattikorkeakoulu Oy

Inhimilliset tekijät kyberturvallisuudessa

Pekka Pulsa

Opinnäytetyö
Tietojenkäsittely
2021

Tiivistelmä

Haaga-Helia
ammattikorkeakoulu Oy

Tekijä
Pekka Pulsa

Koulutusohjelma
Tietojenkäsittely

Raportin nimi
Inhimilliset tekijät kyberturvallisuudessa

Sivu- ja liitesivumäärä
23 + 2

Tämän opinnäytetyön tavoitteena oli löytää yleisimmät inhimilliset tekijät kyberturvallisuuteen liittyen ja niiden aiheuttamat riskit kyberturvallisuudessa. Näiden lisäksi tavoitteena oli esittää lukijalle yrityksien tietoturvallisuuteen liittyviä asioita yleisellä tasolla, sitä miten tieto yrityksissä syntyy ja miten tieto voidaan hävittää tietoturvallisesti. Tutkimuksesta rajattiin pois kyberturvallisuus julkisella tasolla.

Opinnäytetyö aloitettiin tammikuussa 2021 ja se saatettiin päätökseen toukokuussa 2021. Alun perin opinnäytetyö oli määrä toteuttaa kvalitatiivisesti haastatteluiden perusteella, mutta sopivia haastateltavia ei turvallisuussyistä löytynyt. Tämän vuoksi opinnäytetyö toteutettiin erilaisten aineistomateriaalien, kuten aikaisempien tutkimusten, perusteella.

Opinnäytetyön täsmennetyt tutkimuskysymykset olivat:

- Mitkä ovat yleisimpiä inhimillisiä tekijöitä kyberturvallisuudessa?
- Miten ne vaikuttavat kyberturvallisuuteen?
- Kuinka inhimillisiin tekijöihin ja niiden tuomiin riskeihin voi vaikuttaa?

Opinnäytetyössä selvitettiin yrityksen tietoturvaa yleisellä tasolla, sitä miten tieto yrityksissä syntyy ja miten sitä käsitellään. Tämän lisäksi opinnäytetyössä selvitettiin internetin käytön yleisyyttä Suomessa, inhimillisiä tekijöitä kyberturvallisuudessa ja miten niitä voidaan huomioida, tietovuotojen kustannuksia sekä erillinen tutkimusosuus aikaisemmin teetettyjen tutkimusten perusteella.

Tutkimuksessa nousi esille se, että inhimilliset tekijät ovat merkittävä uhka yritysten ja yksilön tietoturvalle. Tietojenkalastelun yleisyys on noteerattu myös Kyberturvallisuuskeskuksessa. Alati digitalisoituvassa maailmassa, jossa elämämme siirtyvät yhä enemmän internetiin, inhimilliset tekijät olisi tärkeää ottaa huomioon jokapäiväisessä elämässä.

Asiasanat
Inhimilliset tekijät, Kyberturvallisuus, Tietovuoto, Internet, Yritysturvallisuus

Sisällys

1 Johdanto

Elämme alati digitalisoituvassa maailmassa, jossa kyberturvallisuuden merkitys nousee ensisijaisen tärkeään asemaan. Verkossa liikkuu nykyisin jatkuvasti kasvavissa määrin rikollisia ja Morganin (Morgan 2020) mukaan verkossa tapahtuvat rikokset ja siitä aiheutuvat kustannukset tulevat ylittämään kuuden biljoonan USA:n dollarin rajan vuoteen 2021 mennessä, tehden siitä näin maailman kolmanneksi suurimman ekonomian. Morgan myös ennustaa (Morgan 2020), että verkossa tapahtuva rikos tulee ylittämään 10.5 biljoonan USA:n dollarin rajan vuoteen 2025 mennessä, tehden siitä näin maailman nopeiten kasvaneen ekonomian maailman historiassa. Suomessa Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta sekä tuottaa tietoturvallisuuden tilannekuvaa (Kyberturvallisuuskeskus).

Tutkimuksen idea sai alkunsa Psykoterapiakeskus Vastaamon tietomurrosta, joka tuli julkisuuteen lokakuussa 2020. Tietomurron yhteydessä nimimerkillä ”ransom_man” kulkenut henkilö kertoi, että hänen hallussaan on 40 000 ihmisen psykoterapiaistuntojen tiedot. Tietojen poistamisesta hän vaati 40 Bitcoinin, eli noin 450 000 euron, lunnaita. Tietomurron seurauksena tietomurron uhrit tekivät marraskuun alkuun mennessä noin 25 000 rikosilmoitusta (Paakkanen 2020). Vastaamon tarina tuli päätökseen helmikuussa 2021, kun yritys haettiin konkurssiin ja entisten omistajien omaisuutta takavarikoitiin 10 miljoonan euron edestä.

Internetissä ja sen keskustelupalstoilla, kuten Ylilaudalla, käytiin rohkeaa spekulaatiota siitä, että Vastaamon tietokannan kirjautumistunnus sekä salasana olisivat olleet ”root”. Tämän rohkean väitteen vuoksi halusin tutkia kyberturvallisuutta inhimillisten tekijöiden osalta, ja kuinka nämä inhimilliset tekijät vaikuttavat yrityksen tai yksityishenkilön kyberturvallisuuteen ja kuinka näitä tekijöitä voisi minimoida. Tämä myös johti siihen, että tutkimus ylipäätään kirjoitettiin.

Vastaamon tietomurtotapaus toi myös mieleeni omia kokemuksiani sosiaali- ja terveysalalta. Olen työskennellyt useassa eri yksikössä ja lähes jokaisessa yksikössä huomasin sen, että esimerkiksi potilastietojärjestelmät jätettiin tietokoneilla auki, kun potilaita lähdettiin hoitamaan. Tämän lisäksi on myös hyvä huomioida organisaatioon mahdollisesti kohdistuva maineriski. Maineriskin kautta yhtiö voi menettää imagonsa ja tuhota sen täydellisesti hetkessä, aiheuttaen myös mahdollisen taloudellisen riskin – esimerkiksi vuonna 2018 henkilökuljetuspalveluita tarjoava Uber tuomittiin 148 miljoonan USA:n dollarin sak-

koihin, kun Uber peitti tietoisesti tietomurron yli vuoden ajan, jossa jopa 57 miljoonan asiakkaan ja kuskin tiedot vuodettiin internetiin (BBC 2018). Sijoittajaguruksi tituleeratun Warren Buffetin sanoin:" It takes 20 years to build a reputation and five minutes to ruin it". Tämän takia on ensisijaisen tärkeää pyrkiä tunnistamaan yleisimmät inhimilliset tekijät ja niiden aiheuttamat riskit kyberturvallisuudessa.

1.1 Tavoitteet ja rajaukset

Tutkimuksen tavoitteena on selvittää yleisimmät inhimilliset tekijät ja niiden aiheuttamat riskit kyberturvallisuudessa. Tutkimuksen tavoitteena on selvittää, että miten yritys tai yksityishenkilö voi välttää näitä tekijöitä arjessaan alati digitalisoituvassa maailmassa. Tämän lisäksi tutkimuksessa käsitellään yrityksen tietoturvaa yleisellä tasolla sekä sitä, että mistä yritysten tieto syntyy ja miten nämä tiedot hävitetään oikeaoppisella tavalla. Tutkimuksen tarkoituksena on käydä myös läpi tietovuotojen ja -murtojen kustannuksia organisaatiolle yleisellä tasolla.

Tutkimusraportin on tarkoitus toimia eräänlaisena ohjeena niin yrityksille, kuin yksityishenkilöille inhimillisten tekijöiden minimoimisesta kyberturvallisuuden parissa.

Tutkimuskysymyksiksi opinnäytetyölle valikoitui seuraavat kysymykset:

- Mitkä ovat yleisimpiä inhimillisiä tekijöitä kyberturvallisuudessa?
- Miten ne vaikuttavat kyberturvallisuuteen?
- Kuinka inhimillisiin tekijöihin ja niiden tuomiin riskeihin voi vaikuttaa?

Tutkimuksessa ei käsitellä kyberturvallisuutta julkisella tasolla, vaan tutkimus keskittyy juuri inhimillisiin tekijöihin ja niiden vaikutuksiin kyberturvallisuudessa.

2 Tutkimusmenetelmät

Alun perin opinnäytetyössä oli määrä hyödyntää erilaisten IT-alan ammattilaisten ja eritoten tietoturva-asiantuntijoiden haastatteluita, mutta Vastaamon tapaus vuoden 2020 loppupuolella sai monet potentiaaliset haastateltavat kavahtamaan haastatteluita. Ongelmakohdaksi kehkeytyi myös se, että moni potentiaalisista haastateltavista pelkäsi enemmän tai vähemmän sitä, että heidät voisi tunnistaa haastatteluiden perusteella, vaikka haastattelut olisi tuotettu nimettöminä.

Tämän vuoksi haastattelut piti jättää tässä opinnäytetyössä kokonaan sivuun ja keskittyä puhtaasti erilaisiin aineistoihin, jotka ovat yhteydessä inhimillisiin tekijöihin kyberturvallisuudessa. Käytettyä aineistoa on vertailtu keskenään ja näiden vertailuiden pohjalta opinnäytetyö kirjoitettiin.

Tutkimusraportin sisältö on koostettu erilaisten tietoturva-asiantuntijoiden sekä tietoturvayhtiöiden tekemistä tutkimuksista. Nämä tutkimusmenetelmät ovat raportin luontiin parhaimmat ja luotettavimmat lähteet, mutta esimerkiksi tietoturvayhtiöiden materiaaleissa on hyvä olla tiettyyn pisteeseen myös lähdekriittinen, koska osissa näissä lähteissä on myös taustalla markkinointia. Markkinoinnin vuoksi lähteiden sisältö on äärimmäisen hyvä tarkastaa aina, kun käy lähteitä läpi.

Internetlähteiden lisäksi lähteiksi valikoitui Juha Leppäsen kirjoittama ja Talentumin julkaisema kirja vuodelta 2006, ”Yritysturvallisuus käytännössä – Turvallisuusjohtamisen portfolio” ja erityisesti kappale 7.5 ”Tietoturvallisuus”, Paul Kearneyn kirjoittama ja IT Governance Ltd:n julkaisema ”Security: The Human Factor” ja David Laceyn kirjoittama ja John Wiley & Sonsin julkaisema ”Managing the Human Factor in Information Security : How to Win over Staff and Influence Business Managers”.

Tutkimusraportin sisällön lähteiksi valikoitui verrattain tuoreet lähteet, koska digitalisoituvassa maailmassa tietoturvauhat voivat olla myös muuttuvia. Lähteiden päivämäärä takarajaksi on otettu Leppäsen kirjaa lukuun ottamatta 10 vuotta.

3 Tietoturva yleisesti

Elämäämme ympäröi nykyisin internet ja erilaiset IoT-laitteet. Aamulla herätessämme älypuhelin ilmoittaa säätiedot ja saat muistutuksen aamupäivän kokouksesta sähköpostiisi. Koronaviruksen aiheuttaman etätyöpandemian vuoksi moni avaa jo työpäätteensä aamukahvia keittäessä, tarkistaen samalla uusimmat koronavirusluvut älypuhelimeltaan. Muistat samalla, että olet unohtanut illalla vastata ystäväsi WhatsApp-viestiin, joten kaiken muun kiireen ohella vastaat ystäväsi viestiin. Päivän päätteeksi huomaat, että jääkaapista alkaa loppua ruoka, joten päätät tehdä ruokatilauksen älypuhelimesi kanssa.

Moni ei välttämättä edes huomaa, että kuinka paljon he ovat tekemisissä internetin kanssa päivittäin, koska sen käytöstä on tullut jo jonkin asteen ”normi”. Internetin normalisoitumisen vuoksi onkin tärkeää kysyä, että miten ihminen voi itse vaikuttaa omaan turvallisuuteensa internetin maailmassa. Teoriaosassa on tarkoitus käsitellä yleisellä tasolla internetin käytön yleisyyttä Suomessa ja sellaisia inhimillisiä tekijöitä, jotka voivat vaikuttaa yksilön tai yrityksen turvallisuuteen.

3.1 Internetin käytön yleisyys Suomessa

Vuonna 2019 79 prosenttia 16–89-vuotiaista käytti internetiä useita kertoja päivässä. Näistä lähes kaikki alle 45-vuotiaat käyttivät internetiä useita kertoja päivässä. Tätä vanhemmissa ikäryhmissä internetin samanlainen käyttö ei ollut yhtä yleistä. Kaiken kaikkiaan 90 prosenttia kaikista 16–89-vuotiaista suomalaisista käyttää internetiä (Tilastokeskus 2019).

Yleisimmin internetiä käytetään matkapuhelimen välityksellä, 83 prosenttia suomalaisista oli vuonna 2019 käytössään älypuhelin, joista valtaosa käytti internetiä sen kautta. Lähes kaikki alle 45-vuotiaat käyttivät internetiä älypuhelimellaan. Älypuhelimet ovat melko yleisiä myös vanhemmilla ihmisillä, mutta vanhemmat ihmiset eivät käytä internetiä älypuhelimilla yhtä yleisesti kuin nuoremmat ihmiset (Tilastokeskus 2019).

Tyypillisesti internetiä käytetään erilaisten asioiden hoitamiseen, eri medioiden seuraamiseen ja viestintään. Verkkopankin käyttö oli Tilastokeskuksen mukaan yleisin asiointitapa internetissä, verkkopankkia olikin käyttänyt viimeisen kolmen kuukauden aikana 85 prosenttia kaikista 16-89-vuotiaista internetinkäyttäjistä. Tilastokeskuksen mukaan joka toinen suomalainen oli ostanut internetin kautta joko tavaroita tai palveluita (Tilastokeskus 2019).

3.2 Yleisesti yrityksen tietoturvasta ja tiedon synnystä

Leppänen määrittelee tietoturvan kirjassaan seuraavasti: ”Tietoturvallisuus koostuu tietoainestoturvallisuudesta, hallinnollisesta ja fyysisestä tietoturvallisuudesta, tietoliikenne-, laitteisto-, ohjelmisto- ja käyttöturvallisuudesta”. Leppäsen mukaan tämän vuoksi ihmiset ja heidän toimintansa vaikuttavat kokonaisuudessaan tietoturvallisuuteen. Leppäsen mukaan tietoturvallisuudella on myös erinäisiä yhtymäkohtia muihin turvallisuuden osa-alueisiin (Leppänen 2006, 260).

Leppänen kertoo, että tietoturvallisuus voidaan jakaa kolmeen eri kategoriaan (Leppänen 2006, 260):

Tiedon käytettävyys

Tiedon käytettävyydellä voidaan mahdollistaa se, että tiedon oikealla käsittelijällä on mahdollisuus synnyttää, käsitellä, muuttaa, hyödyntää, siirtää sekä tarvittaessa mahdollisuus tuhota luomansa tieto. Leppäsen mukaan käytettävyydellä voidaan myös mahdollistaa se, että se on aina yhteydessä työn tehokkuuteen ja laatuun. Käytettävyydellä voidaan myös varmistaa se, että erilaisten tietojen käyttäjä voi hyödyntää tietojärjestelmissä ja organisaation fyysisessä muodossa olevaa tietoa kaikissa työhönsä liittyvissä olosuhteissa. Tiedon käytettävyyteen vaikuttavat organisaation käytössä olevat tietojenkäsittelyresurssit, toimintavarmuus ja tiedon laatu.

Tiedon eheys

Tiedon eheydellä voidaan määritellä se, että kuinka ehyttä tieto on. Ehyt tieto on kokonaisuudessaan saatavilla, se on muuttumatonta, sitä ei ole vääristelty tai muutoin muutettu. Tiedon eheydellä on tarkoitus varmistaa tiedon sisällön vahingoittumattomuus. On ensisijaisen tärkeää, että tiedon käsittelijä voi luottaa siihen, että hänen käsittelemänsä tieto on oikeaa eikä se edellytä tietojen käsittelijältä minkäänlaisia varmennustoimenpiteitä.

Tiedon luottamuksellisuus

Tiedon luottamuksellisuus kasvaa aina, kun tiedon sisällön merkittävyys kasvaa. On hyvä huomioida, että tiedon luottamuksellisuuteen kuuluu esimerkiksi tiedon käytön oikeutus. Tiedon luottamuksellisuus määritellään sen merkittävyyden ja tiedon mahdollisen väärinkäytöksen aiheuttamien vahinkojen perusteella. Hyvällä luottamuksellisuuden ja erilaisten suojaustoimenpiteiden avulla varmistetaan, että tiedot säilyvät vahingoittumattomina

(eheys) ja minimoidaan väärinkäytöksien mahdollisuus. Leppänen kertoo luottamuksellisuudesta seuraavasti: ”Luottamuksellisuuteen kuuluu tietojen luokittelu, käyttäjien hallinta, suojaamistoimenpiteet sekä yksityisyyden suojan varmistaminen” (Leppänen 2006, 261).

Leppäsen mukaan organisaatioissa tietoa syntyy silloin, kun se on organisaation henkilöstön käytettävissä. Syntyneen tiedon pohjana voi olla organisaation henkilöstö tai organisaation ulkopuolinen taho. On hyvä huomata, että tässä kohtaa myös määritellään tiedon omistaja – tämän tarkoituksena on määritellä se, että kuka tiedon oikeasti omistaa. Yleisesti ottaen voidaan katsoa, että henkilöstön tuottama tieto siirtyy työnantajan omistukseen, ellei toisin ole erikseen sovittu. Ulkopuolisista lähteistä saatu tieto voi saada tekijänoikeussuojan, jonka vuoksi heiltä saatuun tietoon tulee rajoitteita (Leppänen 2006, 263).

Alati digitalisoituvassa maailmassa korostuu tiedon alkuperän todentaminen, ja mitä yksittäinen tiedon soveltaja on tuonut lisää alkuperäiseen tietoon. Leppäsen mukaan tietoturvallisuuden kannalta tiedon alkuperällä on suuri merkitys esimerkiksi tutkimus- ja kehityshankkeissa. Tässä tilanteessa on hyvä määritellä mahdollisimman tarkasti jokaisen osapuolen lähtöaineisto, joka tuotetaan uuteen tietoa synnyttävään hankkeeseen (Leppänen 2006, 263–264).

3.3 Tiedon hävittäminen

Leppäsen mukaan kaikenlainen tieto on pystyttävä hävittämään niin, että sen palauttaminen alkuperäiseen, tunnistettavaan, muotoonsa ei ole mahdollista. Tiedon tai tietojen hävittämiskäytäntöjen on oltava yhteneväisiä tietoturvallisuusluokitusten ja tiedon käsittelyprosessien kanssa. Leppänen kertoo, että yksi laittomista tiedonhankinnan muodoista on roskisvakoilu. Roskisvakoilussa erilaista tietoa, joka voi olla luottamuksellista ja tärkeää, hankitaan fyysisesti roskiksista – sellaisesta paikasta, johon tiedon ei olisi alun alkaenkaan pitänyt päätyä (Leppänen 2006, 283).

Tieto tulee tuhota ja hävittää tiedon käsittelypaikalla. Tiedon hävittämisessä voidaan hyödyntää myös ulkopuolisia toimijoita, mutta silloin organisaation on varmistuttava siitä, että tuhottava tieto on vain alemman turvallisuusluokituksen saanutta tietoa. Salaiset ja erittäin salaiset tiedot on hävitettävä poikkeuksetta tiedon käsittelypaikassa.

Leppänen kertoo, että data-aineisto on hävitettävä päällekirjoituksella ja sen on oltava riittävän tehokasta. Riittävän tehokkaana päällekirjoituksena voidaan pitää sitä, jos haluttu tieto päällekirjoitetaan vähintään seitsemän kertaa. Tämä estää sen, että tietoa ei voi saada enää alkuperäisessä muodossaan takaisin. Leppänen tuo myös esille sen, että esi-

merkiksi tietokoneiden kovalevyt tulee poikkeuksetta irrottaa ja tuhota erillään muista teknisistä jätteistä. Tietoaineistoturvallisuus koostuu esimerkiksi seuraavista asioista; tietojen luokitus, käyttöoikeudet, salassapitosopimukset, tietojärjestelmissä olevien tietojen säilytysajat ja yksityisyydensuoja (Leppänen 2006, 284).

4 Inhimilliset tekijät kyberturvallisuudessa

Ray Stantonin mukaan yrityksen tietoturvallisuus on suuremman uhan alla kuin koskaan aikaisemmin. Stanton kertoo, että syy tälle on yksinkertainen – jokainen meistä on joutunut varkaiden, hakkereiden ja pahanilmanlintujen sekä valkohattuhakkereiden sissisodan keskelle, nykyaikaisen digitalisaation myötä elämämme siirtyvät enenevissä määrin verkkoon, jonka vuoksi riskit kasvavat jatkuvasti (Kearney 2016, 5).

Stantonin mukaan olisi houkuttelevaa keskittyä vain tietoturva-asiantuntijoihin, koska he ovat alansa ammattilaisia ja osaavat toimia erilaisten hyökkäysten mukaan, mutta Stantonin mukaan tämän kaltainen ajattelutapa on liian yksinkertainen. Stantonin mukaan sillä ei ole mitään merkitystä, että kuinka kovan luokan ammattilaisia tietoturvapuolella työskentelee. Stantonin mukaan nykyisin harvemmin ja harvemmin luetaan siitä, että kuinka hakkerit ovat onnistuneet murtautumaan yrityksen tietokantoihin, mutta vaakakupissa painaa se tosiasia, että uutisissa on kasvavissa määrin kertomuksia siitä, että kuinka yksittäinen työntekijä on unohtanut esimerkiksi tietokoneensa junaan tai luottamuksellisia papereita näkyville (Kearney 2016, 5).

Stantonin mukaan yrityksen investointi, kokoluokasta riippumatta, tietoturvallisuuteen menee täysin hukkaan, jos yrityksen työntekijät eivät ymmärrä tietoturvaan liittyviä riskejä, kuinka he voivat toimillaan auttaa yritystä ja sitä, että kuinka tietoturvaan liittyvät prosessit ja teknologiat todellisuudessa toimivat (Kearney 2016, 6). Procedian tutkimus tukee Kearneyn näyttöä. Heidän tutkimuksensa mukaan inhimilliset tekijät ovat suurin yksittäinen tekijä yrityksen tietoturvaan (Metalidou ym. 2014).

Kearney itse kertoo, että yrityksen työntekijöitä kritisoidaan ja jopa syytetään tietovuodoista heidän toimistaan johtuen. Työntekijät saattavat kirjoittaa salasanojaan muistilapuille, unohtaa tietokoneensa julkiselle paikalle tai keskustella sellaisista asioista julkisesti, joista ei olisi suotavaa keskustella julkisesti. Tämän vuoksi monelle tulee mieleen kysymys siitä, että miksi työntekijät eivät yksinkertaisesti vain voi totella annettuja ohjeita tai tietoturvapolitiikkaa? Kearneyn mukaan tämänkaltainen ajattelumalli on liian yksinkertainen, vaikka hän myöntää, että ihmiset aiheuttavat ongelmia tietoturvaan liittyen. Kearney kuitenkin painottaa sitä, että useimmiten työntekijä on yrittänyt parhaansa mukaan toimia tietoturvallisesti, mutta hänen saamansa tietoturvakoulutus on ollut puutteellista tai yksinkertaisesti työntekijä ei ole ymmärtänyt tekojensa seuraamuksia (Kearney 2016, 7).

Kearneyn mukaan yrityksen tietoturvaan liittyy todellisuudessa kolme asiaa: ihmiset, prosessit ja teknologiat. Yrityksen ohjelmistojen ja tietojen turvassa pitämiseksi yrityksen tulisi

huomioida kaikki kolme asiaa toiminnassaan, Kearney painottaa, että yrityksen ei tulisi huomioida näitä komponentteja yksittäisinä asioina, vaan toisiaan tukevina komponentteina (Kearney 2016, 7).

Kearney kertoo kirjassaan, että aikaisemmin yrityksessä työskentelevät ihmiset ottivat tapaamisiin mukaansa vain tarvittavat tiedot. Nykyisin tapaamisiin tuodaan paljon tietoa; Kearney näkee, että tämä on ongelma. Digitalisaation myötä on lähes mahdotonta, että unohtaisit tärkeät dokumentit tapaamisesta, mutta toisaalta tämä itsessään voi olla myös äärimmäisen suuri riski. Kearney tuo kirjassaan esille esimerkin siitä, kun Kuninkaallisen laivaston rekrytoija Iso-Britanniassa unohti vuonna 2008 tietokoneensa autoonsa. Tämä kyseinen tietokone sisälsi yli 600 000 Iso-Britannian armeijaan liittyneen, tai liittymisestä kiinnostuneiden, henkilökohtaiset tiedot. Kearneyn mukaan samassa hyökkäyksessä selvisi myös kyseisten sotilaiden osoitteet ja pankkitiedot. Kearney kertoo, että tämä on arkipäivää ja tämä tulee yrityksille kalliiksi – Ponemon Instituten teettämän tutkimuksen mukaan yritykselle tulee keskimäärin 204 dollarin lasku jokaisesta kadonneesta henkilötiedosta (Kearney 2016, 15–16).

Kearney tuo kirjassaan myös ilmi, että ihmiset saattavat myös paljastaa salattuja tietoja vahingossa. Kearney tuo ilmi tapauksen, jossa Iso-Britanniassa työskennellyt anti-terrorismiyksikössä työskennellyt poliisi kantoi julkisesti asiakirjaa, jonka sisällöstä kävi ilmi terroristisolu Manchesterissä, joka oli tarkoitus tuhota poliisin toimesta. Valitettavasti sivullisiin lukeutui paparazzi, joka sai kamerallaan kuvan asiakirjasta ja vaikka kuvan julkaisu yritettiin estää, oli se liian myöhäistä. Kearney pitää tätä vain yhtenä esimerkkinä isosta ongelmasta. Kearney tuo esille huolensa siitä, että ihmiset käyvät julkisesti keskusteluita luottamuksellisista asioista tai lukevat luottamuksellisia asiakirjoja julkisesti (Kearney 2016, 19–20).

Kearney tuo esille myös sen, että ihmiset eivät ole yhtä luotettavia kuin tietokoneet, jotka kykenevät tekemään niille osoitetut tehtävät lähes poikkeuksetta oikein. Kearney kertoo, että ihmiset saattavat tehdä asiat väärin, jos he eivät ole esimerkiksi ymmärtäneet saamiaan ohjeitaan ja yrittävät täten soveltaa itse ”sinne päin”. Yhtenä ongelmana Kearney nostaa esille sen, että työntekijä voi päästää kollegansa omilla tunnuksillaan sisäverkkoon ajan säästämisen vuoksi (Kearney 2016, 22).

Kearney kertoo yhdeksi ongelmakohdaksi myös sen, että jos esimerkiksi palkka määräytyy työtuloksen myötä, niin työntekijät löytävät yleensä keinoja, joilla tietoturva voidaan joko kiertää tai jättää tietyissä kohdissa huomiotta, jos ne hidastavat yksilön työntekoa. Tämä voi valitettavasti myös johtaa siihen, että työntekijät näkevät tietoturvan enemmän

uhkana, kuin hyötynä. Kearney nostaa esille myös sen, että mikäli tietoturvaohjelmistot ovat vaikeakäyttöisiä saattaa se myös johtaa ajattelutapaan, jossa tietoturvaa pidetään enemmän vihollisena, kuin hyötynä. Tämän lisäksi ongelmia saattaa syntyä silloin, kun tietoturva-asiat viedään sille tasolle, että ohjeita pitää seurata tarkalleen tietyn kehyksen mukaan ilman varsinaista selitystä sille, että miksi niin riski sille, että työntekijä unohtaa jonkin askeleen tällä kehyksellä kasvaa. Ihminen saattaa tällöin tehdä omatoimisesti myös johtopäätelmän siitä, että tietyt kohdat tässä kehyksessä eivät ole tärkeitä (Kearney 2016, 23). Samalla linjalla Kearneyn kanssa on myös Procedian tutkimus vuodelta 2014, jossa kävi ilmi, että kehittyneestä tietoturvallisuusteknologiasta huolimatta ongelma piilee usein juuri käyttäjissä itsessään. Nämä käyttäjät saattavat omilla toimillaan (he saattavat olla varomattomia tai eivät yksinkertaisesti ymmärrä tietyn toimen aiheuttamaa uhkaa) mahdollistaa tietoturvariskin (Metalidou ym, 2014).

Kearney tuo kirjassaan esille myös salasanat ja niihin liittyvät ongelmat. Toistaiseksi yritykset käyttävät vielä paljon käyttäjänimiä ja salasanoja määrittääkseen sen, että kenellä on oikeus päästä yrityksen verkkoon ja kenellä ei, vaikka uudet teknologiat, kuten erilaiset kortit, ovat nostamassa suosiotaan. Kearneyn mukaan tässä piilee myös yksi ongelmakohta: salasanan tulisi olla sellainen, joka on vain käyttäjän itsensä tiedossa, mutta ihmiset valitsevat todella usein sellaisen salasanan, joka on äärimmäisen helppo muistaa ulkoa. Tämä itsessään auttaa myös täysin ulkopuolista henkilöä vain arvaamaan salasanan oikein. Kearney tuo esille New York Timesin teettämän tutkimuksen erään tietovuodon seurauksena, jossa selvisi, että yleisin salasana kyseiseen palveluun oli ”123456”. Tämän lisäksi palvelussa oli käytetty paljon salasanoina esimerkiksi ”abc123” ja ”password” (Kearney 2016, 25–26).

Kearney kertoo, että ihmiset myös usein valitsevat salasanoikseen sellaisia asioita, jotka liittyvät tavalla tai toisella heidän elämäänsä. Nämä voivat olla esimerkiksi puolison nimi tai lemmikkien nimet – ongelmaksi kehkeytyy kuitenkin se, että nämä samat ihmiset saattavat kertoa näitä tietoja suoraan esimerkiksi julkisella sosiaalisen median tilillään, jolloin potentiaalinen pahanilmanlintu pääsee arvaamaan salasanaasi hetkessä. Kearney nostaa esille myös huolen siitä, että ihmiset käyttävät samoja salasanoja useissa eri palveluissa, ellei kaikissa, joissa he ovat rekisteröityinä. Tämä voi johtaa suoraan siihen, että yksi heikompi lenkki laajassa palveluiden kirjossa voi saattaa kaikkien muiden palveluiden käyttäjätunnukset, ja täten kaiken tiedon sen takana, vaaraan (Kearney 2016, 26).

Minkälainen on sitten hyvä salasana? Kearney kertoo, että hyvässä salasanassa tulisi olla vähintään erikoismerkkejä, numeroita, isoja ja pieniä kirjaimia ja sen tulisi ylittää yrityksen asettama minimipituus. Kearney kertoo, että hyvä salasana on yhdistelmä satunnaisuutta,

monimutkaisuutta ja pituutta. Kearney muistuttaa, että salasanaa ei tulisi kirjoittaa paperille ylös, ellei tätä kyseistä paperilappua pidä mukanaan esimerkiksi lompakossa, jolloin sen katoaminen huomataan nopeasti (Kearney 2016, 26–27).

Viimeisenä uhkanaan Kearney tuo kirjassaan esille sen, että ihmiset ovat usein avuliaita ja luottavaisia. On luontevaa, että me ihmisinä luotamme ja yritämme avustaa parhaamme mukaan esimerkiksi kollegoita tai asiakkaita. Meille on usein opetettu jo lapsesta pitäen hyviä käytöstapoja, jolloin nämä voivat myös kostautua. Kearney tuo esimerkkinä ilmi skenaarion, jossa työntekijä pitää yrityksen ovea auki kiireellisen näköiselle, hyvin pukeutuneelle henkilölle, jonka kulkukorttia ei näy. Moni saattaa ajatella, että tämä kulkukortti on paidan alla piilossa tai taskussa ja kiireiden vuoksi tämä henkilö ei ehdi sitä sinulle näyttää. Todellisuudessa tämä kiireessä oleva, hyvin pukeutunut henkilö, voi olla esimerkiksi yritysvakoilija (Kearney 2016, 30).

Kearney tuo esille myös tietojenkalastelun ja sen, että kuinka nämä kalasteluhuijaukset ovat nykyisin parempia ja aidomman näköisiä, kuin ennen. Nykyisin kalasteluyritykset saatetaan suunnata yhteen yritykseen ja ne saattavat sisältää esimerkiksi yleistä yritysjargonia tai johtotason henkilöiden nimiä ja jopa yhteystietoja. Nykyisin kalasteluyritykset saatetaan osoittaa myös suoraan yrityksen johdolle, jolloin ne Kearneyn mukaan saatetaan naamioida esimerkiksi veroilmoituksiksi. Tästä syntyneen paniikin johdosta yrityksen johtohahmot saattavat painaa kalasteluviesteissä olevaa linkkiä, ja tietämättään asensivat juuri näppäilytallennin-viruksen tietokoneelleen. Tämä näppäilytallennin puolestaan rekisteröi jokaisen näppäimistön painalluksen, sisältäen kaiken tarpeellisen tiedon, jonka pahanilmanlintu tarvitsee (Kearney 2016, 33).

Procedian tutkimus tukee Kearneyn väitettä siitä, että erilaiset kalasteluyritykset ovat varteenotettavia uhkia. Procedian mukaan eräässä tutkimuksessa käytettiin huonosti tehtyä kalasteluviestiä, jonka tarkoituksena oli olla mahdollisimman epäluotettava ja näyttää selkeältä kalasteluviestiltä. Tästä huolimatta jopa 37 prosenttia työntekijöistä avasi kalasteluviestin ja painoi sen mukana tullutta linkkiä. Näistä ihmisistä jopa 13 prosenttia päätyi myös avaamaan linkin takaa löytyneen tiedoston. Procedian tutkimuksessa laadittiin myös toinen osa, jossa kalasteluviesti naamioitiin näyttämään aidommalta, jolloin 42 prosenttia työntekijöistä avasi sähköpostin, seurasi siinä ollutta linkkiä ja täytti sen takana sijainneeseen lomakkeeseen henkilökohtaisia tietojaan. Toisessa tutkimuksessa huomattiin myös se, että 30 prosenttia työntekijöistä latasivat tämän linkin takaa tietokoneilleen tiedoston, jonka olisi ollut määrä parantaa tietokoneen suorituskykyä (Metalidou ym, 2014).

Viimeisenä asiana Kearney tuo esille sen, että mitä ihmiset ovat valmiita tekemään ilmaisten asioiden eteen. Liverpoolissa Englannissa järjestettiin useita vuosia eräänlainen koe, jossa erilaisissa työtehtävissä työskentelevät toimistotyöntekijät saivat yhden suklaapatukan, jos he osallistuivat kyselyyn. Kyselyssä kysyttiin erilaisia henkilökohtaisia asioita sekä heidän salasanaansa. Monien yllätykseksi moni suostui kyselyyn vastaamaan. Kokeen jälkeen ihmisten antamia salasanoja ei toisaalta testattu, joten on myös mahdollista, että ihmiset ovat antaneet salasanansa kohdalla vääriä vastauksia. Kearney tuo myös esille toisen kokeen, jossa USB-muistitikkuja jätettiin tahallaan yrityksen tiloihin. Nämä USB-muistitikut sisälsivät yksinkertaisen ohjelman, joka lähetti kokeen tekijöille vain ilmoituksen siitä, jos muistitikku liitettiin tietokoneeseen. Jälleen kerran kokeesta pystyttiin päättelemään, että ihmiset unohtivat turvallisuusprotokollat, kun tarjolla oli jotain ilmaista (Kearney 2016, 34).

4.1 Inhimillisten tekijöiden huomiointi kyberturvallisuudessa ja sen luomien riskien minimointi

David Lacey nostaa kirjassaan esille sen, että organisaation johdon on hyvä osata ottaa vastuu siitä, että riskienhallinta ja sen dokumentointi tehdään riittävän laajasti, koska muutoin on vaarana, että riskienhallintaa ja sen dokumentointia ei oteta riittävän tosissaan. Lacey kertoo, että huonosti toteutettu ”rasti ruutuun” protokolla johtaa helposti siihen, että näitä asioita ei johtoporras tai työntekijät ota kovin helposti tosissaan. Lacey myös kannustaa siihen, että organisaation johtoportaan tulee osata ajatella jopa sellaisia skenaarioita, joiden he eivät usko koskaan tapahtuvan. Laceyn mukaan tämä on yksi suuri askel sille, että yritys itsessään voi menestyä ja täten myös varautua tietynlaisiin riskeihin etukäteen, koska niistä mahdollisesti koituvat haitat on osattu ottaa huomioon jo etukäteen (Lacey 2009, 35–36).

Lacey nostaa kirjassaan myös esille päällikkötason työtehtävissä työskentelevät ihmiset. Heillä on Laceyn mukaan usein kiire ja he saattavat olla usein tekemisissä lyhytaikaisissa projekteissa, joissa aika ja raha on äärimmäisen tärkeitä tekijöitä. Lacey kertoo, että vaikka tämän tason työtehtävissä työskentelevät ihmiset ovat usein vastuussa riskienhallinnassa, niin juuri kiire ja tarkat aikarajat saavat heidät usein unohtamaan tietoturvallisuuden, koska se vie usein aikaa ja täten myös rahaa. Lacey nostaa esille myös sen, että usein ihmiset eivät ajattele tietoturvallisuuden olevan kovin tärkeää, koska se ei suoraan kosketa heitä – mikäli heille kuitenkin kerrottaisiin, että tietyn tietoturvallisuuden osan huomioimatta jättäminen veisi heidät vankilaan, niin tämä ihminen tekisi kaikkensa, että tämä asia huomioitaisiin (Lacey 2009, 38).

Lacey kertoo, että jokaiselta organisaation työntekijältä löytyy aina joitain henkilökohtaisia asioita, joihin tietoturvallisuutta voidaan verrata. Nämä henkilökohtaiset asiat voivat johtaa siihen, että organisaation sisällä ohjelmistoissa esiintyviä virheitä korjataan ennen kuin ulkopuolinen henkilö voi niitä hyödyntää (Lacey 2009, 38).

Laceyn mukaan organisaation työntekijöiden ymmärrys ja tietoisuus tietoturvauhista on ensisijaisen tärkeä askel siihen suuntaan, että tietoturvapolitiikasta tulee toimiva. Toisaalta on hyvä huomioida, että työntekijät ja muut sidosryhmät eivät tule koskaan täysin ymmärtämään esimerkiksi uhkia, riskejä tai tietoturvapolitiikkaa, koska ne ovat usein liian vaikeaselkoisia. Laceyn mukaan myös ihmisten asenteet ovat todella erilaisia – toinen ihminen saattaa olla uraputkessa oleva riskinottaja, kun toinen samassa organisaatiossa työskentelevä voi olla seesteinen ihminen, joka ottaa kaikki ohjeistukset kirjaimellisesti vastaan ja toimii niiden mukaan. Lacey kertookin, että on ensisijaisen tärkeää hyväksyä se, että organisaatiossa on aina paljon parannettavaa, mutta organisaatio itsessään ei voi muuttaa kaikkea kerralla. Tämän vuoksi on tärkeää, että organisaatio tähtää siihen, että vain tiettyjä osa-alueita organisaation sisällä pyritään parantamaan kerralla – hyvä tietoturvaohjelma tai sen uudistus tähtää siihen, että se osa-alue, jossa eniten apua tarvitaan, laitetaan ensimmäisenä kuntoon (Lacey 2009, 211).

Lacey kertoo, että on tärkeää tehdä selkeät erot sille, että mitä asioita pitää muuttaa organisaation työntekijöiden tietotaitoon, asenteisiin ja todelliseen käyttäytymiseen työskentely ympäristössä. Tietotaidon ja ymmärtäväisyyteen puuttuminen on Laceyn mukaan helpohko asia, joskin se vaatii organisaatiolta tarkkaa suunnittelua ja harkintaa. On tärkeää, että muutos tapahtuu niin, että organisaatio osaa antaa oikeanlaista tietoa tietyille ihmisille sopivassa muodossa. Nämä muodot voivat olla esimerkiksi sähköpostiviestejä, uutiskirjeitä tai esimerkiksi julisteita, joissa tarpeellinen tieto tuodaan esille (Lacey 2009, 212).

Laceyn mukaan organisaation työntekijöiden asenteiden muuttaminen on huomattavasti vaikeampaa. Tähän prosessiin liittyy usein erilaisia henkilökohtaisia kokemuksia, joita voi olla vaikea saavuttaa. Organisaation työntekijät saattavat olla myös muutosvastarintaisia, jolloin on tärkeää, että asennemuutoksessa otetaan hillitympi linja. Organisaatio voi esimerkiksi tuoda ongelman hiljalleen esille ja täten kannustaa ihmisiä, hiljalleen, muuttamaan asenteitaan tietoturvaa kohtaan (Lacey 2009, 212).

5 Tutkimus aineiston perusteella

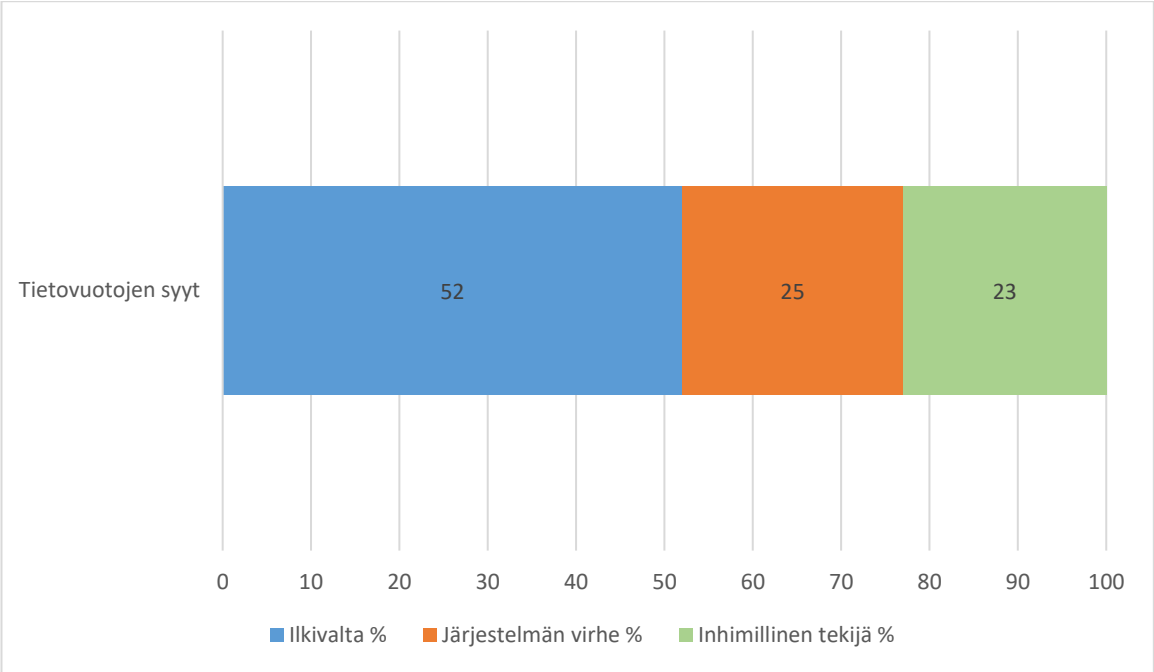
Kappale käsittelee tietoturvaloukkauksia ja tietomurtoja sekä globaalilla että Suomen tasolla. Ajankohtaisen näkökulman opinnäytetyölle antaa IBM Securityn teettämä tutkimus, koska siinä huomioitiin myös COVID-19 tilanne ja sen tuomat mahdolliset haasteet yrityksille. Suomen tasolla tutkimuksessa on hyödynnetty Kyberturvallisuuskeskuksen julkaisemaa vuosiraporttia sekä Kyberturvallisuuskeskuksen kuukausittain julkaisemaa kybersääpalvelua, joka antaa kuukausittaisen ”kybersään” valtakunnallisesti. Kybersää muun muassa listaa kuukausittain suurimmat yksittäiset uhat tietoturvan kannalta.

5.1 IBM Securityn teettämä Globaali tutkimus

IBM Securityn teettämässä tutkimuksessa tutkittiin 524 organisaatiota, jotka olivat joutuneet tietomurron kohteeksi. Kyseiset organisaatiot olivat 17 eri maasta ja tutkimus kattoi 17 erilaista toimialaa. Tutkimuksessa haastateltiin myös yli 3200 henkilöä, jotka olivat tietoisia siitä, että heidän organisaationsa oli joutunut tietomurron kohteeksi. Haastatteluissa kysyttiin lukuisia kysymyksiä, joiden perusteella oli määrä saada tietoa siitä, että miten organisaatiot reagoivat tietomurtoihin. Haastatteluiden pohjalta haluttiin myös tietää se, että kuinka pitkään kesti, että organisaatio huomasi tietovuodon ja kuinka nopeasti tietovuodon aiheuttamat ongelmat saatiin korjattua sekä se, että kuinka tietovuoto on vaikuttanut organisaation asiakkaisiin ja täten yrityksen tuloihin/kustannuksiin (IBM Security 2020, 3–4).

IBM:n tutkimus teetettiin hieman ennen COVID-19 pandemiaa, mutta IBM on ottanut tämän huomioon tutkimuksessaan ennen sen julkaisua. IBM:n haastatteluiden perusteella jopa 76 prosenttia organisaatioista on huolissaan siitä, että lisääntyneiden etätöiden vuoksi mahdolliset tietovuodot on vaikeampi huomata tai toimia niiden ehkäisemiseksi (IBM Security 2020, 5).

IBM Securityn tutkimuksen mukaan yleisin syy tietovuodoille ja -murroille oli tarkoituksella tehdyt ilkivallalliset teot kuten kuva 1 kertoo. Nämä kattoivat hieman yli 50 prosenttia kaikista tietovuodoista tai -murroista. Toiseksi yleisin syy tietovuodoille tai -murroille oli järjestelmistä löytyvät virheet, jotka kattoivat noin 25 prosenttia kaikista tietovuodoista tai -murroista ja kolmanneksi yleisimmäksi syyksi IBM:n tutkimuksessa nousi esille ihmisten tekemät virheet. IBM Securityn arvion mukaan inhimillisistä tekijöistä johtuneiden tietovuotojen tai -murtojen keskiarvo kustannus organisaatiolle oli vuonna 2020 3.3 miljoonaa USA:n dollaria. (IBM Security 2020, 30–31).



Kuva 1. Tietovuotojen syyt (mukaillen IBM Security 2020, 30)

IBM Securityn teettämässä tutkimuksessa ilkivallassa huomioitiin myös sellaiset asiat, jotka voidaan esimerkiksi Kearneyn teorian mukaan laskea myös inhimillisiksi tekijöiksi. Tutkimuksen mukaan tähän reiluun 50 prosenttiin sisältyi myös erilaisten tietojen kalastelu (14 %), järjestelmän käyttäjien manipulointi (3 %) ja esimerkiksi pilvipalveluiden ja muiden järjestelmien vääränlainen konfiguraatio (25 %), jotka johtivat tietovuotoihin tai -murtoihin (IBM Security 2020, 36).

IBM Securityn teettämän tutkimuksen mukaan inhimillisistä tekijöistä johtuvien tietovuotojen ja -murtojen tunnistamiseen meni keskimäärin 182 vuorokautta, jonka lisäksi kesti vielä 57 vuorokautta siihen, että tietovuoto tai -murto saatiin aisoihin. Keskimäärin siis tietovuodon tai -murron huomaaminen ja sen hoito kesti 239 vuorokautta (IBM Security 2020, 55).

IBM Security teetti tutkimukseensa ensimmäistä kertaa osion, jossa tutkittiin myös täysin tai osittain automatisoituja turvallisuusohjelmistoja ja niiden vaikutusta tietovuotojen tai -murtojen huomaamiseen. Täysin automatisoitu järjestelmä kykeni huomaamaan tietovuodot tai -murrot keskimäärin 175 vuorokaudessa ja korjaamaan sen 59 päivässä, jolloin vuodosta oli kulunut kaikkinensa 234 vuorokautta. Osittain automatisoitu järjestelmä kykeni huomaamaan saman asian 202 vuorokaudessa ja korjaamaan sen 73 päivässä, jolloin vuodosta oli kulunut kaikkinensa 275 vuorokautta. Täysin manuaalinen järjestelmä pärjäsi vertailussa huonointen; vuoto huomattiin keskimäärin 228 vuorokaudessa ja sen korjaamiseen meni 80 päivää, jolloin aikaa oli kulunut jo 308 vuorokautta (IBM Security 2020, 56).

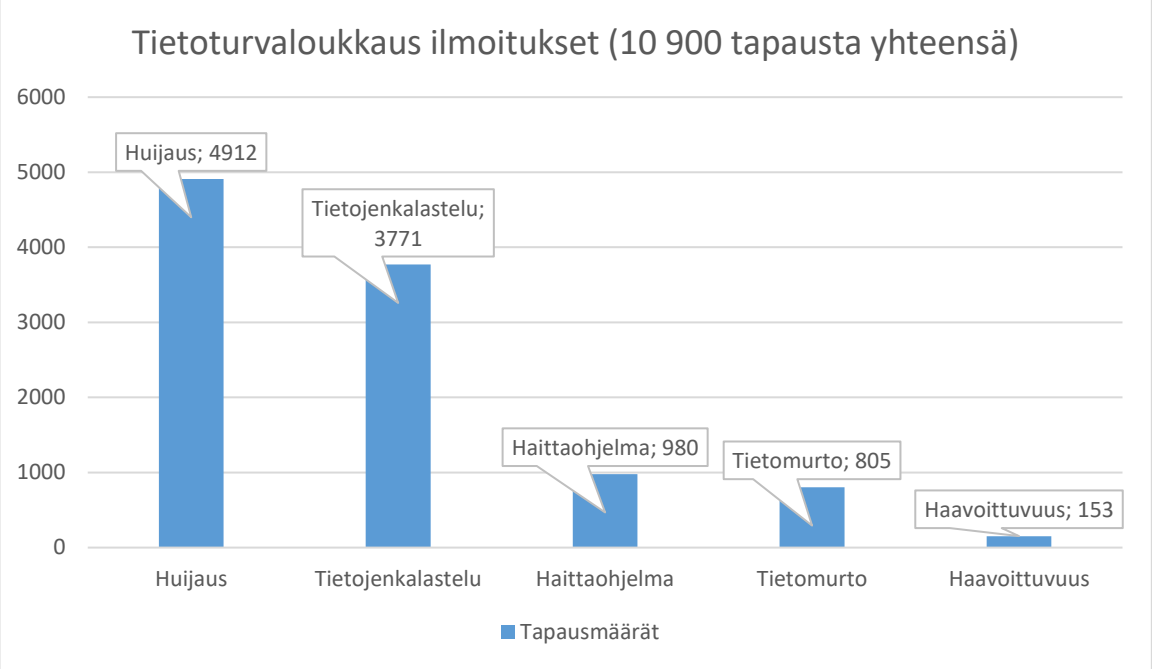
5.2 Tilanne Suomessa

Suomessa Kyberturvallisuuskeskus on arvioinut viisi merkittävintä pidemmän aikavälin uhkaa, joista Kyberturvallisuuskeskus nostaa suurimmaksi huolenaiheeksi tietojenkalastelun ja niiden yritykset. Muita merkittäviä pidemmän aikavälin uhkakuvia ovat kyberhyökkäysmenetelmien käyttö kiristämiseen, haavoittuvuuksien hyväksikäyttö, heikko kyberriskien hallinta ja palveluidenhallinnan epäselvä vastuunjako sekä lokitietojen puutteellisuus (Kyberturvallisuuskeskus 2021a, 5–10).

Kyberturvallisuuskeskuksen mukaan vuoden 2020 neljännen kvartaalin yleisin uhka oli tietojenkalastelut, jotka olivat tavallisin tapa päästä yrityksen verkkoon. Tietojenkalastelussa ulkopuolinen tekijä yrittää saada organisaation työntekijöiden käyttäjätunnuksia ja salasanoja tietoonsa, jotta hän pääsee yrityksen järjestelmiin käsiksi (Kyberturvallisuuskeskus 2021a, 19).

Kyberturvallisuuskeskuksen vuosittaisessa raportissa nousee esille se, että erilaisissa verkkoon kytketyissä älylaitteissa on tuntuvasti tietoturvapuutteita. Kyberturvallisuuskeskuksen tutkimuksessa löydettiin noin 500 000 suojaamatonta tulostinta, joista tutkimuksessa 50 000 otettiin tarkempaan analyysiin. Kyberturvallisuuskeskus kykeni ottamaan näistä laitteista noin puolet haltuunsa. Kyberturvallisuuskeskus löysi samassa tutkimuksessa 1000 suojaamatonta automaatiojärjestelmää. Kyberturvallisuuskeskus korostaa sitä, että mitä enemmän suojaamattomia laitteita yrityksen verkkoon tuodaan, niin sitä enemmän verkon käytettävyys ja ennen kaikkea sen tietoturva kärsii. Kaapatun laitteen voi Kyberturvallisuuskeskuksen mukaan myös valjastaa niin, että sen kautta voidaan päästä helposti yrityksen verkkoon tai sen kautta tunkeutuja voi löytää helpon pääsyn yrityksen verkkoon (Kyberturvallisuuskeskus 2021b, 15).

Kyberturvallisuuskeskuksen mukaan heidän tilannekeskukseensa tulleiden yhteydenottojen määrä kasvoi vuodesta 2019 vuoteen 2020 yli 100 prosenttia. Vuonna 2019 yhteydenottoja oli noin 4500, kun viime vuonna yhteydenottoja oli yli 10 900, kuten kuva 2 kertoo. Näistä valtaosa, 79 prosenttia, koski joko huijausta tai tietojenkalastelua (Kyberturvallisuuskeskus 2021b, 17).



Kuva 2. Tietoturvaloukkausten ilmoitukset (mukaillen Kyberturvallisuuskeskus 2021b, 17)

Kyberturvallisuuskeskuksen mukaan heidän tilannekeskukseensa ilmoitetaan viikoittain erilaisista haavoittuvuustapauksista, joista valtaosa on melko yksinkertaisia ja ne liittyvät usein nettipalveluihin tai IoT-laitteisiin. Nettipalveluihin liittyvät ongelmat olivat lähes poikkeuksetta erilaisia toteutusvirheitä joko yksittäisissä palveluissa tai näiden taustajärjestelmissä. Kyberturvallisuuskeskuksen mukaan tämän kaltaisissa tapauksissa organisaatio voi itse korjata havaitun haavoittuvuuden, jonka vuoksi näistä ei päässyt aiheutumaan merkittävää vahinkoa. IoT-laitteisiin liittyvissä haavoittuvuuksissa oli useimmiten kyse alkeellisista toteutustason virheistä tai laitteet oli jätetty oletusasetuksilleen. Kyberturvallisuuskeskuksen mukaan näissä tapauksissa hyökkääjä voisi kyseiset laitteet saada haltuunsa melko helposti. Kyberturvallisuuskeskus linjaa, että tämän kaltaisissa haavoittuvuuksissa korjaamisprosessit ovat usein hankalia sekä hitaita (Kyberturvallisuuskeskus 2021b, 18).

Kyberturvallisuuskeskuksen mukaan vuonna 2020 vakavimmat haavoittuvuudet liittyivät sellaisiin tapauksiin, joissa löydettiin uusia haavoittuvuuksia erilaisista palveluista, jotka olivat avoimina verkkoon. Kyberturvallisuuskeskuksen mukaan tämän kaltaisten palveluiden lukumäärä ei näytä vähentyvän vuoden takaiseen verrattuna mitenkään (Kyberturvallisuuskeskus 2021b, 18).

Kyberturvallisuuskeskus nostaa vuosittaisessa raportissaan kymmenen uhkakuvaa vuodelle 2021, joista muutama liittyy suoraan aiheeseen. Näistä suurimmaksi uhaksi Kyberturvallisuuskeskus nostaa vision siitä, että ”myös vuonna 2021 tapahtuu jotakin ikävää”.

Kyberturvallisuuskeskuksen mukaan monet organisaatiot eivät pysy digitalisaation vauhdissa, jolloin riskienhallinta kärsii. Heidän mukaansa organisaatiot ottavat käyttöönsä erilaisia uusia ratkaisuja niin, että niiden aiheuttamia riskejä ei ymmärretä tai arvioida. Tämä voi Kyberturvallisuuskeskuksen mukaan johtaa siihen, että hätiköidystä ratkaisusta kärsii niin kansalainen, organisaatio kuin pahimmassa tapauksessa koko yhteiskunta (Kyberturvallisuuskeskus 2021b, 36).

Kyberturvallisuuskeskus nostaa raportissaan myös esille huolen siitä, että COVID-19 pandemian aiheuttama äkillinen etätyöaalto on aiheuttanut sen, että osa organisaatioista on rakentanut nykyiset, etätyöskentelyn mahdollistavat, järjestelmänsä heikosti tai monimutkaisesti ja niiden korjaamiseen menee Kyberturvallisuuskeskuksen mukaan aikaa. Tämän lisäksi Kyberturvallisuuskeskus nostaa esille huolenaiheensa siitä, että tietoturvaosaamisen saaminen riittävän hyvälle tasolle voi kestää pitkään. Alati digitalisoituvassa maailmassa tietoturvaosaajien määrä kasvaa, mutta osaaminen ei ole silti vielä riittävällä tasolla. Toisaalta Kyberturvallisuuskeskuksen raportissa käy myös ilmi, että tietoturvaosaajien tarve on nyt tunnistettu ja koulutusten määrää ja kehittämistä on nyt edistetty (Kyberturvallisuuskeskus 2021b, 36–37).

5.3 Inhimilliset tekijät kyberturvallisuudessa, Kaspersky ja B2B International

Kaspersky Labin ja B2B Internationalin teettämässä tutkimuksessa 52 prosenttia kaikista tutkimukseen osallistuneista (5000 yritystä) yrityksistä myönsi, että työntekijät ovat suurin riski yrityksen tietoturvaan. Työntekijöiden ajattelemattomuus asettaa yrityksen tietoturvastrategian suuren riskin alle. Tutkimuksen mukaan yritysten johtoa huolettaa eniten aran datan siirto mobiililaitteiden välillä, muita merkittäviä huolenaiheita tietoturvaan liittyen on esimerkiksi laitteiden katoaminen työntekijän toimesta sekä yrityksen sidosryhmiin kohdistuvat virheet, esimerkiksi sellaisiin sidosryhmiin, joiden kanssa organisaatio jakaa erilaista tietoa organisaatioon liittyen (Kaspersky Lab & B2B International 2017).

Kaspersky Labin vuoden 2017 tutkimuksessa huomattiin myös, että mitä pienemmästä yrityksestä on kyse, niin sitä suurempana riskinä yrityksen johto piti inhimillisistä virheistä johtuvia tietoturvaongelmia. Tutkimuksessa huomattiin myös, että yrityksen työntekijät saattavat tehdä virheitä huolimattomuuttaan tai sen takia, että työntekijöillä ei ole ollut riittävää koulutusta tietoturvaan liittyvissä asioissa. Tutkimuksessa kiinnitettiin myös huomioita siihen, että tietotaidottomat työntekijät ovat yritykselle toisiksi suurin riski tietomurrolle, ollen oleellisena tekijänä jopa 46 prosentissa kaikista tietomurroista ja jopa 11 prosenttia vakavimmista tietovuodoista johtui juuri työntekijöiden inhimillisistä virheistä.

Tutkimuksessa kävi myös ilmi, että jopa 49 prosenttia tutkimukseen osallistuneista yrityksistä olivat joutuneet erilaisten hyökkäysten kohteeksi. Valtaosassa tapauksissa kyse oli erilaisista viruksista ja haittaohjelmista. Tutkimuksen mukaan kasvua edeltävään vuoteen (2016) oli jopa 11 prosenttia. Samassa kyselyssä tuli myös ilmi, että ne yritykset, jotka olivat joutuneet hyökkäyksen kohteeksi, yli puolet (53 prosenttia) kokivat, että välinpitämättömät ja tietämättömät työntekijät olivat suurin osatekijä näille ongelmille. Reilu kolmasosa (36 prosenttia) pitivät kalastelua ja käyttäjien manipulointia suurimpana osatekijänä sille, että he ovat joutuneet hyökkäyksen kohteeksi.

Kasperskyn tutkimuksen mukaan on ensisijaisen tärkeää, että yrityksen työntekijät ovat tarkkoja ja rehellisiä hyökkäyksen sattuessa ja on tärkeää, että työntekijät yrittävät tehdä kaikkensa pienentääkseen hyökkäyksestä seuraavia riskejä. Jokaisella työntekijällä on äärimmäisen tärkeä rooli siinä, että he myös suojelevat työnantajaansa ja heidän tietojaan. On myös tärkeää, että työntekijä on vilpittömän rehellinen mahdollisen tietovuodon tapahtuessa, eikä työntekijä yritä peitellä jälkiään. Rehellisyydellä voidaan ehkäistä mahdollisia suurempia haittoja.

Kasperskyn tutkimuksessa tuli myös esille huolestuttavia asioita. Heidän mukaansa jopa 40 prosentissa tapauksissa, joissa yritys on joutunut tietovuodon uhriksi, työntekijät eivät ole ottaneet lainkaan vastuuta mahdollisista tietovuodoista. Tutkimuksen mukaan työntekijät ovat näissä tapauksissa yrittäneet peitellä jälkiään tietovuodon sattumisen jälkeen.

Työntekijän toteuttamalla tietovuodon peittämisellä voi Kasperskyn tutkimuksen mukaan olla äärimmäisen huonoja vaikutuksia ja todellisuudessa myös pahentaa tietovuodon aiheuttamia vahinkoja. Kasperskyn tutkimuksessa kerrottiin tapauksesta, jossa yksi ilmoittamaton tietovuoto johti siihen, että vuodosta tuli huomattavasti laajempi, koska hakkeri pääsi lopulta koko organisaation infrastruktuuriin, johtaen suurempiin vahinkoihin. Kaspersky oli saanut tutkimuksessa tiedon kyseisestä tapauksesta konsulttiyrityksen työntekijältä, mutta valitettavasti tarkempaa tietoa kyseisestä yrityksestä ei tutkimuksessa annettu.

Tutkimuksessa tuli myös ilmi se, että tietovuotojen peittäminen on huomattavasti suurempi ongelma suuremmissa, yli 1000 työntekijän, yrityksissä kuin pienemmissä yrityksissä. Tutkimuksen mukaan jopa 45 prosentilla suuremmista yrityksistä oli jonkin lainen kokemus siitä, että työntekijät ovat peitelleet tietovuotoja/tietovuotouhkia, kun vastaava luku alle 49 työntekijän yrityksistä oli 29 prosenttia.

Kasperskyn mukaan reaaliaikainen tietovuodon havaitseminen on tärkeimpiä asioita sille, että vuotoa päästään tutkimaan oikein ja jotta siitä voidaan tehdä riittävän hyvä analyysi.

Kasperskyn mukaan sokea luottamus siihen, että työntekijä raportoi tapahtuneen vuodon ei ole riittävä. Kasperskyn mukaan onkin tärkeää, että yritykset hyödyntävät sellaisia ratkaisuja ja teknologioita, jotka auttavat yrityksiä tunnistamaan automaattisesti mahdolliset tietovuodot tai tietoturvauhat. Näiden järjestelmien käyttö ehkäisee virheitä ja työntekijöiden välinpitämättömyyttä, koska tutkimus myös osoitti sen, että inhimilliset virheet ja jatkuvasti kehittyvät hyökkäykset ovat yrityksille suuri riski.

Kasperskyn tutkimus osoitti, että tietotekniset tietoturvapolitiikat eivät ole itsessään riittäviä, koska ne eivät koskaan ota huomioon työntekijöitä ja sitä, että kaikki työntekijät eivät välttämättä näitä tietoturvapolitiikkoja seuraa ja myös siksi, että nämä politiikat eivät koskaan kata kaikkia mahdollisia tietoturvariskejä.

Tutkimuksessa kävi ilmi, että tutkimukseen osallistuneista yrityksistä jopa 44 prosenttia kertoi, että heidän työntekijänsä eivät seuraa laadittua tietoturvapolitiikkaa oikein ja riittävän turvallisesti. Kaksiviidesosaa yrityksistä raportoi tutkimuksessa, että heidän työntekijänsä eivät seuraa lainkaan tietoturvapolitiikkaa. Tämän lisäksi Kasperskyn tutkimus osoitti, että vain hieman yli neljännes (26 prosenttia) yrityksistä aikoo tehdä jotain tietoturvapolitiikalleen – tämä puolestaan osoitti sen, että harva yritys aikoo ottaa oikeita askelia parantaakseen tietoturva-asioitaan omatoimisesti.

Kaspersky näkee myös tietoturvapolitiikoissa ongelman; yleensä työntekijälle annetaan useita sivuja pitkä dokumentti, jonka todella moni allekirjoittaa ja hyväksyy, mutta harva työntekijä dokumenttia todellisuudessa lukee. Kasperskyn mukaan tähän voisi olla ratkaisuna se, että työntekijöille kerrottaisiin riskeistä, vaaroista sekä hyvistä ja toimivista toimintatavoista selkokielisesti yhdistettynä tietoturvapolitiikkaan.

Kasperskyn mukaan on ensisijaisen tärkeää, että työntekijöitä koulutetaan tietoturvaan liittyen. Hyvät tietoturvakoulutukset auttavat työntekijöitä ymmärtämään tietoturva-asioita ja motivoimaan heitä kiinnittämään huomiota kyberuhkiin. Hyvä koulutus myös takaa sen, että työntekijä osaa toimia myös hyökkäyksiä vastaan oikea oppisesti. Onkin tärkeää, että työntekijät asentavat esimerkiksi uudet päivitykset, varmistavat, että virustentorjuntaohjelmistot ovat päällä ja pitävät huolta salasanoistaan oikeaoppisesti.

Kasperskyn tutkimuksen mukaan 35 prosenttia yrityksistä näkee tietoturvatilanteensa parantuvan, jos työntekijöitä koulutetaan enemmän. Nyt on aika Kasperskyn mukaan yritysten aika ottaa vastuuta sille, että inhimilliset virheet voidaan estää tulevaisuudessa.

5.4 Inhimilliset tekijät kyberturvallisuudessa, Bowen, Devarajan, Stolfo

Bowenin, Devarajanin ja Stolfon tutkimus tehtiin satunnaisesti valituille 4000 ihmisille, jotka eivät tienneet osallistuvansa tutkimukseen, Columbian yliopistossa New Yorkissa. Tutkimuksessaan he lähettivät kaikille osallistujille yhden väärennetyn huijaussähköpostiviestin, jotka oli toteutettu oikeiden huijausviestien pohjalta. Näissä sähköpostiviesteissä oli erilaisia liitteitä, URL-osoitteita ja muita kaavakkeita, joilla tutkimusryhmä pystyi keräämään käyttäjätietoja. Käyttäjät, jotka syöttivät tietonsa väärennettyyn huijausviestiin, valittiin jatkamaan tutkimuksessa (Bowen, Devarajan & Stolfo 2011).

Bowenin mukaan tietoturvallisuudessa ei ole kyse vain teknologioista tai erilaisista järjestelmistä, vaan siinä pitää ottaa huomioon myös inhimilliset tekijät ja erilaiset prosessit. Heidän tutkimuksensa mukaan vuonna 2009 tapahtuneista tietomurroista 28 % johtui sosiaalisista hyökkäyksistä, kuten esimerkiksi sähköpostin kautta lähetettyjen kalasteluviestien vuoksi. Kalasteluviesteissä on usein kyseessä esimerkiksi väärennetty viesti pankilta tai sosiaalisen median sivuilta. Käyttäjän nämä avatessaan käyttäjä saa usein tietokoneelleen ohjelman, jonka kautta hakkerit voivat saada pääsyn tietokoneelle ja pahimmillaan koko tietokantaan. Heidän tutkimuksensa mukaan kalasteluyritykset ja ennen kaikkea niiden onnistuminen olivat yrityksille suurin taloudellinen taakka verrattain muihin hyökkäyksiin. Jatkuvista teknologisista ponnisteluista huolimatta ei tutkimuksen kirjoitushetkellä ollut löydetty 100 prosenttisesti toimivaa ratkaisua kalasteluviestien estämiseen (Bowen ym. 2011).

Tutkimuksessa tuli myös ilmi, että usein taustalla on se tekijä, että työntekijöitä ei olla koulutettu riittävän hyvin tunnistamaan erilaisia kalasteluviestejä. Heidän mukaansa myös perinteiset koulutukset eivät ole usein riittäviä ja heidän mielestään työntekijän tietoturvataitoja on parempi koulia ja parantaa tekemällä väärennettyjä huijaussivuja. Heidän keräämän datan mukaan tämä on ollut perinteistä koulutusta tehokkaampaa. Tutkimuksessa nostettiin myös esille se, että käyttäjän reagoinnilla voi olla myös merkitystä sen suhteen, että miten tietoturva yrityksen sisällä voidaan saada parempaan kuntoon.

6 Yhteenveto

Paha vaanii – kyberuhat ovat arkipäivää alati digitalisoituvassa yhteiskunnassa, jonka vuoksi tietoturvaa ei pidä väheksyä.

Maailmassa on olemassa satoja, ellei tuhansia, tietoturvaohjelmistoja ja tietoturvapolitiikkoja, mutta jokainen niistä on yhtä vahva kuin sen heikoin lenkki.

Tutkimuksen aikana nousi useita kertoja esille se, että yrityksen työntekijät eivät yksinkertaisesti ymmärrä yrityksen tietoturvapoliittisia asioita, he ovat ymmärtäneet ne väärin tai heidän saamansa tietoturvakoulutus ei ole ollut riittävää. Väärinymmärrettyinä tietoturvapoliittiset asiat saattavat aina yrityksen tietoturvan vaaraan. ”Rasti ruutuun”-ajattelutapa ei ole nykypäivää tietoturvapolitiikassa, koska harva ihminen jaksaa niitä lukea. Tämä ajattelutapa pitäisi korvata. On myös tärkeää, että yrityksen työntekijät ymmärtävät tietoturvauhat ja niiden vaikutukset koko yritykseen. Ilman tätä ymmärrystä tietoturvapolitiikka ei yrityksessä voi koskaan toimia. Tutkimuksen aikana nousi esille se, että myös työntekijöiden riittävä koulutus voi taata sen, että tietoturvapolitiikat saadaan toimimaan paremmin.

Tietojenkalastelu on sekä maailmanlaajuisesti että Suomen tasolla edelleen erittäin suuri ongelma, jonka vuoksi on tärkeää, että työntekijät osaavat olla myös kriittisiä sähköposteja avatessaan. Nykyiset tietojenkalasteluviestit on osattu myös tehdä niin hyviksi, että työntekijöiden tarkkaavaisuuden tulee olla riittävän hyvää. Tämän vuoksi on myös tärkeää, että työntekijöitä ja johtoporrasta osataan kouluttaa niin, että sähköpostiviestit katsotaan tarkasti läpi.

Inhimilliset tekijät ovat merkittävä riski yksilön ja yrityksen tietoturvalle, jonka vuoksi jokaisen yrityksen ja yksilön tulisi ottaa tietoturvapoliittiset asiat tosissaan, eikä nähdä pahimmillaan vihollisena. Tietovuodot ja -murrot ovat merkittävä kuluerä maailmanlaajuisesti ja sen tuottamat tappiot kasvavat vuosittain merkittävästi. On myös käsittämätöntä, että pelkästään Suomessa löydettiin kymmeniä tuhansia suojaamattomia tai tehdasasetuksilla olevia laitteita yritysten verkoista. On siis aika lisätä työntekijöiden koulutusta ja ennen kaikkea ihmisten tulee ymmärtää tietoturvan merkitys. Tämä oivallus on täysin ihmisestä kiinni oleva asia – ei olla enää nyky-yhteiskunnassa välinpitämättömiä tietoturvan suhteen.

Maailmalla vallitseva koronatilanne on myös odotetusti osoittanut omanlaisiaan ongelmia, koska koronan myötä on seurannut myös eräänlainen etätyöpandemia. Olisiko tilantee-

seen kuitenkin pitänyt varautua jo silloin, kun COVID-19 lähti leviämään maailmanlaajuisesti? Valitettavasti todella moni yritys esimerkiksi Suomessa painii edelleen etätöistä johtuvien muutosten kanssa. Toisaalta lienee asiallista huomioida, että jälkiviisaus on paras viisaus – tammikuussa 2020 meistä tuskin kukaan osasi arvata, että korona iskee Suomeen niin miten se on iskenyt. Tai sitä, että olisimme samassa tilanteessa edelleen, toukokuussa 2021.

Opinnäytetyötä oli mielenkiintoista ja mielekästä kirjoittaa, vaikka sen suunta muuttui radikaalisti kesken kaiken. Alun perin olin aivan satavarma, että ilman haastatteluita en opinnäytetyötä tule ”maaliin asti” viemään, mutta onneksi aiheesta on tehty laajalti tutkimuksia. Tämän vuoksi koen, että myös tämän kaltaisten tutkimusten muuttaminen kesken kaiken on ollut itselleni suuri opetus – etenkin nyt, kun opinnäytetyö on saatu valmiiksi.

Olen ollut aina tietoinen siitä, että inhimilliset tekijät ovat suuri tekijä yrityksen tai yksilön tietoturvalle, mutta sen yleisyys ja vakavuus olivat itselleni eräänlainen shokki. Itselleni oli myös yllättävää se, että ihmisten luottamusta ja ystävällisyyttä voidaan käyttää yllättävän helposti hyväksi, ihan vaikka pukeutumalla työympäristöön sopivalla tavalla esittäen kiireistä, lupaamalla ihmisille erilaisia asioita tai jättämällä tyhjiä USB-muistitikkuja julkisille paikoille. Henkilökohtaisesti en voi itse ymmärtää, että miksi kukaan liittäisi tietokoneeseensa täysin tuntematonta laitetta, mutta osa tutkimuksista osoitti toista.

Opinnäytetyötä kirjoittaessani minulle myös valkeni se, että kuinka suuri bisnes verkkorikollisuus todellisuudessa on. Olen ollut tietoinen siitä, että se on suurta, mutta arviot siitä, että se on maailman kolmanneksi suurin ekonomia vuoteen 2025 mennessä on järisyttävä arvio.

Pidä mieli kirkkaana – Yksinkertaisilla ja pienillä asioilla kohti turvallisempaa huomista. Ei säilytetä salasanoja näppäimistön alla. Suljetaan päätteet, kun lähdetään työpisteeltä. Vaihdetaan laitteiden oletusasetukset. Pidetään ohjelmistot päivitettyinä ja ajan tasalla.

Lähteet

BBC. 2018. Uber pays $148m over data breach cover-up. Luettavissa: https://www.bbc.com/news/technology-45666280. Luettu: 14.12.2020.

Bowen, B., Devarajan, R. & Stolfo, S. 2011. Measuring the Human Factor of Cyber Security. Luettavissa: https://www.researchgate.net/publication/232747655_Measuring_the_Human_Factor_of_Cyber_Security. Luettu: 29.11.2020.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C. & Giannakopoulos, G. 2014. The Human Factor of Information Security: Unintentional Damage Perspective. Luettavissa: https://www-sciencedirect-com.ezproxy.haaga-helia.fi/science/article/pii/S1877042814040440?via%3Dihub. Luettu: 14.3.2021.

IBM Security. 2020. Cost of a Data Breach Report 2020. Luettavissa: https://www.ibm.com/downloads/cas/RZAX14GX. Luettu: 13.4.2021.

Kaspersky Daily. 2017. The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. Luettavissa: https://www.kaspersky.com/blog/the-human-factor-in-it-security/. Luettu: 15.11.2020.

Kearney, P. 2016. Security: The Human Factor. IT Governance Ltd. Cambridgeshire.

Kyberturvallisuuskeskus. 2021a. Kybersää – Tammikuu 2021. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4_tammikuu_2021_TLP_WHITE.pdf. Luettu: 09.04.2021.

Kyberturvallisuuskeskus. 2021b. Tietoturvan vuosi 2020. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Tietoturvan-vuosi-2020_210212_FIN.pdf. Luettu: 10.04.2021.

Lacey, D. 2009. Managing the Human Factor in Information Security: How to Win over Staff and Influence Business Managers. John Wiley & Sons Inc. New Jersey.

Leppänen, J. 2006. Yritysturvallisuus käytännössä – turvallisuusjohtamisen portfolio. Talentum. Helsinki.

Morgan, S. 2020. Cybercrime to Cost the World $10.5 Trillion Annually By 2025. Luettavissa: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/. Luettu: 14.12.2020.

Paakkanen, M. Psykoterapia-keskus Vastaamo vaihtaa hallituksen puheenjohtajaa, tietomurrosta tehty rikosilmoituksia jo noin 25 000. 2020. Luettavissa: https://www.hs.fi/kotimaa/art-2000007608441.html. Luettu: 15.11.2020.

Tilastokeskus. 2019. Suomalaisten internetin käyttö 2019. Luettavissa: https://www.stat.fi/til/sutivi/2019/sutivi_2019_2019-11-07_kat_001_fi.html. Luettu: 27.11.2020.