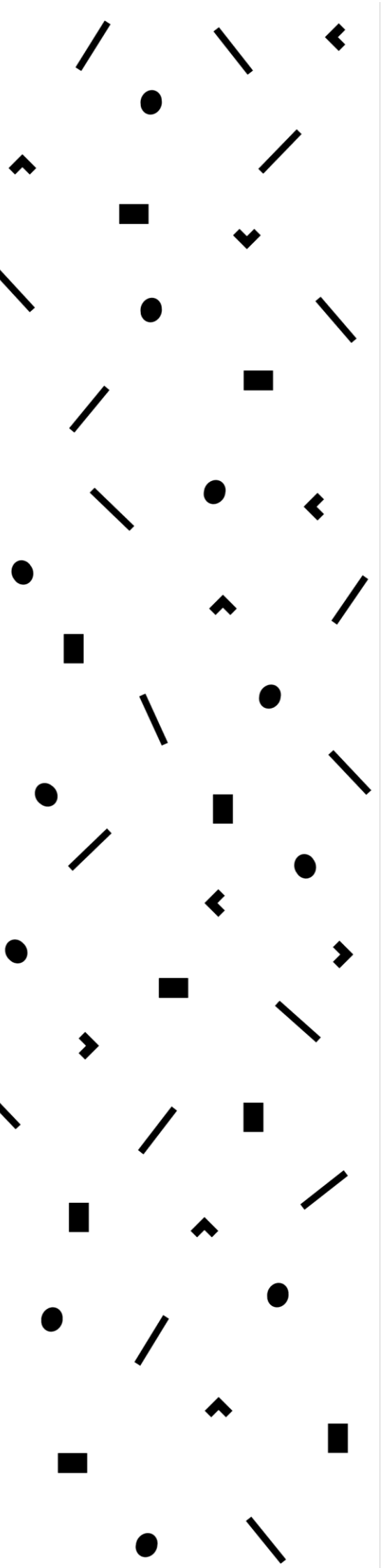


LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

Tietoturvan ja yksityisyyden suojaamisesta huolehtiminen

Miten tietoturvaa ja yksityisyyden suojaa edistetään?

LAHDEN
AMMATTIKORKEAKOULU
Liiketalous
Tietojenkäsittely
Opinnäytetyö AMK
Kevät 2018
Reino Raski
Joni Oinas

Lahden ammattikorkeakoulu
Tietojenkäsittely

RASKI, REINO
OINAS, JONI

Tietoturvan ja yksityisyyden suojaamisesta huolehtiminen
Miten tietoturvaa ja yksityisyyden suojaa edistetään?

Tietojenkäsittelyn opinnäytetyö, 38 sivua, 1 liitesivu

Syksy 2017

TIIVISTELMÄ

Opinnäytetyössä tulemme käymään läpi, kuinka ihmiset huolehtivat ja edistävät tietoturvaansa sekä yksityisyyden suojaansa. Keskityimme tietokoneen ja puhelimen käyttöön liittyvään tietoturvaan ja yksityisyydensuojaan.

Tavoitteena oli saada selville pienellä otannalla kuinka hyvin ihmiset huolehtivat tietoturvastaan ja yksityisyyden suojasta.

Tutkimusaineisto kerättiin kuudelta henkilöltä kyselylomakkeiden avulla. Kävimme läpi ensin aiempia tutkimuksia ja raportteja aiheesta. Tämän jälkeen vertailimme aineiston ja henkilöiden tuloksia keskenään, sekä sen jälkeen tutkimustuloksiin.

Tutkimuksessa selvisi, että tietoturvan ja yksityisyyden suojan edistämisessä havaittiin puutteita. Nämä puutteet olivat esimerkiksi samojen salasanojen käyttö eri palveluissa, VPN-ohjelmien puuttuminen ja reitittimien asetusten muokkaaminen turvallisemmaksi. Virustorjuntaohjelmien käyttö oli kuitenkin vastanneiden keskuudessa hoidettu hyvin.

Asiasanat: tietoturva, yksityisyyden suoja, MAC-filtteri, VPN

Lahti University of Applied Sciences
Degree Programme in Information Technology

RASKI, REINO
OINAS, JONI

Internet security, privacy concerns and how to improve them.

Bachelor's Thesis in Information Technology, 38 pages, 1 page of appendices

Autumn 2017

ABSTRACT

In this thesis we investigated how people took care of their information security and privacy concerns. We focused on computer and mobile phone related security and privacy.

The goal was to find out how well people took care of their information security and privacy.

The research material was collected from six different people. First, we went through previous research results and reports about the subject. After this we compared the results between each other.

In this study we found out that there was severe problems about information security and privacy. The problems were in example: usage of the same passwords in different services, lack of VPN-software's and changing routers settings to more secure ones. Anti-Virus software usage was taken care well.

Keywords: information security, privacy, MAC-filter, VPN

SISÄLLYS

1 JOHDANTO

Ilmiönä tutkimme tietoturvan huolehtimisesta ihmisten keskuudessa, kuinka sitä edistetään ja sekä yksityisyyden suojaamisesta. Nykyään verkostoituminen on niin yleistä, että suurin osa uusista esineistä (jääkaappi, puhelin, tv ja ajoneuvot) käyttävät verkkoyhteyksiä ja erilaisia komponentteja, joissa olisi hyvä olla suojaukset kunnossa. Esimerkiksi Yhdysvalloissa ihmiset pelkäävät nykyään enemmän kyberrikollisia kuin fyysistä rikollista, joka tulee talon sisälle varastamaan tavaroita (Cloudmask 2016).

Aiheena toimi tietoturva ja yksityisyyden suoja. Ilmiönä tutkimme kuinka ihmiset huolehtivat tietoturvasta, kuinka tietoturvaa edistettiin ja yksityisyyttä suojattiin. Tutkimusongelmana: Miksi tietoturvasta ja yksityisyyden suojasta kannattaa huolehtia? Tutkimusmetodina käytimme kvalitatiivista tapaa.

Tutkimuksen alussa kerromme hieman aiheesta ja mitä/kuinka tutkimme. Tämän jälkeen kerromme haastateltavien henkilöiden taustoista sekä heidän vastauksistaan kysymyksiimme. Tämän jälkeen kirjoitamme niistä ja vertailemme eri tutkimustulosten tuloksiin kyseisiä haastatteluita. Lopuksi vertailemme haastateltavia keskenään.

Tutkimuskysymyksenä toimi: Kuinka tietoturvasta ja yksityisyydensuojasta huolehditaan sekä miten sitä edistettiin? Tutkimuksemme tavoite oli saada selville pienellä otoksella kuinka hyvin ihmiset oikeasti huolehtivat tietoturvastaan ja yksityisyyden suojastaan.

Kuten aiemmin mainitsimme, käytimme tutkimuksessa kvalitatiivista tutkimusmenetelmää. Yritimme selvittää kuinka/miten eri henkilöt pitivät huolta tietoturvastaan ja yksityisyyden suojastaan.

Ilmiönä toimi ihmisten huolehtiminen tietoturvasta, kuinka tietoturvaa ja heidän yksityisyyden suojaa edistettiin. Tutkimaan ilmiötä ottamalla pienen otannan ja kysymällä heiltä, kuinka he huolehtivat tietoturvastaan ja yksityisyyden suojastaan.

Toinen opinnäytetyön tekijöistä on itse huomannut, kuinka jotkut ihmiset eivät välitä tietoturvastaan tai yksityisyyden suojastakaan. Hän oli myös itse samanlainen ennen. Hän käytti samoja salasanoja joka paikassa, ei muuttanut mitään asetuksia reitittimessä, kun sai sen ja kytkin sen internettiin. Lisäksi hän asenteli ohjelmia, joista ei ikinä ollut kuulutkaan. Nuorena hän joutui myös itse lukitusohjelman kohteeksi, tällöin kiristysohjelma lukitsi selaimen ja vaati rahaa tietyn ajan sisään, jotta saisi selaimen auki. Kyseisen tapaturman olisi voinut välttää paremmalla internet selailulla ja katsomalla tarkemmin sivustojen nimiä ja URL-osoitteita. Hän sai kuitenkin poistettua kiristysohjelman helposti, poistamalla pelkästään selaimen ja asentamalla sen uusiksi.

Tämän jälkeen hän alkoi olla huomattavasti varovaisempi ja harkitsi enemmän mitä sivuja selaili. Samalla hän myös alkoi hieman yleisemmällä tasolla ottamaan asioista selvää, kuinka voi suojautua paremmin erilaisilta uhilta ja ylipäätänsä edistää tietoturvaa. Hän on myös auttanut monia ystäviä erilaisten virusten ja haittaohjelmien poistamisessa. Ongelman tarkentamiseksi hän kysyi usein, että mitä käyttäjä teki ennen kuin sai viruksen koneeseen. Usein selitys oli, että selaili tuntemattomilla sivuilla, joista ei ollut kuulutkaan. Samalla hän huomasi, että heillä ei ollut käytössä virustorjuntaohjelmia.

Usein uusien tavaroiden hankinnoissa ei paneuduta tarkemmin laitteen asetuksiin tai tietoihin. Laitteet kytketään vain kiinni ja aloitetaan käyttäminen. Kyseinen tapa on ollut hyvin yleistä ystäviemme keskuudessa varsinkin reitittimien osalta. Tavassa on se vaara, ettei edes vaihdeta reitittimen oletus Käyttäjä/Salasana tietoja. Kyseiset tiedot ovat yleensä oletuksena ”admin/admin” tai ”admin/password”. Internetistä löytyy monia sivuja, joihin on koottu kaikkien reitittimien oletustiedot (käyttäjä, salasana ja IP tiedot). Hyökkääjä saa nopeasti selville reitittimen tiedot, jonka jälkeen yleensä koitetaan syöttää oletus salasanoja. Moni tekee kyseisen virheen, ettei vaihda oletustietoja. Kyseinen toimenpide on helppo ja nopea tehdä. Tällä tavalla vaikeutetaan huomattavasti hyökkääjien pääsyä reitittimeen tai langattomaan verkkoon. Pienillä ja helpoilla teoilla voi parantaa jo paljon tietoturvaa ja yksityisyyden suojaa.

Edellä mainittuja toimia ei kannata pitää mitättömänä toimenpiteenä. Tutkimuksessamme keräsimme aineistoin kyselylomakkeella, kuinka he edistivät tietoturvaan liittyviä asioita.

2 KIRJALLISUUSKATSAUS ERILAISISTA TIETOTURVAUHISTA

Kirjallisuuskatsauksen syvällisempi analysointi tapahtuu myöhemmässä vaiheessa, sillä käytimme induktiivista menettelytapaa tutkimuksessa. Johdannossa tuli jo ilmi, että ihmiset ovat melko tietoisia tietoturvan tärkeydestä. Varsinkin henkilöt, jotka olivat joutuneet hakkeroinnin uhreiksi.

Suomessa on kaavailtu jokaiselle autolle omia ”mustia laatikoita”. Nämä laatikot keräisivät autoilijoista tietoja, kuten niiden sijainnit ja nopeustiedot. Kyseiset tiedot lähetettäisiin automaattisesti tietokeskukseen, jossa kyseistä dataa analysoitaisiin. Mustia laatikoita pyrittäisiin hyödyntämään myös tulevaisuudessa verotuksessa, jos esimerkiksi tienkäyttömaksulaki tulee voimaan. Liikenteen turvallisuusvirasto (Trafi) on testannut skenaariota, jossa he ovat kytkeneet autoihin mustia laatikoita ja keränneet tietoja kyseisistä autoista. (Koskinen 2017)

Mustista laatikoista on löytynyt jo tähän mennessä isoja haavoittuvuuksia, jotka voivat vaarantaa ihmisen yksityisyyden suojaa. Disobey -niminen hakkeriyhteisö oli testannut mustien laatikkojen tietoturvaa. Testausten yhteydessä he löysivät haavoittuvuuden. Haavoittuvuuden avulla hakkeri pystyisi saamaan reaaliajassa kaiken datan, jonka olisi tarkoitus mennä ”viranomaisten” käsiin. Tämä kuitenkin vaatisi fyysisen pääsyn mustaan laatikkoon, jotta siihen voisi tehdä muutoksia. (Mansikka 2017)

Travelers raportissa haastateltiin yli 1000 amerikkalaista kansalaista, jossa kysyttiin erilaisista uhista mitkä pelottavat heitä. Vuonna 2015 tehdyssä raportissa 57% prosenttia vastaajista kertoi pelkäävänsä kyberrikollisuutta. Vuonna 2014 luku oli 36%. Jopa 25% haastateltavista kertoi, että heidän tietoihinsa oli päästy käsiksi tai he olivat joutuneet hyökkäyksen kohteeksi. Eli heidän tietojaan oli varastettu verkon välityksellä, esimerkiksi pankkitunnukset tai muut henkilökohtaiset tiedot. (Travelers 2015, 2.)

Jopa 25% prosenttia pelkäsi kovasti yksityisyyden menettämistä tai identiteetti varkautta, 60% oli huolissaan siitä jonkin verran. Sekä tietotekniikka ja tietomurtoja pelkäsi todella paljon 21% vastaajista ja 57%

jonkin verran. Kun taas erilaiset pelot luonnonilmiöistä ja matkustus tapaturmista heiluivat lukemissa 11%-13% (kovasti pelkäävät) ja n.43% (lievästi). Eli ihmisillä oli suuri pelko tietoturvan ja yksityisyyden suhteen, vaikkakin auto-onnettomuuteen voi myös joutua päivittäin esimerkiksi töihin mennessä. (Travelers 2015, 3.)

Samassa tutkimuksessa kysyttiin hakkeroinnin kohteeksi joutuneilta, kuinka hyvin he valitsivat salasanansa. Vastaajista 86% sanoo, että ne olivat vahvoja ja ne pidettiin salassa. Aikuisista 78% ketkä eivät olleet joutuneet hakkeroinnin kohteeksi, sanoivat salasanojen olevan vahvoja. Toisessa kysymyksessä 84% hakkeroinnin kohteeksi joutuneista kertoivat rajoittavansa henkilökohtaisten tietojen laittamista internettiin. Luku on 76% sellaisilla ketkä eivät olleet hyökkäyksen kohteena. Uhreiksi joutuneilla oli enemmän tietoisuutta ja halua parantaa omaa tietoturvaa sekä yksityisyyden suojaa. (Travelers 2015, 9.)

Viestintäviraston raportissa ”Tietoturvan vuosi 2016” käytiin läpi vuotta 2016 millaisia uhkia ja haavoittuvuuksia tuli esille. Johdannossa mainittiin iskusta Lappeenrannassa olevien asuntojen lämmönsyöttö laitteisiin. Tämä tapahtui marraskuussa, jolloin oli pakkasta. Tämä ei suoranaisesti vaikuttanut yksilöityyn ihmiseen. On hyvin tärkeää, että yrityksetkin tajuaisivat tietoturvan tärkeyden. Hyvällä tietoturvalla Lappeenrannan hyökkäys olisi mahdollisesti voitu estää. (Saarimäki 2017, 3.)

2.1 Yritysten tietoturvauhat

Yrityksillä on vielä isompi syy olla tarkempia tietoturvansa hoitamisessa. Yrityksillä on aina jotain sellaista tietoa, mikä olisi hyvä pitää salassa esimerkiksi kilpailijoilta tai pitää asiakkaidensa tietoja turvassa. Riskienhallinta ennakkoon oli usein paljon halvempaa kuin tapahtuneen hyökkäyksen vahinkojen korjaaminen jälkikäteen. (Kurittu 2015, 1.)

2.1.1 Tietojenkalastelu yritykset

Tietojenkalastelu yritykset, jotka kohdistuvat yrityksiin ovat todella yleisiä nykypäivänä. Tietojenkalastelun tavoitteena on saada kohteen tärkeitä tietoja tai tunnuksia, esimerkiksi käyttäjätunnuksia sähköpostitileihin, pankkitunnuksia tai luottokorttitietoja. Tietojenkalastelu yritykset tapahtuvat yleisesti sähköpostiviesteillä. Kirjeitse on myös mahdollista tulla ”oikea” lasku. (Viljanen 2017)

Sähköpostiviestien aiheena on yleensä tekaistu lasku tai ilmoitus, että pankkitililläsi on ollut epäilyttävää toimintaa. Usein näissä sähköpostiviesteissä ohjeistetaan kirjautumaan pankkitunnuksilla pankkiin sähköpostissa olevan linkin kautta. Kyseinen linkki vie tekaistulle pankkisivustolle. Jos uhri syöttää tekaistulle pankkisivustolle pankkitunnuksensa, hyökkääjät saavat tunnukset haltuunsa ja pahimmassa tapauksessa he voivat tyhjentää koko pankkitilin. (Viljanen 2017)

Tietojenkalastelun huomaa helposti siitä, että sähköpostiviestissä on kielioppivirheitä tai niissä kysytään suoraan pankkitunnuksia. Mikäli sähköpostissa on linkki esimerkiksi pankkisivustoille, on hyvin tärkeää katsoa, että linkin URL -osoite on oikea. Yleensä oikean pankkipalvelun linkki on valmiiksi suojattu eikä siinä ole mitään erikoisia numerosarjoja, esimerkiksi: https://www.op.fi. Huijausviesteissä on yleistä, että linkin URL –osoite on suojaamaton ja siinä on epämääräistä tekstiä, esimerkiksi: http://www.nordea.fi.sitemod.session82456133790.hsa.hk/client.aspx. (Viljanen 2017)

Tiedämme yhden tapauksen, jossa yritykseen tuli kirjeitse huijauslasku ulkomailta. Kirjeessä oli laskun lisäksi toinen paperi, joka oli huomautus. Huomautuksessa mainittiin, että maksu pitää suorittaa mahdollisimman pian tai muuten asia viedään pidemmälle. Kyseinen huijausyritys oli helppo tunnistaa, koska yritys ei ollut ikinä ollut tekemisissä laskussa mainitun yrityksen kanssa ja laskuttajan yritys oli ulkomailta.

Yritykset voivat suojautua tietojenkalastelulta kouluttamalla henkilökuntaansa toimimaan turvallisesti verkossa. Hyviä keinoja on välttää menemästä tuntemattomille sivuille tai avata tuntemattomista sähköposteista tulleita viestejä. Sähköpostilaatikoihin voi myös asentaa erilaisia lisäohjelmia, jotka tunnistavat roskapostit ja vievät ne automaattisesti karanteeniin. Tällöin sähköpostin käyttäjät saavat tiedon, että karanteenissa on sähköposteja. Karanteenissa olevista viesteistä näytetään uhkataso, otsikko ja lähettäjän tiedot. Tällöin käyttäjät saavat oman harkinnan mukaan palauttaa karanteenissa olevan sähköpostin, jos käyttäjä on täysin varma sähköpostin luotettavuudesta.

2.1.2 Työntekijöiden kouluttaminen

Vuonna 2017 THL:n työntekijä vuoti vahingossa 6000 hengen henkilötiedot ja laboratoriotulokset internettiin. Nämä kaikki tiedot olivat löydettävissä yleisillä hakukoneilla, esimerkiksi Google ja Bing. THL pyysi Googlea poistamaan kyseiset hakutulokset. Tiedot kerettiin lataamaan ainakin viisi kertaa eikä THL:llä ole tietoa kuka ne oli mahdollisesti ladannut. Nämä tiedot voivat tulla esille vielä tulevaisuudessa, sillä tietoja oli ladattu eikä kenelläkään ole varmaa tietoa kuka ne oli ladannut. (STT 2017)

Työntekijöiden koulutus on myös tärkeää hyvän tietoturvan kannalta. Toisen opinnäytetyön tekijän kokemuksen mukaan esimerkiksi sairaalan vastaanottotiskin läheisyydessä oli paljon erilaisia papereita, joissa oli mahdollisesti erilaisia henkilötietoja. Vastaanottotiskin ovi oli auki. Tällöin kuka tahansa sairaalan potilaista tai vierailijoista olisi voinut käydä tutkimassa sairaalan tietokoneilta löytyviä tiedostoja tai dokumentteja.

Tämän kaltaiset tapaukset voitaisiin välttää hyvällä koulutuksella ja huolellisuudella. On hyvin tärkeää esimerkiksi kirjautua ulos koneelta, jos on poistumassa työpisteeltä edes vähäksi aikaa.

2.1.3 TOP-5 uhkaa organisaatioilla

1. Päivitysten asentamatta jättäminen
    - Jos eri ohjelmia/käyttöjärjestelmiä ei päivitetä, niihin voi jäädä erilaisia turva-aukkoja, joita hyökkääjät voivat hyödyntää.
2. Erilaiset tietokoneen lukitusohjelmat eli ”kiristyshaittaohjelmat”
    - Kyseiset ohjelmat lukitsevat tietokoneen joko kokonaan tai ainoastaan tietyn osion tietokoneesta. Tämän jälkeen hyökkääjä vaatii rahaa. Rahan saannin jälkeen hyökkääjä lupautuu avaamaan lukituksen. Käyttäjän ei tulisi ikinä noudattaa kiristäjän ohjeita.
3. Erilaiset huijausviestit ja phising viestit eli ”tietojenkalastelu”
    - Yrityksille lähetetään erilaisia huijausviestejä, esimerkiksi laskuja tai pankkivarmennusta vaativia toimenpiteitä.
4. Esineiden ulkoistaminen
    - Esineitä ulkoistetaan nykyään niin paljon, jonka takia sopimuksissa voi olla epämääräiset tekstit esimerkiksi vastuunottajista.
5. Palvelunestohyökkäykset
    - Palvelunestohyökkäykset ovat yksi yleisimmistä ongelmista internetissä. Niillä pyritään lamauttamaan yritysten järjestelmät, kuten esimerkiksi verkkosivut tai verkkokaupan.

Ratkaisut organisaation uhkiin: ohjelmistojen päivittäminen automaattisesti, hyvin koulutettu henkilöstö, varmuuskopioiden tekeminen, erilaisten tietojen tallentaminen ja tietoturvaan liittyvien henkilöiden valitseminen. (Saarimäki 2017, 4.)

2.2 Yksityishenkilöiden tietoturvauhat

Yksityishenkilöiden yleisimpiä tietoturvauhkia on tietojenkalastelu ja erilaiset rahalliset menetykset. Tässä kappaleessa kerromme tarkemmin yksityishenkilöiden uhista ja kuinka niiltä voi pyrkiä suojautumaan.

2.2.1 TOP-5 uhkaa yksityishenkilöillä

Tutkimuksessamme keskityimme tarkemmin yksityishenkilöihin. Tutkimusaineiston kerääminen tapahtui yksityishenkilöiden avulla eikä yrityksiltä, mutta huomioimme myös yritysten erilaisia uhkia ja ratkaisuja.

TOP-5 uhkaa, joita yksityishenkilöillä oli:

1. Erilaiset huijaukset ja valemainokset
    - Eri yritysten nimissä liikkuu valeposteja, joissa pitää kirjautua pankkitunnuksilla tai syöttää luottokortin tietoja.
2. Haittaohjelmien leviäminen älylaitteisiin
    - Esimerkiksi puhelimiin ja älytelevisioihin tehdään enemmän erilaisia viruksia.
3. IoT= Internet Of Things
    - Erilaisia laitteita aletaan yhdistää internettiin, kuten jääkaappeja ja televisioita. Niiden tietoturva on todella heikolla pohjalla tällä hetkellä.
4. Yksityisyyden suoja
    - Ihmiset laittavat kuvia itsestään ja läheisistään sosiaaliseen mediaan. Mahdollisesti tiedostomatta, että niitä tullaan käyttämään mainostamisen kohdistamisessa. Huonoimmassa tapauksessa erilaisiin huijauksiin.
5. Samojen salasanojen käyttäminen eri palveluissa

- Käytetään samoja salasanoja eri sivustoilla ja ohjelmissa. (Saarimäki 2017, 4.)

2.2.2 Ratkaisuja yksityishenkilöiden ongelmiin

Ratkaisut yksityishenkilöiden ongelmiin ovat yksinkertaisia ja helppoja toteuttaa suurimmaksi osaksi.

- Huijauspostien erottaminen voi olla välillä vaikeaa, mutta sen useimmiten erottaa huijaukseksi kielen ulkoasusta tai esimerkiksi linkin ulkoasusta. Linkkiä tai tiedostoa, joka on liitteenä ei saa ikinä avata.

- Salasanojen vaihtaminen ja niiden muistaminen on tehty helpoksi erilaisilla ohjelmilla. Ohjelmien avulla voi luoda vahvoja salasanoja ja tallentaa ne hyvin suojattuina omalle koneelle.

- Virustorjuntaohjelmien käyttö on pakollista, se on yksi parhaista tavoista edistää tietoturvaa.

- Varmuuskopiointia on hyvä myös tehdä. Ei pelkästään tietoturvan vuoksi, mutta jos tietokone rikkoutuu niin voit palauttaa tärkeitä tiedostoja itsellesi.

- Laitteistojen pitäminen ajan tasalla. Päivitetään aina kaikki mahdolliset laitteet, kun niihin on tullut päivityksiä. Tämä ei ole aina mahdollista, jos tuotteentarjoaja ei julkaise päivityksiä. (Saarimäki 2017, 4.)

2.3 Yksityishenkilöiden suurimpia uhkia

Viestintäviraston raportin mukaan yksityishenkilöillä suurimpia uhkia huijauksissa ja kalasteluissa on rahallinen ja tiedollinen menetys. Henkilö voi kärsiä mittavaa vahinkoa, jos hän tulee huijatuksi erilaisilla huijausviesteillä tai laskuilla. Yleensä, jos maksaa jonkin laskun tai

kirjautuu pankkitunnuksilla huijaussivustolle, pyritään kohteen tilit tyhjentämään saman tien. Tällä tavalla huijarit saavat henkilön pankkitietoja, luottokorttitietoja tai salasanoja. (Saarimäki 2017, 5.)

Viestintäviraston raportissa tuli esille paljon erilaisia uhkakuvia ja piileviä vaaroja, joita yksityishenkilöillä ja yrityksillä on. Uhkia tulee tulevaisuudessa vain enemmän, sillä teknologia kehittyy kovaa vauhtia. Tämä tuo paljon hyviä puolia ja helpottavia elementtejä, mutta varjopuolena on se, että sitä myös tullaan käyttämään erilaisiin viruksiin ja haittaohjelmiin.

2.4 Yhteenveto kirjallisuuskatsauksesta

Tämä pienimuotoinen kirjallisuuskatsaus antoi hieman kuvaa jo siitä, kuinka pienillä teoilla ihmiset voivat parantaa tietoturvaansa sekä yksityisyyden suojaa. Tietoturvan vuosi 2016 raportissa oli hyviä ja yksinkertaisia vinkkejä, joita olisi hyvä noudattaa. Esimerkiksi salasanojen päivittäminen ja vaihtaminen jokaiselle sivulle omaksi edistää jo huomattavasti tietoturvaa. Tämä tuli myös ilmi Consumer Risk Index tutkimuksessa. Ihmiset, jotka joutuivat hyökkäyksen kohteeksi vaihtoivat salasanansa vahvempiin. He olivat muutenkin varovaisempia ja tietoisempia tietoturvan tärkeydestä. Yksityisyyden suojaa voi edistää myös vähentämällä kuvien laittoa erilaisiin sosiaalisiin medioihin sekä pitämällä siellä yksityistiedoista tiukasti kiinni. Ei esimerkiksi anna oikeaa nimeä tai koko nimeä. Viestintäviraston ja Consumer Risk Indexin raporteissa olevat keinot ovat melko helposti toteuttavissa, joilla voi parantaa helposti tietoturvaa.

3 KUINKA TEHDÄÄN DEAUTENTIKOINTI-HYÖKKÄYS JA KUINKA SILTÄ VOI SUOJAUTUA

Tässä kappaleessa tulemme käymään läpi, kuinka tehdään pienimuotoinen deautentikointi-hyökkäys langattomaan verkkoon liitettyyn laitteeseen. Tätä varten tarvitaan vain Kali linux käyttöjärjestelmä, johon on jo itsessään asennettu erilaisia tietoturva testi ohjelmia ja sekä langaton verkko johon on liitetty laite. Emme tule mainitsemaan mitään tarkempia komentoja vaan selitämme hyökkäyksen kulun pääpiirteittäin. Emme myöskään näytä laitteiden MAC-osoitteita kokonaisuudessa.

Haluamme näyttää, kuinka helppoa kyseisen hyökkäyksen teko on. Hyökkäyksen avulla voidaan aiheuttaa harmia yritykselle tai yksityishenkilöille. Valitsimme tämän menetelmän, koska tältä ei voi suojautua muulla tavalla kuin olla käyttämättä langatonta verkkoa.

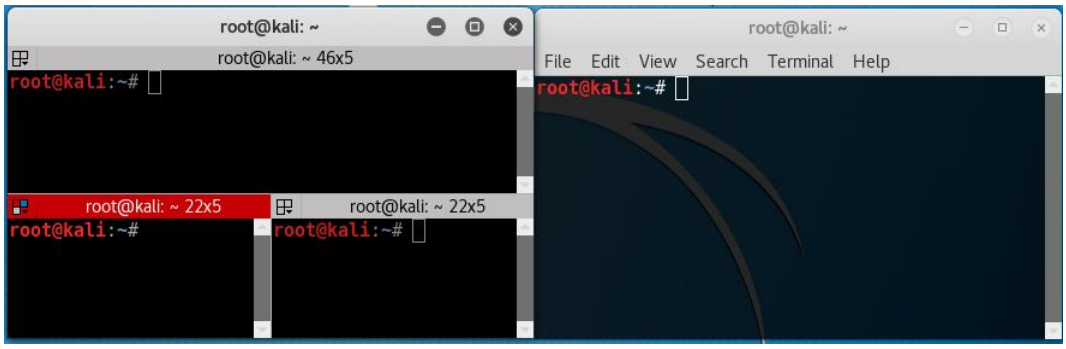
Hyökkäyksen teossa käytimme apuna maksullisen StackSkills -palvelun video-ohjeita. Kappaleissa 6.2 Hyökkäyksen valmistelu ja 6.3 Hyökkäyksen teko, on seurattu monesta eri video-ohjeesta, jolla tavalla kyseinen hyökkäys saatiin toteutettua. (StackSkills 2017)

3.1 Mikä on Kali Linux?

Kali Linux on Debian järjestelmään pohjautuva Linux käyttöjärjestelmä. Kali Linuxia käytetään tietoturvan testaamiseen, esimerkiksi langattomaan verkkoon kohdistuviin hyökkäyksiin sekä porttien skannaamiseen. (Kali Linux Official Documentation 2017)

3.2 Hyökkäyksen valmistelu

Asensimme Virtualbox-ohjelmalla Kali Linux:in virtuaalitietokoneeksi. Tämän jälkeen päivitimme käyttöjärjestelmän ja asensimme ”Terminator” -nimisen konsoliohjelman. Terminator -ohjelman asentaminen ei ole pakollista. Terminator on parempi vaihtoehto kuin normaali terminaali, sillä sen avulla pystyy jakamaan yhden ikkunan moneen osaan. Lopuksi tarvitsemme vielä langattoman USB- vastaanottimen jolla toteutamme hyökkäyksen.

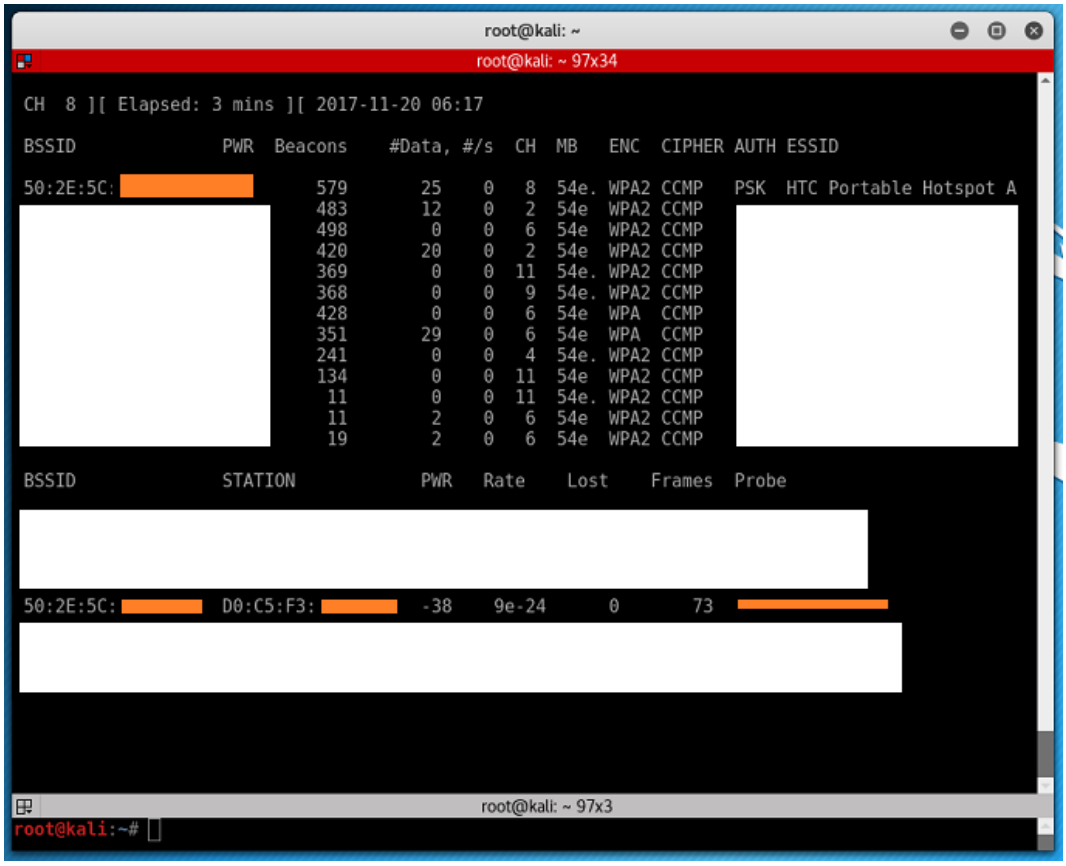


Kuva 1. Terminator – terminaali (vasen) ja normaali terminaali (oikea)

3.3 Hyökkäyksen teko

Kali Linux:in ja Terminator – ohjelman asennusten jälkeen hyökkäyksen voi toteuttaa. Kaikki komennot tehdään suoraan Terminaattori – terminaalissa. USB -langatonvastaanotin pitää olla kiinnitettynä koneeseen, jotta siihen voidaan tehdä tarvittavat muutokset.

Usb-vastaanotin pitää sammuttaa Terminator -terminaalin avulla, jotta saamme tehtyä siihen kaikki tarvittavat muutokset. Tämän jälkeen vastaanotin pitää konfiguroida ”Monitor” -tilaan. Kun olemme muokanneet vastaanottimeen tarvittavat muutokset, voimme käynnistää vastaanottimen uudelleen päälle. Vastaanottimen käynnistyksen jälkeen syötetään komento, jolla aletaan monitoroimaan langattomia verkkoja ja niihin yhdistettyjä laitteita.

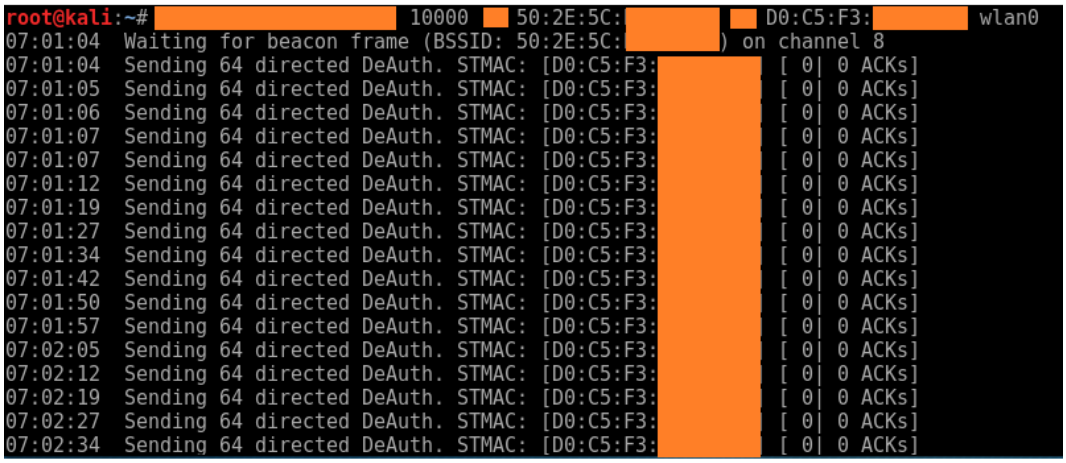


Kuva 2. Näkymä kun langaton vastaanotin monitoroi verkkoja (Oranssilla peitetyt tiedot ovat meidän laitteita)

Kuten kuvassa 2. näkyy, vastaanotin löytää kaikki verkot jotka ovat kantaman sisällä. Riippumatta siitä onko kyseinen verkko piilotettu tai

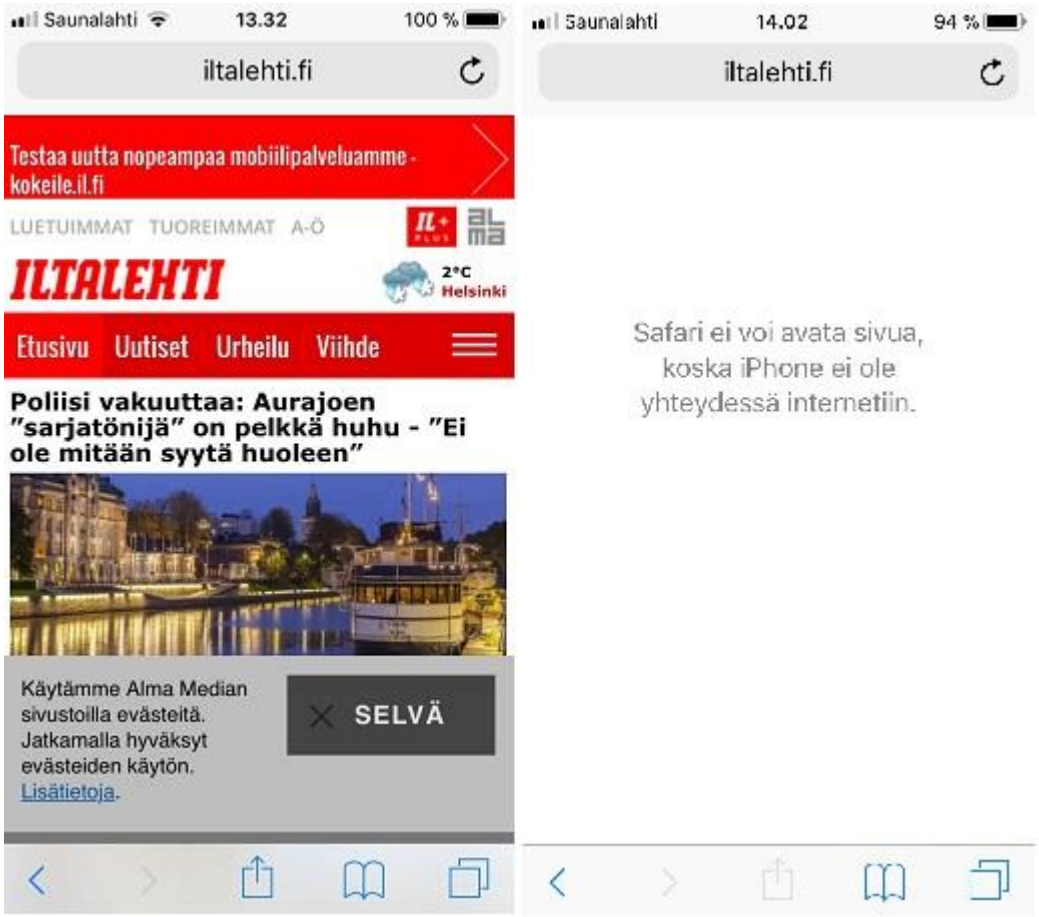
suojattu. Kuvan ylemmässä osassa näkyy saatavilla olevat tukiasemat (BSSID) ja alemmassa taulukossa näkyy sekä tukiasemiin yhdistetyt laitteet (STATION).

Kun olemme löytäneet kohteen, johon haluamme hyökätä, keräämme tarvittavat tiedot alemmasta taulukosta. Nämä tiedot ovat tukiaseman tiedot (BSSID) ja yhdistetty laite (STATION).



Kuva 3. Pakettien lähetys laitteeseen joka on yhdistetty verkkoon. (Oranssilla peitetyt tiedot sisältävät komentoja ja MAC-osoitteita)

Hyökkäyksen aikana lähetetään erittäin suuri määrä paketteja laitteeseen, joka on langattomassa verkossa. Tällöin laite menettää yhteyden tukiasemaan ja verkko häviää.



Kuva 4. Kuvassa näkyy ennen hyökkäystä (vasen kuva) ja hyökkäyksen aikana (oikea)

4 TUTKIMUSMENETELMÄT

Käytimme kvalitatiivista tutkimusmetodia. Kyseinen tutkimusmetodi sopi mielestämme sen takia hyvin tutkimukseemme, koska yritämme saada vastauksia ”Miten…” kysymykseen. Tutkimuksemme aineisto oli myös suhteellisen suppea ja valikoitu, jonka takia kvalitatiivinen tutkimusmetodia oli mielestämme oikea. Tutkimuskysymyksenä toimii: ”Kuinka tietoturvasta ja yksityisyyden suojasta huolehditaan sekä miten sitä edistetään?”. Kvalitatiivisella tutkimusmetodilla saimme vastauksen tutkimuskysymykseen, jota pystyimme analysoimaan tarkemmin induktiivisella lähestymisellä.

Kyseiseen aiheeseen päädyimme, koska aihe on ajankohtainen nyt ja tulevaisuudessa. Tulevaisuudessa yhä useampi laite kytketään internettiin, jonka myötä yhä useampi laite on haavoittuvainen hyökkäyksille tai väärinkäytölle. Tämän lisäksi vanhempia laitteita ei välttämättä tueta uusilla ohjelmistopäivityksillä, joka altistaa entistä enemmän tietoturvauhille.

4.1 Tarkat kuvaukset aineiston keräämisessä

Tutkimuksen aikana keräsimme aineiston kuudelta henkilöltä. Ensimmäinen askel oli tehdä kyselylomake tai kyselykaavake, jota käytimme haastatteluissa. Tällä tavalla pystyimme kysymään monenlaisia erilaisia kysymyksiä tietoturvasta ja yksityisyyden suojasta. Pystyimme selvittämään millaisia keinoja haastateltavat käyttivät tietoturvansa edistämisessä.

Tämän jälkeen valitsimme sellaisia henkilöitä, joiden tiesimme huolehtivan ja ottavan tosissaan tietoturva ja yksityisyysasiat. Sekä sellaisia henkilöitä, joita kyseinen asia ei pahemmin kiinnostanut tai he eivät ajatelleet asiaa syvällisemmin. Henkilöiden valinnassa käytimme yleisiä kysymyksiä mitä mieltä he ovat tietoturvasta ja yksityisyyden suojasta. Vastauksien perusteella päätimme, että onko kyseistä henkilöä syytä ottaa tarkempaan tutkimukseen vai etsimmekö toisen henkilön. Tällä tavalla saimme hyvän

otannan, jossa tulee ilmi eri ääripäät ja monia erilaisia tapoja, kuinka kukin on huolehtinut omasta tietoturvasta.

Löydettyämme hyvät henkilöt joita haastatella, aloitimme haastattelun kyselylomakkeella. Käytimme kyselylomakkeita, joihin olimme määritelleet kysymykset ja henkilö vastaa niihin parhaansa mukaan.

Aineiston keräämisen jälkeen analysoimme jokaisen henkilön tulokset erikseen ja toimme esille mahdollisia riskitekijöitä vastauksien perusteella. Lopuksi vertailimme henkilöitä keskenään. Kokosimme myös kaavioita, joista käy ilmi henkilöiden vastaukset kysymyksiin.

5 TUTKIMUSDATA KEVÄÄLTÄ JA SYKSYLTÄ (2017)

Keräsimme aineiston kahdella eri tutkimuksella. Ensimmäinen tutkimus tehtiin 2017 keväällä, tällöin haastattelimme kolmea henkilöä tarkemmin. Syksyn 2017 haastatteluihin osallistui myös kolme henkilöä. Kevään ja syksyn haastateltavat eivät olleet samoja henkilöitä. Kyselyissä käytettiin samaa kyselylomaketta. Tutkimusdataa analysoidaan tarkemmin kappaleessa 8.

5.1 Tutkimusdata keväältä 2017

Tutkimusaineistomme koostui kolmesta henkilöstä, jotka tunnemme entuudestaan hyvin (nimet muutettu). Yksi henkilö (nimi: Pentti) oli sellainen joka tiedostaa tietoturva uhkia, muttei välttämättä kiinnitä niihin niin paljon huomiota. Perusturvallisuus oli kunnossa ja se riitti hänelle.

Toinen henkilö (nimi: Pekka) piti tietoturvaansa tärkeämpänä ja tiesi hyvin erilaisista uhista sekä kuinka niiltä voi välttyä. Hän piti yksityisyyden suojaa tärkeänä ja pitää siitä hyvää huolta.

Kolmas henkilö (nimi: Erkki) teki usein varmuuskopioita järjestelmästänsä ja oli hyvin tietoinen tietoturvauhista. Hän osasi suojautua todella hyvin erilaisilta tietoturvauhilta ja oli tarkka yksityisyyden suojasta.

Aineisto, jonka keräsimme kyselylomakkeiden avulla antaa vastauksia tutkimuskysymykseen melko hyvin. Aluksi kysymyslomakkeessa oli avoin kysymys, johon vastaaja sai kertoa vapaasti mielipiteensä tietoturvasta ja yksityisyydensuojasta. Tämän jälkeen oli seitsemän tarkentavaa kysymystä, jotka viittasivat erilaisiin uhkiin, joita oli mainittu aiemmin käydyissä raporteissa. Kyselylomakkeen pituus oli sivu, emme määritelleet mitään minimi/maksimi vastaus pituutta. Vastaaja siis sai kirjoittaa sen verran kuin halusi. Aineiston määräksi tuli kolme dokumenttia, eli jokaiselta vastaajalta yksi dokumentti. Vastattujen kyselylomakkeiden pituus vaihteli puolesta sivusta sivuun.

5.2 Tutkimusdata syksyltä 2017

Syksyn tutkimusaineistokin koostui kolmesta henkilöstä, henkilöt olivat opinnäytetyön tekijöiden tuttuja (nimet muutettu). Haastateltavien nimet: Matti, Tuomas, Pertti. Näistä kolmesta Pertti ja Tuomas huolehtivat tietoturvasta heikoiten. Virustorjuntaohjelma löytyi, mutta muuten muut osa-alueet olivat heikkoja. Tuomas ja Pertti molemmat käyttivät yleisesti käytettyä virustorjuntaohjelmaa; Avastia. Kumpikaan heistä ei ole edistänyt yksityisyyden suojaansa esimerkiksi VPN-palvelulla. Tuomas käytti VPN-yhteyttä koulutehtävien tekemiseen, mutta ei muuten päivittäisessä käytössä. Matille tietoturva oli tärkeää, sillä hän huolehti työtehtävissäkin yhtiönsä tietojen suojaamisesta. Sen lisäksi kyselyssä hän mainitsi, että kotioloissa hän tunsi uhaksi kaikki erilaiset lukitusohjelmat tai salasanavakoilut. Hän myös tiedosti yksityisyyden suojan tärkeyden ja haluaisi oppia niistä enemmänkin.

5.3 Kysymyslomakkeen kysymykset

”Kerro lyhyesti mielipiteesi tietoturvasta ja yksityisyydensuojasta. Esimerkiksi haittaako sinua, jos koneellasi on virus, joka ei ulkoisesti näyttäisi tekevän mitään? Haittaako sinua, jos internet palveluntarjoajasi voi nähdä kaiken tiedon missä sivustoilla olet käynyt ja milloin? ”. Tähän vastaaja sai vastata oman mielensä mukaan. Tämän jälkeen oli seitsemän tarkempaa kysymystä:

1. Mitä virustorjunta ohjelmaa käytät?
2. Milloin viimeksi teit virustarkistuksen?
3. Oletko vaihtanut modeemisi/reitittimesi salasanaa?
4. Käytätkö langatonta verkkoa kotona? Jos käytät, oletko esim. laittanut MAC-suodatusta päälle tai piilottanut verkon?
5. Käytätkö VPN-ohjelmia tietokoneellasi tai puhelimessasi?
6. Oletko laittanut virustorjunta ohjelmaa puhelimeesi?
7. Käytätkö samoja salasanoja eri palveluissa?

6 DATAN ANALYSOINTI

Tässä kappaleessa käydään läpi kevään ja syksyn kyselyn tuloksia. Kerromme ensin kevään tuloksista ja havainnoista, jonka jälkeen kerromme syksyn tuloksista ja havainnoista tarkemmin. Lopuksi koostamme kaavioihin, joiden avulla suoritamme vielä lisää vertailua.

6.1 Kevään 2017 kyselytulosten analysointi

Tässä kappaleessa käymme läpi kyselylomakkeesta saadut aineistot. Aineisto koostuu kolmelta henkilöltä saaduista vastauksista, henkilöt olivat Erkki, Pekka ja Pentti. Järjestys tulee olemaan parhaimmasta heikompaan. Kyselylomakkeella selvisi hyvin erilaisia keinoja tietoturvan ja yksityisyydensuojaamisessa.

6.1.1 Erkin tulokset

Erkki tiedosti tietoturvauhat näistä kolmesta henkilöstä kaikkein parhaiten kyselyn vastauksien perusteella. Avoimeen kysymykseen Erkki vastasi näin:

> *”Tietoturvan ja yksityisyydensuojan merkitys on tänä päivänä yhä enemmän merkittävässä roolissa, johtuen teknologian nopeasta kehityksestä ja sen seurauksena olevasta verkostoitumisesta ihmisten tai päätelaitteiden kesken. Minua ei itse haittaa, jos palveluntarjoaja kerää tietoa minusta. Enemmän haittaa, jos joku epämääräinen sivusto tai siihen upotettu elementti kerää minusta tietoa.” -Erkki*

Vastauksesta tulee ilmi, että Erkki oli tietoinen tulevaisuuden näkymästä, jossa erilaiset laitteet tulevat käyttämään internet-yhteyttä. Vastauksesta tulee ilmi, että hän välitti jonkin yksityisyyden suojastaan. Samalla hänellä oli luottamusta internet-operaattoreihin. Tarkentavissa kysymyksissä oli myös hyviä huomioita. Vastauksista tuli selkeästi ilmi, että hän tiesi tietoturvauhista ja kuinka niiltä pystyi suojautumaan.

Erkki käytti tunnettuja ja luotettavaksi osoitettuja (monen eri vertailusivun mukaan) virustorjuntaohjelmia. Virustorjunta ohjelmat, joita hän käytti: F-

Secure Safe ja MalwareBytes. Näillä kahdella ohjelmalla pystyy suojautumaan todella hyvin erilaisilta viruksilta ja haittaohjelmilta. Virustarkistuksen hän oli tehnyt edeltävänä päivänä lomakkeen täyttämisestä. Reitittimen salasanan muuttamatta jättäminen on yleinen virhe, mutta Erkki oli vaihtanut reitittimensä salasanan.

Langattoman verkon käytön kysymykseen Erkki vastasi seuraavasti:

> *”Kyllä wlan on käytössä. Käytän myös Mac-suodatusta ja WPA2-salausta johtuen siitä, että kiinteistössä on muitakin wlan-reitittimiä. En piilota verkkoa, koska mielestäni se on aivan turhaa. Tämän lisäksi tietyt laitteet, eivät välttämättä osaa yhdistää automaattisesti kotiverkkoon wlanin avulla. Jos joku haluaa oikeasti aiheuttaa pahennusta, niin kyllä sen piilotetunkin ssd:n löytää ja helposti.” – Erkki*

Mac- suodatus on todella hyvä keino suojata langattoman verkon ulkopuolisilta. Vaikka ulkopuoliset tietäisivätkin langattoman verkon salasanan, he eivät pääse käyttämään kyseistä verkkoa, jos Mac-suodatus on päällä. Mac-suodatus toimii siten, että jokaisella tietokoneella on yksilöllinen ”tunnus”, jota kutsutaan Mac-tunnukseksi (Fyysinen osoite). Reitittimen asetuksista voi määritellä laitteet, joille sallitaan yhteys verkkoon. Kaikki ne laitteet, jotka ovat lueteltuna Mac-suodatuksen listalla ja tietävät langattoman verkon salasanan, voivat liittyä kyseiseen reitittimeen. Jos ulkopuolisen koneen Mac-tunnus ei ole reitittimen listalla, hän ei pysty yhdistämään kyseiseen langattomaan verkkoon, vaikka hän tietäisi kyseisen salasanan.

Kuten Erkki mainitsi verkon piilottaminen voi tuoda enemmän haittaa kuin hyötyä, pitää paikkaansa tietyissä tilanteissa. Kuten hän mainitsi, että jotkin laitteet eivät osaa välttämättä yhdistää piilotettuun verkkoon. Tämä on varsin yleistä vanhoilla ja jopa uusimmillakin laitteilla. Uudelleen käynnistämisen jälkeen laitteet eivät välttämättä osaa enää yhdistää automaattisesti piilotettuun verkkoon. Jos käytössä on esimerkiksi tietokoneita ja älypuhelimia, niiden kanssa ei pitäisi tulla kyseistä ongelmaa. Langattoman verkon piilottaminen tuo pientä lisäturvaa tietoturvan kannalta. Langattoman verkon voi kuitenkin löytää helposti, jos hyökkääjä tietää mitä tekee.

Erkki käytti myös VPN palveluja, joiden avulla hän pystyi luomaan suojaamattomasta verkosta salatun yhteyden. Tähän hän käytti OpenVPN -ohjelmaa. Kyseistä ohjelmaa käytetään todella paljon varsinkin erilaisissa yrityksissä ja kouluissa. Kyseisen ohjelman avulla voi luoda salatun yhteyden omasta kotiverkosta esimerkiksi koulun tai työpaikan verkkoon, joten etätyöskentely onnistuu hyvin. Puhelimessa Erkki ei käyttänyt mitään virustorjuntaohjelmaa. Tämä johtuu siitä, että hänellä oli käytössään sellainen puhelin missä oli Sailfish- käyttöjärjestelmä.

> *”Käytössä on Sailfish-käyttöjärjestelmällä toimiva puhelin. Siihen ei ole suoraan mitään virustutkaa. Riski saada tartunta on huomattavasti pienempi kuin androidilla, koska käyttäjäkuntakin on huomattavasti suppeampi ja johtuen sovellusten käyttöoikeus-hierarkiasta.” – Erkki*

Vastauksen perusteella tuli ilmi, ettei Sailfish- käyttöjärjestelmään ole tehty mitään virustorjuntaohjelmaa. Tämä ei välttämättä ole hirveän iso riski, koska käyttäjäkunta on pieni kyseisellä käyttöjärjestelmällä. Kuten Erkki itse sanoi. Virustorjuntaohjelman puuttuminen voi olla iso tietoturvauhka puhelimissakin nykyään, mutta Sailfish käyttäjäkunta on niin pieni, ettei sinne välttämättä olla tehty mitään erityisiä viruksia. Lopuksi Erkki mainitsi, ettei käytä samoja salasanoja eri palveluissa. Tämä on todella tärkeää ja hyvä tiedostaa. Aiemmissa raporteissa joita kävimme läpi tuli ilmi, että monella oli heikkoja salasanoja ja niitä saatettiin käyttää monessa eri palvelussa.

6.1.2 Pekan tulokset

Pekka oli tietoinen tietoturvauhista ja piti tietoturvaa hyvin tärkeänä asiana. Pekan avoimessa vastauksessa tuli hyvin ilmi myös, että hän välitti yksityisyyden suojastaan. Hänen vastauksensa avoimeen kysymykseen:

> *”Tietoturva on mielestäni vakava asia. Itse henkilökohtaisesti pidän tietoturvasta huolta. Virustarkistuksen teen säännöllisesi virusten varalta, vaikka virus olisikin sellainen joka ei näkyvästi ole esillä. Itse pidän ns. viruksena jo cookieita joita pakostikin tulee, jolla seurataan käyttäjän tekemisiä esimerkiksi iltalehden sivuilla. Näillä voidaan identifioida tietyn käyttäjän lukemat*

> *uutiset ja täten esimerkiksi muodostaa ko. henkilön poliittinen näkökanta. Tietoturvan kannalta on huono asia, että ihmisestä voidaan kerätä liikaa tietoa, joka voidaan sitten esim. myydä kolmansille osapuolille tai mahdollisesti tietomurron yhteydessä omat henkilökohtaiset tiedot saattavat vuotaa.*
>
> *Virukset koneella saattavat olla huono asia, vaikka ne eivät näkyvästi näy käyttäjälle päälle päin. Esim. keylocker joka rekisteröi kaikki näppäimen painallukset. Tämä virus ei päälle päin näy mutta se voi tallentaa kaikki käyttäjä tunnukset ja salasanat mitä näppäilet koneelle. Huono juttu.*
>
> *Internet palveluntarjoajakaan ei mielestäni saisi kerätä tietoa yksittäisestä ihmisestä tai ylipäätään tietoa ihmisistä mitä he tekevät internetissä. Tietoturvallisesta näkökannasta ihmisten tietojen poistaminen heti kun yhteys on sulkeutunut olisi varma tapa olla vuotamatta tietoja sekä että liikkuvaa dataa ei millään tasolla identifioida tiettyyn käyttäjään (IP osoitteeseen).” - Pekka*

Vastauksesta selvisi, että Pekka tiesi, kuinka käyttäjistä voidaan saada tietoa selailun perusteella ja miten sitä pystytään käyttämään hyväksi. Sen lisäksi hän mainitsi ”Keylocker” nimisen viruksen, joka tallentaa jokaisen näppäin painalluksen. Hyökkääjä voi saada sen kautta henkilöiden yksityistietoja. Pekka oli myös tietoinen yksityisyyden suojasta ja kuinka sitä pystytään käyttämään ”väärin”, eli myymällä tietoja kolmansille osapuolille. Hän myös osasi suojautua kyseiseltä uhalta käyttämällä VPN -ohjelmistoa. VPN -ohjelman avulla yhteytesi suojataan ja salataan niin, että kyseiseen tietoon on todella hankala päästä käsiksi eikä liikennettä pystytä monitoroimaan noin vain.

Virustorjunta ohjelmana Pekka käytti F-Securea. Kyseessä on suomalainen virustorjunta ohjelma ja se on todettu luotettavaksi monissa eri vertailusivustoissa. Virustarkistuksen hän oli tehnyt kaksi viikkoa sitten, mutta hänellä on automaattinen virustarkistus viikoittain joka käy nopeasti tärkeimmät tiedostot läpi. Reitittimen salasana kysymykseen Pekka vastasi näin:

> *”En hetkeen. Tosin salasana on hyvä ja modeemista/reitittimestä itsestään voi seurata onko siellä ollut käyttäjinä ulkopuolisia vai ei.” – Pekka*

Vastauksen perusteella hän olisi jo kuitenkin vaihtanut oletus salasanan toiseen, joka on hyvin tärkeää. Sillä tavalla edistetään hyvin tietoturvaa. Sen lisäksi hän tiesi kuinka hän voi tutkia asiaa enemmän, jos epäili, että joku muu käyttäisi hänen verkkoa. Mac- suodatusta tai verkon piilotusta Pekka ei ollut laittanut päälle. Hän oli kuitenkin pohtinut Mac -suodattimen laittamista. Nämä kaksi keinoa ovat melko helposti toteutettavissa ja niiden avulla vaikeutettaisiin paljon ulkopuolisten pääsyä omaan verkkoon.

Yksityisyyden suojasta hän huolehti F-Securen Freedome VPN-ohjelmalla. VPN ohjelmien avulla ihmiset voivat edistää helposti ja huomattavasti yksityisyydensuojaa. Hän myös käytti Avast- virustorjunta ohjelmaa puhelimessa. Tällä tavalla hän tiesi varmemmin, jos puhelimeen tuli jotain viruksia tai muita haittaohjelmia. Puhelimen virustorjuntaohjelma on todella tärkeää nykypäivänä ja silläkin edistetään huomattavasti ihmisten tietoturvaa. Lopuksi Pekka sanoi, että hän käyttää eri salasanoja eri palveluissa.

6.1.3 Pentin tulokset

Pentti oli myös huolissaan yksityisyydensuojastaan. Hän vastasi avoimeen kysymykseen näin:

> *”Mielestäni on tärkeä pitää tietoturvastaan huolta. Jos tietokoneessani olisi virus, joka ei ulkoisesti näytä tekevän mitään se haittaisi minua silti, sillä tuntisin yksityisyyteni uhatuksi. Jos palvelun tarjoajani näkisi missä sivustoilla käyn ja milloin niin tuntisin yksityisyyteni uhatuksi ja loukatuksi sillä on oma asiani mitä tietokoneellani teen.” – Pentti*

Pentti käytti myös virustorjuntaohjelmana F-Securen ohjelmaa. Hän oli tehnyt kyselyä edeltävänä päivänä virustarkistuksen. Reitittimen salasanaa hän ei ollut vaihtanut, mutta verkon hän oli piilottanut. Mac – suodatusta hän ei nähtävästi ollut laittanut vastauksen perusteella. Verkon piilottaminen on kuitenkin jo hyvä askel. VPN -ohjelmaa Pentti ei käyttänyt. Hän ilmaisi huolensa avoimessa kysymyksessä, mutta nähtävästi hän ei ole tehnyt yksityisyyden suojaamisen isompia ratkaisuja. Puhelimessaan

hän ei käyttänyt virustorjuntaohjelmaa. Hänellä oli käytössään Applen merkkinen puhelin.

Pentillä oli myös samoja salasanoja käytössä eri palveluissa. Tämä on iso riski tietoturvan näkökulmasta. On hyvin tärkeää pitää jokaisessa eri palvelussa omat salasanansa. Markkinoilla on monia hyviä ohjelmia, joilla voi luoda hyviä ja vahvoja salasanoja, sen lisäksi itse ohjelma muistaa ne. Tällöin käyttäjän ei tarvitse itse muistaa kaikkia salasanoja.

6.2 Syksyn 2017 kyselytulosten analysointi

Tulemme käymään tässä kohdassa läpi syksyn 2017 kyselomakkeiden avulla kerätyt haastattelut aineistot. Syksyn 2017 kyselyyn osallistui kolme henkilöä, jotka ovat Matti, Pertti ja Tuomas. Tulokset käydään läpi parhaimmasta heikompaan.

6.2.1 Matin tulokset

Matti oli selvästi syksyn kyselyyn osallistuneista henkilöistä tietoisin tietoturvastaan ja siihen liittyvistä riskeistä. Kyselyssä olevaan avoimeen kysymykseen Matti vastasi seuraavasti:

> *”Tietoturva on minulle päivittäin työn ja kodin puolesta tärkeä asia. Töissä suojataan yhtiön tietoja mahdollisilta ryöstöiltä ja muilta uhilta. Kotona taas uhaksi koen enemmän tietokoneen lukittumisen aiheuttavat ohjelmat tai salasana vakoilut.”*
>
> *”Yksityidensuojaa tulisi erityisesti korostaa tietoturvissa. Niiden kattavuudesta ja varmuudesta olisi kiva ymmärtää enemmänkin.”*
>
> *”Minua haittasi ja häiritsee usein se tunne, että jokin virus saattaisi olla koneellani. Koen viikoittaiset erillisajot virusturvalla hyväksi keinoksi, itselleni varmistukseksi, ettei mikään virus ole sotkemassa elämää.”*
>
> *”Mielestäni internet palveluntarjoajalla ei missään nimessä kuulu millä sivuilla käyn ja milloin. Koen sen loukkauksena yksityisyyttäni kohtaan. Tästä syystä olen alkanut käyttää VPN-palveluita osittain.” – Matti*

Matti oli vastauksesta päätellen hyvinkin tietoinen mahdollisista tietoturvauhista. Suurimmaksi uhkaksi tietoturvalleen hän koki mahdolliset hyökkäykset hänen kotinsa tietokoneelle. Kotonaan Matti suojautui viruksilta käyttämällä Windowsin palomuuria sekä Malwarebytes-virustentorjuntaohjelmaa. Edellä mainitun Malwarebytes -ohjelman avulla Matti suoritti viikoittain virustarkistuksen tietokoneellaan, jotta hän välttyisi viruksilta ja muilta vakoiluohjelmilta. Tietokoneensa Matti oli suojannut hyvinkin mutta matkapuhelimessaan hänellä ei ollut minkäänlaista virustorjuntaa. Matti käytti myös monissa eri palveluissa samaa salasanaa, joka on mahdollisen virustartunnan yhteydessä iso riski. Tällöin monet eri käyttäjätilit ovat vaarassa joutua ulkopuolisten käsiin.

Matilla oli kotonaan myös käytössä langaton lähiverkko. Tämän verkon hän oli suojannut salasanalla ja WPA2-PSK:n avulla. Matilla ei ollut verkossaan käytössä muita suojauskeinoja kuin salasana. MAC-suodatuksessa kysyttäessä Matilla ei ollut mitään tietoa mikä tämä kyseinen suodatus oli. Matti ei ollut myöskään piilottanut langatonta verkkoaan jolloin uuden verkonkäyttäjän tulisi tietää salasanan lisäksi myös verkonnimi, jotta verkon käyttäminen olisi mahdollista.

Matti otti yksityisyytensä melko vakavan oloisesti. Matin mielestä internet-operaattorilla ei ole mitään oikeuksia tarkastella hänen selaushistoriaansa tai muita verkon tietoja. Matti koki tämän suurena loukkauksena yksityisyyttään kohtaan. Tämän takia Matti on siirtynyt osittain käyttämään VPN -ohjelmistoja, joiden avulla verkkoliikenne voidaan salata ja piilottaa palveluntarjoajan tarkasteluilta.

6.2.2 Tuomaksen tulokset

Tuomas piti tietoturvaa ja yksityisyyden suojaa tärkeänä. Hän tiedosti, että hänellä oli mahdollisia puutteita tietoturvan ja yksityisyyden suojaamisen saralla. Sen lisäksi Tuomas oli tietoinen, kuinka verkkokaupat käyttävät kerättyä dataa vierailijoista. Hän ei pidä siitä mihin dataa mahdollisesti tullaan käyttämään.

> *"Tietoturva on todella tärkeä ja joka päivä aina vaan ajankohtaisempi asia. Ihmisten tietoja tuntuu olevan liiankin helppoa kalastaa netistä nykypäivänä. Yritän yleensä pitää tietoni hyvin suojattuna, mutta voisin varmasti panostaa siihen enemmänkin.*
>
> *Ja kyllä, jos koneella on virus tai jokin muu "pienikään ongelma" mikä ei suoranaisesti tunnu vaikuttavan mihinkään niin kyllä se tuntuu ajavan hulluuden partaalle ennen kuin saan sen hävitettyä.*
>
> *Ja kyllä yksityisyys on tärkeää minulle ja inhottaa ajatus siitäkin, että verkkokaupat keräävät dataa haetuista tuotteista yms., vaikka ne muka on luotu helpottamaan shoppailua. Kaikki tietojen keruu tuntuu hämärältä ja epäilyttää aina mihin tietoja käytetään." - Tuomas*

Tuomas suoritti kyselyn ajankohtana viimeisimmän virustarkistuksen viikkoa ennen vastauksen antamista ja virustorjunta ohjelmana hän käytti Avast -nimistä ohjelmaa. Sen lisäksi hän mainitsi, että hän puhdisti konetta sinä aikana kaikesta "turhasta". Tämä voi viitata siihen, että Tuomas yrittää pitää konetta mahdollisimman puhtaana turhista tiedostoista ja ohjelmista. Tuomas oli vaihtanut modeemin salasanankin muutamaan otteeseen, joka voi yleensä unohtua monilta.

Tuomas oli myös jättänyt laittamatta MAC-suodatuksen päälle langattomaan verkkoon. Hänen kommentti kysymykseen neljä:

> *"Käytän langatonta verkkoa. MAC-suojaus pitäisi laittaa todennäköisesti päälle, mutta mielikuva on, että siitä syntyisi ylimääräistä vaivaa. Edelleen: pitäisi kyllä varmasti laittaa se päälle!" - Tuomas*

Hän oli kuitenkin tietoinen, että MAC-suodatuksen laittaminen voi aiheuttaa hieman ylimääräistä vaivaa. Sen lisäksi hän tiedosti, että kyseisen ominaisuuden laittaminen olisi hyödyllistä. Yksityisyyden suojaa Tuomas ei ollut edistänyt millään ohjelmistolla. Hän käytti välillä VPN-yhteyttä koulutehtävien tekemiseen. Tämän lisäksi hänellä ei ollut puhelimessa mitään virustorjuntaohjelmaa. Tästäkin hän oli tietoinen ja ollut aikeissa paneutua asiaan tarkemmin.

Tuomas käytti samoja tai lähes samoja salasanoja muutamassa palvelussa. Yleisesti ottaen hän on pyrkinyt laittamaan eri salasanat jokaiseen palveluun.

6.2.3 Pertin tulokset

Pertti oli syksyn kyselyn tiedottomin tietoturvansa osalta. Pertillä oli kuitenkin aivan perusasiat halussa ja tietoisuutta, miten suojautua internetissä mahdollisista viruksilta ja huijauksilta. Avoimeen kysymykseen Pertti vastasi seuraavalla tavalla:

> *”Kukapa nyt tietokoneelleen viruksia haluaisi? Tämän takia käytänkin montaa eri virustorjunta ohjelmaa. Nykypäivänä olisi myös hyvä käyttää VPN-ohjelmia suojatakseen yksityisyyttään.” – Pertti*

Pertillä tietämys tietoturvasta oli vastausten perusteella hyvin perustasolla. Pertti oli osannut suojautua mahdollisilta uhiltaan kotona mutta ei sen tarkemmin tiedä miltä virustorjuntaohjelmat varsinaisesti suojaavat, hän oli ladannut kyseiset ohjelmat vain koska tämä on yleinen suositus.

Tietokoneellaan Pertillä oli käytössä monta eri virustorjuntaohjelmaa. Nämä ohjelmat ovat Avast, Windows palomuuri sekä Malwarebytes. Pertti otti kumminkin tietoturvansa tosissaan, vaikka tietämystä uhkista ei hirveästi ole. Pertillä oli käytössään siis kolme eri ohjelmaa, joiden avulla hän tarkasti tietokoneensa hyvinkin epäsäännöllisin välein. Pertti käytti virustorjuntaohjelmaa myös matkapuhelimessaan. Pertti käytti samoja salasanoja monessa eri palveluissa, joka on hyvin iso riskitekijä hyökkäyksen sattuessa.

Oman langattoman lähiverkkonsa Pertti oli suojannut salasanalla mutta hän ei ollut ikinä vaihtanut salasanaa. Pertillä ei ollut tietoa mikä on MAC -suodatus ja miten sitä tulisi käyttää.

Perttiä ei haitannut internet-operaattorin mahdollinen selaushistorian tai muiden verkon tietojen urkinta. Pertti ei myöskään tämän takia käyttänyt VPN -ohjelmistoja suojatakseen liikenteensä.

7 VERTAILU HENKILÖIDEN KESKEN JA PÄÄTELMÄ

7.1 Kevään henkilöiden vertailu

Erkki huolehti tietoturvasta parhaiten näistä kolmesta henkilöstä. Hän tiedosti tulevaisuuden riskit (Internet of Things) ja sekä oli kyselyn aikana suojautunut parhaiten tietoturvauhilta. Hänellä oli Mac-suodatus päällä reitittimessä ja hän osasi varautua tulevaisuuden riskeihin.

Pekka tuli toiseksi, sillä hän oli jättänyt Mac –suodatuksen tekemättä. Pekka oli hieman kriittisempi yksityisyydensuojastaan ja sekä oli tietoinen, kuinka hänestä kerättyä tietoa voidaan käyttää hyväksi. Yksityisyyden suojan perusteella Pekka sai parhaimmat pisteet. Sillä hän käytti VPN -ohjelmaa normaali internet selailussa, jonka takia hänestä ei saada kerättyä tietoa, hänen yhteytensä on salattu ja suojattu vahvasti.

Heikoiten tietoturvasta huolehti Pentti. Hän ei ollut vaihtanut salasanaa reitittimeen tai laittanut Mac -suodatusta päälle. Sen lisäksi hän ei käyttänyt mitään ohjelmaa minkä avulla hän salaisia internetin selailua.

Kaikki kolme henkilöä käytti hyviä virustorjuntaohjelmia tietokoneillansa. F-secure on luotettava ja sekä suomalainen yritys, joka nostattaa luottamusta kyseisestä ohjelmasta. Hyvällä virustorjuntaohjelmalla kuitenkin jo pääsee melko pitkälle.

7.2 Syksyn henkilöiden vertailu

Syksyn tuloksissa tuli samanlaisia piirteitä esiin kuin kevään tuloksissa. Matti huolehti syksyn kyselyssä parhaiten tietoturvasta ja yksityisyydensuojastaan. Tämä näkyi myös Matin työelämässä, sillä hän joutui huolehtimaan yrityksensä tietoturvasta töissäkin. Hän välitti yksityisyyden suojastaan ja edisti asiaa käyttämällä VPN -ohjelmistoa.

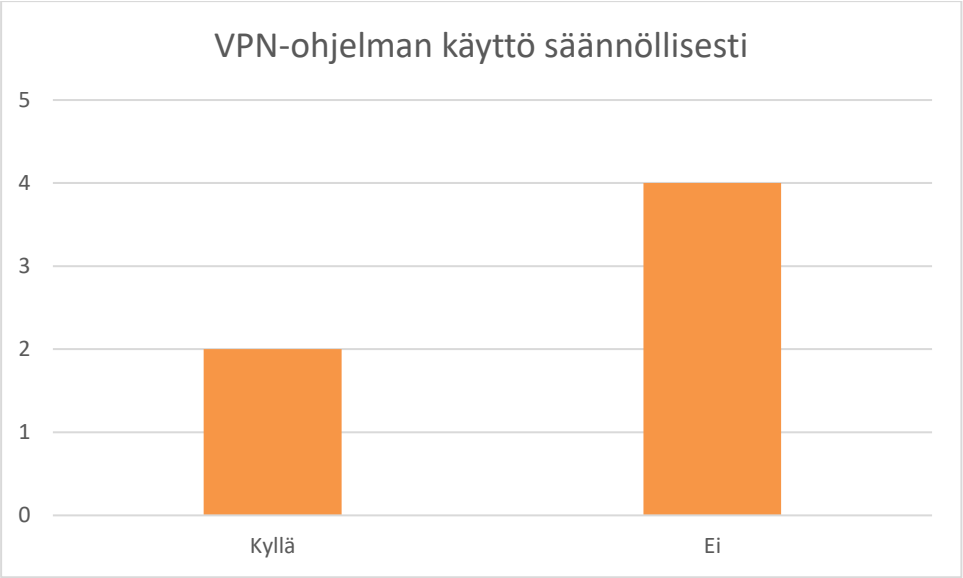
Tuomaksella oli yleisesti tietoturva hallussa perustasolla. Hän käytti yleistä virustorjuntaohjelmaa, oli vaihtanut modeemin salasanan ja pyrki käyttämään eri salasanoja eri palveluissa.

Pertin tietämys oli syksyn kyselyssä heikoimmalla tasolla, vaikka häneltäkin löytyi kyllä jonkin verran tietämystä. Pertti otti mahdolliset uhkatekijät vakavasti, sillä hänellä oli käytössä monia virustorjuntaohjelmistoja. Pertti ei niinkään välittänyt hänen tietojensa yksityisyydestä. Hän ei täten myöskään käytä VPN -ohjelmistoa eikä koe sitä tarpeelliseksi. Pertti oli myös syksyn kyselyn henkilöistä ainoa, joka käytti jonkinlaista ohjelmistoa suojatakseen matkapuhelintaan.

Syksyn tuloksissa tuli ilmi, ettei kukaan haastateltavista käyttänyt MAC-filtteröintiä. Kevään kyselyssä pelkästään yksi käytti kyseistä ominaisuutta. Matti oli ainoa henkilöistä, joka huolehti myös yksityisyyden suojastaan, Pentti oli kuitenkin valmis hankkimaan VPN-ohjelmiston. Jokainen vastaajista sanoi käyttävänsä samoja salasanoja joissakin palveluissa. Matti ja Tuomas käyttivät harvemmin samoja salasanoja, kun taas Pentti hieman yleisemmin. Yleisesti ottaen syksyn kyselyssäkin jokainen vastaajista käytti yleisesti tunnettua virustorjuntaohjelmaa ja yksityisyyden suojaaminen jäi hieman enemmän taka-alalle.

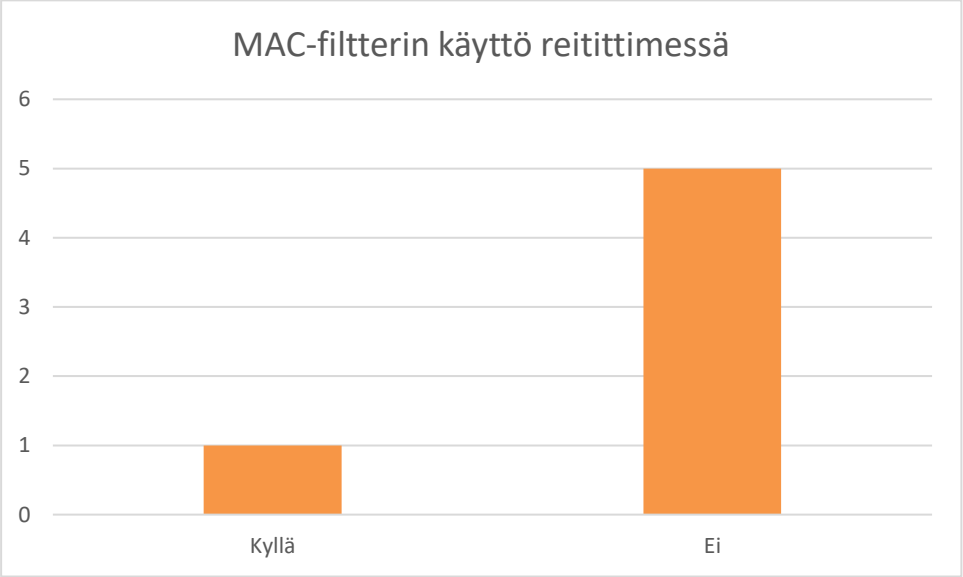
7.3 Loppupäätelmä

Kyselylomakkeen avulla saimme kerättyä hyvin tietoa tutkimuskysymykseemme, joka oli: ”Kuinka tietoturvasta ja yksityisyyden suojasta huolehditaan sekä miten sitä edistetään? ”. Kyselyssä tuli ilmi erilaisia keinoja, joita vastaajat käyttivät tietoturvan huolehtimisessa.



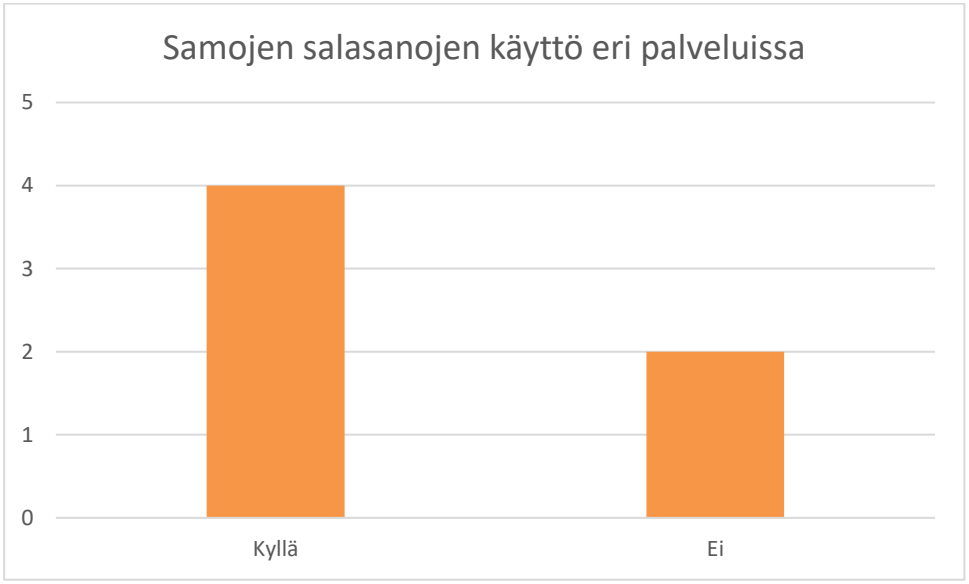
Kaavio 1. VPN-ohjelman käyttö säännöllisesti

Kyselyyn osallistuneista pelkästään kaksi henkilöä käytti säännöllisesti VPN -ohjelmaa. Tämä tarkoittaa sitä, että suurin osa ei välttämättä huolehdi yksityisyydensuojaamisesta niin paljon. Yksi vastaajista myös mainitsi, ettei häntä haittaa, vaikka internet-operaattori voisi mahdollisesti seurata hänen verkon käyttöään. Suurin osa vastaajista kuitenkin tiedosti yksityisyyden suojan tärkeyden, muttei ole välttämättä tehnyt asian edistämiseksi vielä mitään.



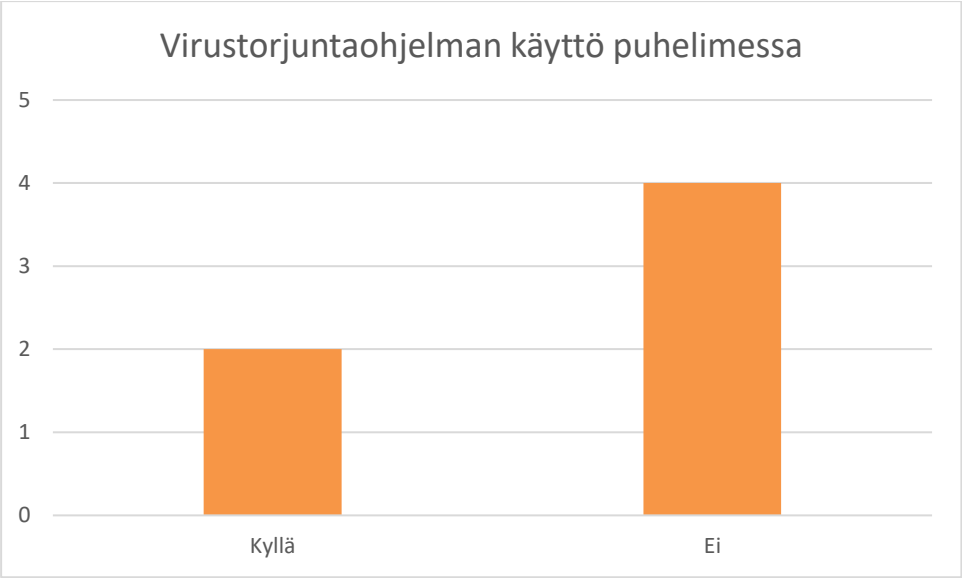
Kaavio 2. MAC-filtterin käyttö reitittimessä

Kyselyssä tuli ilmi, että vastaajista pelkästään yksi henkilö käytti MAC-filtteri ominaisuutta reitittimessä. Osa vastaajista ei tiennyt mikä kyseinen ominaisuus on. Ominaisuuden käyttöönottaminen on helppoa ja yksinkertainen tapa parantaa langattoman verkon suojausta. Kyseisen ominaisuuden saa laitettua päälle reitittimen asetuksista. Yleensä reitittimen valmistaja on tehnyt ohjeet, jossa käydään läpi askel kerrallaan tarvittavat toimenpiteet.



Kaavio 3. Samojen salasanojen käyttö eri palveluissa

Vastaajista neljä henkilöä käytti samoja salasanoja eri palveluissa. Tämä on todella iso riski, sillä tietoturvamurtoja palveluihin tapahtuu hyvin usein. Samojen salasanojen käyttö on helppo välttää käyttämällä salasanan hallintaohjelmia. Salasanojen hallintaohjelmia on saatavilla useita erilaisia, niin maksullisia kuin ilmaisiakin. Tällöin voi helposti käyttää eri salasanoja eri palveluissa ilman, että jokainen salasana pitää muistaa ulkoa. Viestintäviraston raportissa tämä mainittiin olevan yksi suurin uhka yksityishenkilöillä.



Kaavio 4. Virustorjuntaohjelman käyttö puhelimessa

Älypuhelimien yleistymisen myötä olisi todella tärkeää käyttää virustorjuntaohjelmia puhelimissakin. Kyselyyn vastanneista pelkästään kaksi henkilöä käytti virustorjuntaohjelmaa puhelimessaan. Viestintäviraston raportissa painotetaan puhelimien virustorjunta ohjelmista, jotka ovat oikeastaan välttämättömiä, jos haluaa huolehtia tietoturvastaan.

Kyselyssä tuli ilmi, että jokainen vastaajista käytti virustorjuntaohjelmia koneillansa. Useimmilla oli perus virustorjuntaohjelman lisäksi muita apuohjelmia, joiden avulla tietokoneiden tietoturvaa parannettiin. Tätäkin oli painotettu paljon Viestintäviraston raportissa.

8 JOHTOPÄÄTÖKSET

Rajoitukset tutkimuksessa olivat aineiston laajuus. Tutkimuskohteita olisi ollut parempi olla enemmän, jotta pystyisi yleistämään varmemmin tutkimuksen tuloksia. Tällä kertaa oli vain kuusi henkilöä, jotka olivat eri ääripäistä. Sillä tavalla tuli ilmi erilaisuudet vastaajien kesken, kuinka he suhtautuvat tietoturvaa ja miten he edistivät sitä. Haastattelut olisivat olleet hyviä, mutta siihen ei löytynyt sopivia aikoja jotka olisivat käyneet vastaajille ja sekä meille. Mielestämme tutkimus onnistui hyvin, sillä saimme hyviä vastauksia tutkimuskysymykseen.

Tutkimuksen validiteetti on hyvä, sillä kysyimme vastaajilta sellaisia kysymyksiä millä pystyy vertaamaan, kuinka he huolehtivat omasta tietoturvastaan ja yksityisyyden suojasta. Tällä tavalla saimme vastauksia siihen mihin alun perin halusimme. Tutkimuksen reliabiliteettia on vaikea arvioida, sillä se riippuu niin paljon haastateltavista. Voi käydä niin, että jonkin toisen tutkimuksen vastaajista moni huolehtiikin todella hyvin tietoturvasta ja yksityisyyden suojasta. On melko todennäköistä, että suurin osa ei huolehdi niin paljon. Joten tämän tutkimuksen tulokset tulevat todennäköisesti toistumaan, eli ihmiset saattavat käyttää samoja salasanoja palveluissa tai ei muuta reitittimen oletussalasanaa jne.

Tutkimuksen yleistäminen näin pienellä otoksella ei ole mahdollista, sitä varten tarvitsisi laajemman otoksen jossa voitaisiin varmistaa virhemarginaali ja erilaiset heitot.

Tutkimuksessamme tuli ilmi, että jokainen vastaaja käytti hyviä virustorjuntaohjelmia koneillansa ja sekä yksi myös varmuuskopio säännöllisesti konettansa. Tutkimusmateriaalistamme kävi hyvin ilmi vastaajien heikkouksia ja vahvuuksia. Kyseisiä heikkouksia ja vahvuuksia oli mahdollista havaita aikaisemmista tutkimuksista. Osa vastaajista käytti siis samoja keinoja tietoturvan edistämiseen, joita viestintävirastokin suositteli. Samalla kuitenkin vastaajilla oli samoja heikkouksia, joita mainittiin Viestintäviraston ja Travels Risk -raporteissa.

On siis hyvin tärkeää, että ihmiset ottaisivat tosissaan tietoturvansa haavoittuvuudet ja huomioisivat yksityisyyden suojansa. Tulevaisuudessa meno tulee olemaan vielä hurjempi, sillä teknologia kehittyy kovaa vauhtia. Tämä tulee altistamaan entistä enemmän erilaisille tietoturvauhille. Tulevaisuuden tutkimuksiin suosittelemme ottamaan enemmän selvää juurikin IoT-laitteista ja niiden tietoturvasta. Sekä yksityisyyden suojaamisesta olisi hyvä käydä läpi enemmän VPN -ohjelmia. Esimerkiksi Yhdysvalloissa nostettiin esille vuonna 2017 sellainen laki, joka mahdollistaisi internet-operaattoreiden kerätä käyttäjistänsä tietoa ja myydä heidän selailutiedot eteenpäin kolmansille osapuolille (USA Today 2017). Tämän pystyy helposti välttämään VPN -ohjelmien avulla, jotka piilottavat ja salaavat ihmisten selailua internetissä. VPN -ohjelmat tulevat yleistymään todennäköisesti räjähdysmäisesti tulevaisuudessa.

LÄHTEET

Cloudmask. 2017. Is data security more important to consumers than physical well-being? [Verkkolehti] [Viitattu 13.1.2017]. Saatavissa: https://www.cloudmask.com/blog/encryption/is-data-security-more-important-to-consumers-than-physical-well-being

Kali Linux Official Documentation. 2017. What is Kali Linux? [viitattu 20.11.2017]. Saatavissa:

https://docs.kali.org/introduction/what-is-kali-linux

Koskinen, P. 2017. Autojen mustat laatikot voivat rikkoa yksityisyyden suojaa – Professori: Riippuu siitä, miten laitetta käytetään. Yle. [Verkkolehti]. [Viitattu 20.1.17]. Saatavissa: http://yle.fi/uutiset/3-9389773?origin=rss

Kurittu, A. 2015. Tietoturvallisuustilanteen kartoitustyökalu pienille yrityksille. [Verkkodokumentti]. Helsinki: Elinkeinoelämän keskusliitto EK ja Viestintävirasto. [Viitattu 15.10.2017]. Saatavissa:

https://ek.fi/ajankohtaista/uutiset/2015/06/22/kaytannonlaheinen-tietoturvaopas-pk-yritysten-arkeen/

Mansikka, O. 2017. Hakkeriyhteisö sanoo löytäneensä puutteita autoihin asennettavan ”mustan laatikon” tietoturvasta – Trafi testannut vastaavia laitteita. Helsingin Sanomat. [Verkkolehti]. [Viitattu 20.1.17]. Saatavissa: http://www.hs.fi/kotimaa/art-2000005046813.html

Palmolahti, H & Okkonen, K-M. 2017. Yksityisyyden suoja. [Viitattu 13.1.2017]. Saatavissa: http://toimittajanrikoslaki.fi/yksityisyydensuoja/

Saarimäki, J. 2017. Tietoturvan vuosi 2016. [Verkkodokumentti]. Helsinki: Viestintävirasto. Viestintäviraston julkaisu 001/2017 J. [Viitattu 8.2.2017]. Saatavissa: https://www.viestintavirasto.fi/attachments/tietoturva/Tietoturvan-vuosi_2016_ViVi_29-11-2017_L.pdf

Snider, M. 2017. ISPs can now collect and sell your data: What to know about Internet privacy rules. USA Today. [Verkkolehti]. [Viitattu 27.11.2017]. Saatavissa:

https://www.usatoday.com/story/tech/news/2017/04/04/isps-can-now-collect-and-sell-your-data-what-know-internet-privacy/100015356/

Stackskills. 2017. Learn Ethical Hacking From Scratch. [Viitattu 20.11.2017]. Saatavissa (Maksullinen):

https://stackskills.com/courses/learn-ethical-hacking-from-scratch/lectures/1353330

STT. 2017. THL:ltä vuoti verkkoon 6 000 ihmisen henkilötiedot ja laboratoriokokeen tulokset – "Möhlitty on". Etelä-Suomen Sanomat. [Verkkolehti]. [Viitattu 15.10.2017]. Saatavissa:

http://www.ess.fi/uutiset/kotimaa/art2402924

Travelers. 2015. Consumer Risk Index: An annual survey of the risks Americans believe are most prevalent in their lives. [Verkkodokumentti]. [Viitattu 13.1.2017]. Saatavissa: https://www.travelers.com/iw-documents/resources/consumer-risk-index/2015-report.pdf

Viljanen, V. 2017. Verkkourkinta. [Viitattu 15.10.2017]. Saatavissa:

https://www.yksityisyydensuoja.fi/verkkourkinta

LIITTEET

Kyselylomake:

Kerro lyhyesti mielipiteesi tietoturvasta ja yksityisyydensuojasta. Esimerkiksi haittaako sinua, jos koneellasi on virus, joka ei ulkoisesti näyttäisi tekevän mitään? Haittaako sinua, jos internet palveluntarjoajasi voi nähdä kaiken tiedon missä sivustoilla olet käynyt ja milloin?

Muut kysymykset.

1. Mitä virustorjunta ohjelmaa käytät?
2. Milloin viimeksi teit virustarkistuksen?
3. Oletko vaihtanut modeemisi/reitittimesi salasanaa?
4. Käytätkö langatonta verkkoa kotona? Jos käytät, oletko esim. laittanut MAC-suodatusta päälle tai piilottanut verkon?
5. Käytätkö VPN-ohjelmia tietokoneellasi tai puhelimessasi?
6. Oletko laittanut virustorjunta ohjelmaa puhelimeesi?
7. Käytätkö samoja salasanoja eri palveluissa?