Opinnäytetyö (AMK)

Tietojenkäsittely

Yrityksen tietoliikenne ja tietoturva

2017

Toni Tihleman

WINDOWS-YMPÄRISTÖN TIETOTURVALLISUUS KOTIKONEELLA

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Yrityksen tietoliikenne ja tietoturva

2017 | 23

Toni Tihleman

WINDOWS-YMPÄRISTÖN TIETOTURVALLISUUS KOTIKONEELLA

Tämä opinnäytetyö käsittelee tietoturvallisuutta Windows-ympäristössä. Keskeisenä teemana on erilaisten tietoturvariskien läpikäynti ja niiltä suojautuminen. Tavoitteena oli saada yksinkertaisia malleja oman kotikoneen tietoturvan parantamiseksi.

Teoriaosuudessa käydään läpi tietoturvaa ja Windowsia yleisesti, sekä syvennytään lähemmin monimuotoisiin verkossa ja laitteissa oleviin tietoturvariskeihin. Tämän jälkeen teoriaosuudessa siirrytään käsittelemään myös oikeanlaisia riskeiltä suojautumisen keinoja.

Tutkimuksessa käytettiin Windows-tietokonetta, jonka avulla selvitin ja analysoin suurimmat tietoturvariskit, ja miten tietokoneen suojausta voisi parantaa. Tutkimuksessa ilmeni, että salasanojen hallinta ja virustorjunta ovat suurimmat riskitekijät. Tästä syystä opinnäytetyöni soveltuu hyvin myös kaikille muille Windows-tietokoneen käyttäjille, jotka haluavat selvittää, miten oman koneen tietoturvaa voisi parantaa.

ASIASANAT:

Windows, tietoturva, virustorjunta, palomuuri

BACHELOR´S / MASTER'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Business Data Communication and Information Security

2017 | 23

Toni Tihleman

INFORMATION SECURITY IN WINDOWS ENVIRONMENT FOR HOME COMPUTERS

This thesis deals with information security in the Windows environment. The key theme is the screening and protection of various security risks. Aim to get simple models to improve your home computer's security.

The theoretical part is about security across the board and Windows in general, as well as a deepening of the security risks associated with complex networks and devices. After that, the theory section will also go into dealing with the right kind of protection measures.

In my research, I used a Windows computer to find out and analyze the major security risks and how to improve the security of my computer. For this reason, my thesis is well suited to all other Windows computer users who want to find out how to improve the security of the computer.

KEYWORDS:

Windows, information security, antivirus, firewall

SISÄLTÖ

KÄYTETYT LYHENTEET TAI SANASTO.

FTP	File Transfer Protocol. Tiedonsiirto protokolla.
HTTP	Hypertext Transfer Protocol. Hypertekstin siirtoprotokolla.
IP	Internet Protocol. Internet protokolla.
PGP	Pretty Good Privacy. Tietojen salaus järjestelmä.
RAM	Random Access Memory. Keskusmuisti.
SSH	Secure Shell. Salattuun tietoliikenteeseen tarkoitettu protokolla.
SSL	Secure Sockets Layer. Tietoverkkosalausprotokolla.
VPN	Virtual Private Network. Virtuaalinen erillisverkko.
WLAN	Wireless Local Area Network. Langaton lähiverkko.

1 JOHDANTO

Tietoturvallisuus on noussut yhä tärkeämmäksi elementiksi, niin yrityksien, kuin kotikäyttäjienkin näkökulmasta. Internetissä piilee valtava määrä erilaisia tietoturvariskejä ja niiltä täytyy osata suojautua asianmukaisesti.

Tämän opinnäytetyön tarkoituksena on selvittää millaisia tietoturvariskejä kotikäyttäjä kohtaa ja miten niiltä voi suojautua oikein. Erilaiset tietoturvariskit ovat arkipäiväistyneet internetin kasvun myötä ja riskejä on yhä enemmän, jopa tavallisella kotikäyttäjällä. Tämän työn teoriaosuudessa käydään läpi tietoturvallisuutta monelta puolelta ja tutkitaan yleisimmät tietoturvariskit, sekä tavat, miten niiltä voidaan suojautua.

Olen lähtenyt tutkimaan aihetta kartoittamalla Windows-tietokoneen suojaustason ja tietoturvariskit, sekä etsinyt tietoa useista eri kirjallisuus ja -verkkolähteistä. Työtä voi siis huoletta soveltaa jokaiselle kotikoneen käyttäjälle, jos tarkoituksena on selvittää oman koneen tietoturvariskejä.

Valitsin aiheen, koska olen kiinnostunut tietoturva-asioista ja ne ovat tänä päivänä erittäin tärkeä osa jokapäiväistä arkea ja tietokoneen turvallista käyttöä.

2 WINDOWS

Microsoft Windows on varmasti jokaiselle kotikoneen käyttäjälle erittäin tuttu käyttöjärjestelmä. Sen historia juurtaa vuodelle 1985 asti, jolloin ensimmäinen Windows (MS-DOS) lanseerattiin. Windows on graafisten käyttöjärjestelmien tuoteperhe, joita on vuosien varrella julkaistu monia eri versioita. Vuonna 2014 Windowsin markkinaosuus kaikista tietokoneen henkilökohtaisista käyttöjärjestelmistä oli 88,12 %. Windows teki alkujaan IBM:n kanssa paljon yhteistyötä, jolla yritettiin parantaa kilpailumahdollisuuksia Applen Macintosh-koneita vastaan. Vuonna 1981 syntyi Microsoftin ensimmäinen MS-DOS käyttöjärjestelmä, joka oli nimenomaan suunnattu IBM PC-koneiden käyttöön. MS-DOS käyttöliittymä oli tekstipohjainen. (Wikipedia 2017.)

Windowsin tietoturva on yleisesti kritisoitu, mutta se johtunee enemmänkin siitä, että Windows on niin yleinen käyttöjärjestelmä maailmanlaajuisesti, joten luonnollisesti siihen kohdistuvat uhat ovat merkittävän suuret. Kaikesta huolimatta Windowsin eri versiot sisältävät valtavasti erilaisia suojautumiseen tarkoitettuja ohjelmia. Windowsissa on sisäänrakennettu palomuuri ollut jo monia vuosia. Virustorjuntaan on saatavilla Microsoft Essentials (Windows 7) joka on yksinkertainen virustorjuntaohjelma. Uusimpaan Windows 8 ja 10 -versioihin on saatavilla ”Windows Defender” niminen ohjelma, joka on jo huomattavasti Essentialsia monipuolisempi. Windowsin omien päivitysten yhteydessä tulee myös valtavasti erilaisia tietoturva-aukkoihin liittyviä korjauksia ja parannuksia, joten päivitysten tulee olla kunnossa. (Webtieto 2017.)

3 TIETOTURVA

Tietoturvan tarkoitus on pyrkiä suojaamaan yrityksille ja yksityishenkilöille tärkeät tiedot ulkopuolisilta. Kysymys on siis toimenpiteistä, jotka takaavat tietojen koskemattomuuden ja muuttumattomuuden. Tietoturvalle on asetettu kolme eri tavoitetta, joita ovat: luottamuksellisuus, eheys ja kiistämättömyys. Tiedot ovat luottamuksellisia vain mikäli ne ovat niiden ihmisten käytössä, joilla niihin on tarvittavat käyttöoikeudet. Tiedoilla ja dokumenteilla on turvaluokitus, joka määrittelee sen, kenellä on oikeus tietojen käyttöön, muuttamiseen ja tuhoamiseen. (Suomen internetopas 2015.)

Usein tieto on luokiteltua, joten sitä ei ole tarkoitus olla kaikkien saatavilla. Tämä tarkoittaa käytännössä sitä, että vain tietyillä henkilöillä tai tahoilla on oikeus päästä käsiksi johonkin tiettyyn tietoon. Luottamuksellisuus syntyy siis siitä, että oikeaa tietoa käsittelee oikeat henkilöt. Tätä valvotaan ja kontrolloidaan käyttöoikeuksia jakamalla. Niin, että käyttöoikeudet jaetaan koskemaan vain niitä työtehtäviä, joita on tarpeen tehdä. Mikäli käyttöoikeuksia pääsee tietovuodon myötä verkkorikollisille, se voi aiheuttaa merkittäviä vahinkoja ja olla iso särö luottamuksellisuuteen. (Rousku 2014, 47-48)

Tiedon eheys tarkoittaa tiedon muuttumattomuutta. Tieto saa muuttua vain oikean käyttöoikeuden haltijan toimesta. Ongelmien ilmaantuessa tiedot tulee myös olla palautettavissa helposti ja nopeasti. (Rousku 2014, 49)

Saatavuudella tarkoitetaan, että tiedot pitää olla käytettävissä aina, kun niitä tarvitaan. Palvelut yritetään pitää käynnissä vuorokauden ympäri lukuun ottamatta huoltokatkoja. Verkkorikolliset ovat kehitelleet paljon palvelujenestohyökkäyksiä tietojen saatavuutta vastaan. (Rousku 2014, 50)

3.1 Tietoturva internetissä

Internet on lukemattomien aliverkkojen muodostama maailmanlaajuinen tietoliikenneverkko. Internet ei siis ole yksittäinen tietoverkko, eikä myöskään ainoa olemassa oleva tietoverkko. Internet on nimitys kaikkien yhteen liittyneiden palvelimien ja yksityisten käyttäjien muodostamalle globaalille tietoverkolle.

Internetin runko muodostuu palvelimista eli servereistä. Palvelin on teknisesti tavallista pöytätietokonetta muistuttava tietokone, jossa on kovalevy ja RAM-muisti, minkä avulla

ohjelmat suoritetaan. Palvelimet sisältävät internetissä esitetyn tiedon ja kaikki käyttäjälle tarjotut palvelut, joten palvelimelta vaaditaan paljon suurempi muistikapasiteetti, kuin tavalliselta tietokoneelta. Palvelinkoneet on kytketty toisiinsa nopean tietoliikenneyhteyden mahdollistavilla kaapeleilla. Palvelimet ovat usein osa jotakin pienempää lähiverkkoa, joka koostuu esimerkiksi jonkin oppilaitoksen tai yrityksen lähiverkkoon kytketyistä tietokoneista.

Kun käyttäjä muodostaa yhteyden Internetiin esimerkiksi selainohjelmalla, ottaa selain yhteyden palvelinkoneessa olevaan palvelinohjelmistoon. Palvelinohjelmisto lähettää palvelupyynnön kun Internet-sivun avaa ja vastaanottaa palvelimen palauttaman tiedon sekä tulostaa sen käyttäjälle, eli näytölle avautuu haettu internet-sivu. Yhteyden muodostaminen Internetiin tarkoittaa siis yhteyden muodostamista palvelimelle, josta voidaan edelleen muodostaa yhteys muihin palvelimiin. (Wikipedia 2015.)

Tietoturva on noussut erittäin keskeiseen asemaan myös verkossa. Verkossa on mahdollista muunnella internet-sivustojen tietoja, uudelleen ohjata hakuja vääriin osoitteisiin, lähettää sähköpostia väärillä tiedoilla ja nimillä, etsiä rikollisin tarkoituksin muiden käyttäjätunnuksia, salasanoja sekä luottokorttien tietoja. Huonosti ja puutteellisesti toteutetusta tietoturvasta mahdollisia seurauksia ovat virusten tai ulkopuolisten henkilöiden tunkeutumiset tietojärjestelmiin, verkkoihin ja niiden sisältämien tietojen väärinkäytökset tai tuhoamiset. (Suomen internetopas 2015.)

3.2 Tekninen tietoturva

Tekninen tietoturva keskittyy siihen, että käytetyissä laitteissa ja ohjelmistoissa ei ole tietoturva-aukkoja. Tietoturvaa on siis hyvä miettiä jo ennen verkkolaitteiden ja muiden ohjelmien hankintaa. Tietojärjestelmiin pääsyä ja siellä olevien tietojen säilyttämistä luottamuksellisina valvotaan salasanojen ja käyttäjätunnuksien avulla. Käyttäjätunnusten avulla määritellään käyttäjille käyttöoikeudet, jotka määrittelee sen, mihin tietoihin käyttäjällä on oikeus päästä.

Käyttäjätunnukset ja salasanat eivät kuitenkaan ole parhaimpia tietoturvaratkaisuja, sillä salasanojen arvausohjelmat ovat kehittyneet hurjasti ja salasanojen haltuun saaminen tiedonsiirron aikana on muodostunut kohtuullisen helpoksi. Suurempiin tietoverkkoihin yhteyksissä olevissa lähiverkoissa on hyvä varmistua siitä, etteivät mahdolliset verkkorikolliset pääse suoraan käsiksi sisältöön. Hyviä varmistuskeinoja ovat erilai-

set palomuuriratkaisut sekä käsiteltävän tiedon salaaminen eli kryptaaminen, mikä tarkoittaa sitä, että tieto muutetaan lukukelvottomaksi. Tiedon voi avata vain käyttäjä, jolla on käytössä samanlainen, mahdollisesti jopa 128 merkkiä pitkä numerosarja, eli koodiavain. (Suomen internetopas 2015.)

3.3 Fyysinen tietoturva

Fyysinen tietoturva yksinkertaisuudessaan tarkoittaa suljetussa tilassa olevia tietokoneita ja niiden fyysistä turvallisuutta. Lukitulla tilalla varmistetaan, ettei kenelläkään ulkopuolisella ole pääsyä koneisiin, kiintolevyihin tai muuhun tiedontallennusmediaan. Fyysistä tietoturvaa on myös esimerkiksi oikein toteutetut paloturvallisuusratkaisut. (Suomen internetopas 2015.)

3.4 Hallinnollinen tietoturva

Hallinnollinen tietoturva tarkoittaa työntekijöiden ja organisaation henkilöstön riittävää tietoturvaosaamista. Organisaation jäsenten tulee ymmärtää, että salasanoja pitää käsitellä varoen ja huolellisesti. Niitä ei ole järkevää kirjoittaa lapuille tai säilyttää sellaisten henkilöiden ulottuvilla, joilla ei ole mitään asiaa kyseisiin tietoihin. Salasanojen huolellinen käyttö pitää huolen siitä, että riskitekijät ovat pienempiä jos ulkopuoliset yrittävät murtautua organisaation tietoturvajärjestelmiin. (Suomen internetopas 2015.)

4 TIETOTURVARISKIT

Vaikka Windows-käyttöjärjestelmän myyntimäärät ovat vähentyneet, on se silti kotikoneiden suosituin käyttöjärjestelmä. Käsittelen tässä luvassa niihin liittyviä tietoturvariskejä.

4.1 Virukset

Virukset ovat yleisimpiä ja suurimpia riskejä varsinkin kotikäytössä. Virukset ovat pieniä tietokoneohjelman kaltaisia ohjelmia, jotka leviävät joko verkkoselaimen, sähköpostin liitetiedostoina tai erilaisten levykkeiden välityksellä koneesta toiseen käyttäjän huomaamatta. Virukset pystytään jakamaan useaan alaryhmään. PC-laitteille tavallisimpia viruksia ovat erilaiset makro- ja käynnistyslohkovirukset.

Viruksen perustoiminta koostuu joko yhdestä tai useammasta eri vaiheesta. Ensimmäisessä vaiheessa tyypillisesti virus ainoastaan levittää itsestään kopioita. Virus voi kopioida itsensä tietokoneessa käytettäville eri medioille. Mahdollisessa toisessa vaiheessa tapahtuu viruksen aktivoituminen. Jotkin virukset eivät sisällä kuin ainoastaan leviämisosan ja eräät virukset aktivoituvat vasta leviämisensä yhteydessä. Osa viruksista on tehty odottamaan tietty aika ennen leviämistä.

Yleisin vahinko, minkä virukset pääsevät tekemään, päästyään tietokoneeseen, on tietojen tuhoaminen. Virus voi esimerkiksi tyhjentää kovalevyn. Tässä tapauksessa tiedot tai tiedostot ei ole kuitenkaan fyysisesti kadonnut kovalevyltä ja tiedostot on mahdollista palauttaa erilaisilla apuohjelmilla.

Toinen ja paljon tuhoisampi tapa virukselle on toimia täysin näkymättömänä, mutta kirjoittaa vähän kerrallaan kovalevylle roskakoodia, jolloin viruksen havaitseminen on erittäin vaikeaa ja tuhot usein suurempia, koska varmuuskopiotkin saattavat olla saastuneita. Ylikirjoitettuja tietoja ja tiedostoja ei voi mitenkään palauttaa. Virus saattaa myös sotkea tietokoneen muistia, jolloin käyttöjärjestelmän toimintaan voi tulla häiriöitä ja kone alkaa käyttäytyä hyvin epävakaasti. (Virustorjunta 2015.)

4.2 Laitteisto ja ohjelmat

Vaikka Windows käyttöjärjestelmän myyntimäärät ovat vähentyneet, on se silti kotikoneiden suosituin käyttöjärjestelmä. Käsittelen nyt niihin liittyviä tietoturvariskejä ja keinoja suojautumiseen. Mikäli käytössä on vielä Windows-XP käyttöjärjestelmän, niin sen käyttö kannattaa lopettaa välittömästi. Microsoft ei julkaise enää uusia tietoturvapäivityksiä kyseiselle käyttöjärjestelmälle, joten se on todellinen uhka tietoturvalle. Windows-XP käyttöjärjestelmä tulee päivittää joko Windows7 –käyttöjärjestelmään tai poistaa XP-käyttöjärjestelmästä TCP/IP protokolla käytöstä. Näillä keinoilla olet suojassa mahdollisilta tietoturvariskeiltä.

Windows 7 ja 8 käyttöjärjestelmät ovat tällä hetkellä suosituimpia kotikäytössä. On ehdottoman tärkeää ottaa automaattiset tietoturvapäivitykset käyttöön, joten Windows lataa itsenäisesti uudet päivitykset ja auttaa täten suojautumaan riskeiltä. Hanki myös erillinen haittatorjuntaohjelma. Vaikka Windows 7 ja 8 versioiden mukana tuleekin Windowsin oma Defender haittatorjuntaohjelma, se ei ole tarpeeksi riittävä. Useat kaupalliset torjuntaohjelmat ovat parempia, esimerkiksi F-Secure tai ilmaispuolelta Avast. Huolehdi myös muiden ohjelmistojen päivittämisestä, koska päivittämättömät ohjelmat ovat myös suuri uhka tietoturvalle. Älä myöskään pidä koneellasi ohjelmia, joita et käytä.

4.3 Langaton verkko

Yhä useammasta kodista löytyy langaton lähiverkko. Onkin tärkeää selvittää onko se suojattu asianmukaisesti. Mikäli näin ei ole, on mahdollista, että vaikka naapurisi käyttää kotisi langatonta verkkoa. Tällöin yhteys saattaa hidastua tai pahimmassa tapauksessa verkkosi voi joutua väärinkäytön kohteeksi.

Suojautumiseen on monia eri keinoja. Yksi tärkeimmistä on WLAN-tukiaseman suojaus salasanalla. Tällöin avoimesta verkosta tulee suljettu ja sitä voi käyttää vain tietämällä oikean salasanan. Tarkista myös, että tukiaseman laiteohjelmisto on ajan tasalla. Päivitykset korjaavat usein tietoturva-aukkoja ja laitteen vakaata toimintaa. Vaihda tukiaseman hallinta-asetuksista oletussalasana johonkin muuhun, etteivät väärät tahot pääse muuttamaan tukiaseman asetuksia.

Mikäli olet kodin ulkopuolella, on syytä harkita tarkkaan millaisiin WLAN-verkkoihin liittyy. Varsinkin ulkomailla on vaarallisia WLAN-verkkoja, joihin liittymällä voit joutua huijauksen kohteeksi. Pohdi tarkkaan liittyessäsi maksullisiin WLAN-verkkoihin, käytä vain ja ainoastaan luotettavia sikäläisen operaattorin verkkoja. (Rousku 2014, 209-213)

4.4 Verkkopankit

Verkkopankkien käyttö on nykyään todella yleistä. Rikolliset pyrkivätkin saamaan näistä itselleen hyötyä monin eri tavoin. Suurin uhka on rikollisten käyttämät pankkitroijalaiset. Troijalainen on haittaohjelma, joka asentuu huomaamatta käyttäjän koneelle ja toimii taustalla. Tällaisen troijalaisen avulla rikolliset voivat päästä kiinni käyttäjän verkkopankkiin, kun hän sinne kirjautuu. Käyttäjä luulee maksavansa normaalisti laskua, mutta rahat ohjautuukin ulkomaalaiselle tilille.

On tärkeää muistaa pankkiasioinnissa muutamat perusasiat. Säilytä aina pankin antamat käyttäjätunnukset ja avainlukulistat huolellisesti. Käytä tuttuja päälaitteita, kun asioit verkkopankissa. Älä käytä julkisia koneita, kuten esimerkiksi nettikahvilan laitteita. Jos pankki tarjoaa maksun lisävahvistus palvelua, se kannattaa ottaa käyttöön. Pidä tietokoneesi tietoturva aina ajan tasalla. (Rousku 2014, 203-204)

4.5 Sosiaalinen media

Sosiaalinen media, tuttavallisemmin some, käsittää monenlaisia eri palveluita. Näistä tunnetuimpia ovat tietenkin Facebook, Twitter ja esimerkiksi Linkedin. Sosiaaliseksi mediaksi lasketaan myös erilaiset blogit ja oikeastaan kaikki kuvien ja videoiden jakamiseen liittyvä.

Sosiaalinen media aiheuttaa monia yksityisyyden suojaan ja tietoturvaan liittyviä ongelmia ja riskitekijöitä. Suurin uhka käyttäjälle on tietosuoja. Facebook kerää valtavan määrän dataa omille servereilleen ja se tuntee käyttäjän liikkeet hyvinkin tarkasti. Yhdysvaltain tiedustelupalvelulla on pääsy näihin tietoihin. Tämä tarkoittaa sitä, että käytännössä kaikki kuvat, viestit ja asiat mitä on jaettu, pystytään saamaan selville.

Haittaohjelmat ja virukset ovat myös suuri riskitekijä erityisesti Facebookin maailmassa. Ne ovat selaimesta ja käyttöjärjestelmästä riippumattomia ja usein käyttäjä unohtaa

tämän, avatessaan jotain kiinnostavaa linkkiä, joka paljastuukin haittaohjelmaksi tai virukseksi. (Rousku 2014, 205-208)

5 TIETOTURVARISKEILTÄ SUOJAUTUMINEN

On olemassa monia erilaisia keinoja suojautua tietoturvariskeiltä. Käsittelen tässä nyt niistä muutamia, joita on helppo myös tavallisen kotikäyttäjän käyttää.

5.1 Virustorjunta

Erilaiset virukset ovat iso ongelma Windows-käyttöjärjestelmissä, joka monesta kotikoneesta löytyykin. Windows sisältää kolme ilmaista virustarkistinta, joita kannattaa ehdottomasti hyödyntää. Windowsin haittaohjelmien poistotyökalua (mrt.exe) voidaan käyttää komentoriviltä. Se etsii nimensä mukaisesti erilaisia haittaohjelmia. Windows Defender on yksinkertainen turvaohjelma, joka etsii vakoilu ja mainosohjelmia, se ei kuitenkaan riitä yksinään suojaamaan konetta. Security Essentials sen sijaan on ihan oikea tietoturvaohjelmisto, jonka voi ladata ilmaiseksi käyttöön. Myös muutamia ilmaisia torjuntaohjelmia on ladattavissa. Näitä ovat esimerkiksi Antivir ja Avast. Välillä tosin varsinkin kaupalliset ohjelmat saattavat aiheuttaa myös ongelmia. Ne pyrkivät olemaan kokoajan esillä, että käyttäjä uusisi tilauksen. Siitä johtuen voi tulla vääriäkin ilmoituksia viruksista tai ne saattavat kysyä käyttäjältä turhankin teknisiä kysymyksiä, joihin harva peruskäyttäjä osaa vastata. Oli ohjelma ilmainen tai kaupallinen niin muutamat perusasiat on hyvä pitää mielessä. On tärkeää pitää torjuntaohjelma aina päivitettynä. Virusten ja torjuntaohjelmien kilpajuoksu on usein minuuttipeliä. Ei myöskään pidä avata sähköpostiin tulleita epämääräisiä linkkejä tai avata tiedostoja. (Järvinen 2012, 210-212)

5.2 Palomuuri

Palomuurin tarkoituksena on rajoittaa liikennettä koneeseen ja koneesta poispäin internetiin. Palomuurin toimintaperiaate on porttisuodatus. Jokaisella ohjelmalla on oma porttinsa, jota yhteydenpitoon käyttää. Nämä portit täytyy erikseen palomuuriin sallia tai estää. Esimerkiksi internet-liikenne toimii portissa 80. Tavallisesti palomuuri analysoi kyseisen IP-paketin ja päättää saako se jatkaa matkaansa. Käytännössä siis palomuuri toimii liikenteenohjaajana oman yksityisen verkon ja julkisen verkon välissä. Palomuurilla on myös mahdollista torjua osoitteen väärennöksiä ja viruksia. Usein myös reititti-

messä, jossa palomuuri toimii on monia muitakin hyödyllisiä toimintoja, kuten ping-hyökkäysten esto. Palomuuritkaan eivät silti ole täysin ongelmattomia, vaan vaihtoehtoisia reittejä pitkin on mahdollista päästä verkkoon käsiksi. Näitä tapoja ovat esimerkiksi soittosarjat tai murtautuminen langattomaan lähiverkkoon. Eikä tietenkään voi pois sulkea sitä mahdollisuutta, että fyysisesti päästäisiin yrityksen tai kotikoneen tietoihin käsiksi. (Norton 2010.)

5.3 Suojausprotokollat

5.3.1 VPN

VPN eli Virtual Private Network tarkoittaa tekniikkaa, jonka avulla luodaan luotettava salattu yhteys kahden erilaisen verkon tai asiakaspäätteen ja verkon välille. Käyttäjän ei tarvitse ollenkaan itse huolehtia salauksesta, vaan laite tekee salauksen niin, ettei käyttäjän tarvitse tehdä mitään muita toimenpiteitä. VPN:n etuna on sen kiistaton läpinäkyvyys. Sen ratkaisut eivät vaadi muutoksia ohjelmiin, muihin tietoliikenteen tasoille tai verkkokomponentteihin. (Microsoft 2013.)

5.3.2 SSL

SSL on yksi yleisimmistä internetissä käytettävistä salausprotokollista, jolla pystytään salaamaan tunnistus asiakaspäätteen ja palvelimen välillä, tunnistaa palvelin ja neuvotella liikenteessä käytettävästä salauksesta. SSL esiintyy esimerkiksi pankkiyhteyksien suojausmenetelmänä. (Viestintävirasto 2017.)

5.3.3 SSH

SSH on suomalaista alkuperää oleva keksintö, joka turvaa tiedonsiirron Unix-koneiden sekä Unix-palvelimien välillä. SSH suojaa liikennettä vain Unix-palvelinten käytössä, mutta ei esimerkiksi Windows-verkon liikennettä, joten siinä on puutteensa salausprotokollana. (Linux wiki 2015.)

5.3.4 PGP

PGP on lyhenne sanoista Pretty Good Privacy, joka on yleisin sähköpostin salaamiseen käytetty menetelmä ja monet eri sähköpostiohjelmat tukevat sen käyttöä. Sillä käyttäjä voi suojata sähköpostiliikennettä, tiedostoja sekä lähettää ja vastaanottaa luottamuksellisia sähköpostiviestejä ja niiden liitteitä. Tiedostot ja sähköpostit on mahdollista myös varmentaa sähköisellä allekirjoituksella. (Tampereen teknillinen yliopisto 2006.)

5.4 Salasanat

Salasanat ja niiden oikeanlainen käyttö on tärkeä suojautumisen keino. Hyvällä salasanasuunnittelulla ja toteutuksella pääsee jo pitkälle. Yksinkertainen keino on käyttää eri salasanaa eri palveluissa. Siitä syystä, että jos jokin palvelu joutuu tietomurron kohteeksi ja siellä oleva salasanasi paljastuu, niin se voi olla riskitekijä, jos käytät samaa salasanaa muissakin palveluissa. Salasanoihin liittyy usein tiettyjä laatuvaatimuksia riippuen palvelusta. Yleisin ohje on, että käyttää isoja ja pieniä kirjaimia, sekä numeroita ja erikoismerkkejä. Minimipituus on kymmenen merkkiä, mutta mitä pidempi, sen parempi. Tällöin salasanan murtaminen on vaikeampaa. Salasanaa on myös tärkeä vaihtaa säännöllisesti. Jos salasana päätyy vääriin käsiin, niin vaihtamalla salasanan voi tilanteen vielä pelastaa. Missään tilanteessa salasana ei saa myöskään olla mikään selväkielinen sana. Hakkerit käyttävät sanakirjojen apua murtaessaan salasanoja. (Rousku 2014, 179-181)

5.5 Kaksivaiheinen tunnistus

Kaksivaiheinen tunnistus on nykypäivän tärkeimpiä suojautumiskeinoja. Monet eri palvelut tarjoavat sitä. Käytännössä homma toimii niin, että selaimella kirjautuessa saat tekstiviestin, jossa ilmoitetaan numerosarja, joka täytyy syöttää kirjautumisen yhteydessä. Tällöin mahdollisella hakkerilla pitäisi olla palvelun salasanan lisäksi myös puhelimesi hallussa. Tekstiviestit kuitenkin maksavat, joten monella ilmaispalvelun tarjoajalla ei ole mahdollisuuksia toteuttaa kaksivaiheista tunnistusta. Kaksivaiheisen tunnistuksen ollessa mahdollista, se kannattaa ehdottomasti ottaa käyttöön. Tällaisia pal-

veluja ovat esimerkiksi Googlen eri palvelut. Samaa tekniikkaa käyttää myös pankkien lisämaksun vahvistus -palvelut. (Järvinen 2012, 144-145)

6 CASE-TUTKIMUS: ISOVANHEMPIEN TIETOKONE

Lähdin tutkimaan isovanhempieni tietokoneen tietoturvaa. Valitsin heidän kotikoneensa sen takia, että ikäihmisten tietoturvaosaaminen on yleensä heikompaa, kuin vaikka nuorison.

6.1 Tietokoneen perustiedot

Kyseessä oli Samsung -merkkinen kannettava tietokone vuodelta 2011. Käyttöjärjestelmänä toimi Windows 7. Prosessori oli Intelin 2,40ghz ja keskusmuistia koneesta löytyi 4GT:n verran.

Kone oli suojattu Microsoftin omalla Security Essentials -ohjelmalla. Internet yhteys koneeseen tuli DNA-Kotimokkula 4G+ WLAN MF286 nimisellä langattomalla 4G/WLAN reitittimellä.

6.2 Tietoturvaraportti

Tietokoneen pääasiallisena tietoturvaohjelmana toimi Microsoftin oma Security Essentials -ohjelma. Essentialsin reaaliaikainen suojaus oli päällä, mutta viimeisestä tarkastuksesta oli kulunut jo kuukausi. Palomuurina käytössä oli Windowsin oma palomuuri.

DNA-Kotimokkulan hallintapaneeliin pääsi oletussalasanalla, joten se tulisi vaihtaa. Muutoin verkko oli suojattu asianmukaisesti wpa2-salauksella. Reitittimen oma palomuuri ei ollut käytössä.

Internet-selaimina toimivat Firefox ja Chrome. Chrome oli päivitetty ajan tasalle, mutta Firefoxista oli todella vanha versio 39.0 käytössä. Koneeseen oli myös asennettuna Malwarebytes –ohjelma, jonka avulla pystyy etsimään koneesta erilaisia vakoilu ja haittaohjelmia. Samsung Recovery -niminen ohjelma oli myös asennettu, mutta varmuuskopiointi ei ollut käytössä eikä varmuuskopiointeja ollut otettu.

6.3 Raportin analysointi ja toimenpiteet

Essentials ohjelman virustarkastuksesta oli kulunut jo kuukausi. Tein ohjelmalla nopean tarkastuksen, joka tarkisti 111765 tiedostoa koneelta, eikä uhkia havaittu. Reitittimen hallintapaneeliin pääsi oletussalasanalla, joten kävin muuttamassa sen toiseen. Windowsin palomuuri on näissä olosuhteissa mielestäni riittävä, joten en käynyt laittamassa reitittimen omaa palomuuria erikseen päälle.

Malwarebytesilla ajoin myös tarkastuksen, se löysikin 31 uhkaa, jotka ohjelma poisti. Kaikki uhat olivat pup.optional tyypin uhkia, joka käytännössä tarkoittaa erilaisia selaimeen kohdistuneita mainoshaittaohjelmia.

Internet-selaimina toimivat Firefox ja Google Chrome. Näistä Chrome oli ajan tasalla, eikä sieltä löytynyt uhkaavia lisäosia. Firefoxista sen sijaan oli todella vanha versio 39.0, joka on selvä tietoturvariski. Päivitin sen uudempaan 57.0.1. versioon. Salasanoja myös säilytettiin kaapissa paperilapuilla, joten se ei missään nimessä kovin hyvä keino ole, mikäli paperit häviää, tuhoutuu tai joutuu vääriin käsiin.

Sosiaalinen media oli Facebookin muodossa käytössä. Sieltä löytyi liuta erilaisia pelejä, mutta on vaikea sanoa onko niiden käyttö aiheuttanut konkreettisia tietoturvauhkia. Varmuuskopiointi olisi myös syytä ottaa käyttöön, mikäli tiedot pääsisivät häviämään, niin ne voisi vielä palauttaa.

7 POHDINTA

Aluksi oli vaikea rajata aihetta, koska tietoturva on käsitteenä niin laaja. Päädyin lopulta tarkastelemaan aihetta kotikoneen näkökulmasta, peilaten sitä muihin tietokoneen peruskäyttäjiin. Rajasin aiheen myös koskemaan pelkkää Windows-ympäristöä.

Tutkimuksessa selvitin yleisimmät tietoturvariskit ja yksinkertaisimmat keinot niiltä suojautumiseen. Tapaustutkimuksessani käsittelin Windows-tietokonetta. Suurimmat riskit kotikäyttäjälle ovat virustorjuntaohjelman puute, käyttöjärjestelmän päivittämättä jättäminen sekä suojaamaton WLAN-yhteys. Yksinkertaisimmat suojausmenetelmät ovat käytännössä näiden mainitsemieni riskien eliminointi. On syytä pitää koneella ajan tasalla oleva virustorjuntaohjelma sekä langaton internet-yhteys suojattuna. Näin ollen käyttäjä on jo poistanut suurimman osan koneelle tulevista uhista.

Tutkimuskysymykseni olivat, minkälaisia ovat tietoturvariskit kotikoneella ja miten niiltä voi suojautua. Tutkimukseni avulla pystyin vastaamaan tutkimuskysymyksiin niin, että kartoitin mahdolliset tietoturvariskit sukulaiseni kotikoneella ja selvitin suojautumiskeinot niitä vastaan. Kuitenkin tietoturvariskejä tulee päivittäin aina uusia, joten kaikkien tietoturvariskien ennakointi on mahdotonta ja suojauskeinoja sekä menetelmiä kehitetään koko ajan lisää.

Tutkimustani voi hyödyntää jokainen ihminen, jolla on kotona Windows-tietokone. Tutkimukseni avulla ihmiset saavat yksinkertaisen katsauksen erilaisiin tietoturvariskeihin ja suojautumiskeinoihin.

Tutkimusta voisi kehittää teettämällä kyselytutkimuksen, jossa kysyttäisiin ihmisten tietoutta tietoturvariskeistä ja suojautumiskeinoista. Tämän avulla pystyisin teettämään yksinkertaisen ohjekirjan ihmisille, jotka voisivat sitten hyödyntää sitä tietokoneensa suojaamisessa.

LÄHTEET

Jyväskylän yliopisto, Tietoturva ja virukset 2012. Viitattu 20.4.2015 http://appro.mit.jyu.fi/tyovaline/luennot2/luento9/#TOC3

Järvinen, P. 2012. Arjen tietoturva. Vinkit&Ratkaisut. Jyväskylä: Docendo

Linux wiki, SSH 2015. Viitattu 18.4.2015 http://www.linux.fi/wiki/SSH

Microsoft. How to configure a connection to a virtual private network (VPN) in Windows 2013. Viitattu 17.4.2015 https://support.microsoft.com/en-us/kb/314076/fi

Norton, Palomuurit 2010. Viitattu 17.4.2015 http://fi.norton.com/yoursecurityresource/detail.jsp?aid=firewalls

Rousku, K. 2014. Kyberturvaopas. Tietoturvaa kotona ja työpaikalla. Helsinki: Talentum.

Suomen internetopas, Tietoturva 2015. Viitattu 15.4.2015 http://www.internetopas.com/yleistietoa/tietoturva/

Suomen internetopas, Suojausmenetelmät 2015. Viitattu 16.4.2015 http://www.internetopas.com/yleistietoa/tietoturva/suojausmenetelmat/

Tampereen teknillinen yliopisto, PGP:n käyttö Windowsissa 2006. Viitattu 19.4.2015 https://www.cs.tut.fi/~jkorpela/softa/pgp.html

Viestintävirasto, Langattomasti, mutta turvallisesti 2014. Viitattu 21.4.2015 https://www.viestintavirasto.fi/ohjausjavalvonta/ohjeetjajulkaisut/ohjeidentulkintojensuositustenjaselvitystenasiakirjat/ohje22014langattomastimuttaturvallisesti.html

Viestintävirasto, Tietoturvaohjeet 2017. Viitattu 22.11.2017 https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvaohjeet/palveluidenturvallinenkaytto/viestinnansalaus.html

Virustorjunta 2015. Viitattu 20.4.2015 http://www.virustorjunta.net/modules.php?name=Artikkelit&op=viewarticle&artid=14

Webtieto, Windows-tietoturva 2017. Viitattu 24.10.2017 http://www.webtieto.com/p/windows-tietoturva.html

Wikipedia, Windows 2017. Viitattu 19.9.2017 https://fi.wikipedia.org/wiki/Microsoft_Windows

Wikipedia, Internet 2015. Viitattu 15.4.2015 http://fi.wikipedia.org/wiki/Internet