HAAGA-HELIA
ammattikorkeakoulu

Kotikäyttäjän tietoturva

- case eräs Nordean yksikkö

Jaana Laaksonen

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2010

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

1.4.2010

Tietojenkäsittelyn koulutusohjelma

Tekijä Jaana Laaksonen	**Ryhmä** TIKO06SI
Opinnäytetyön nimi Kotikäyttäjän tietoturva - case eräs Nordean yksikkö	**Sivu- ja liitesivumäärä** 45 + 16
Ohjaaja Titta Ahlberg	

Tutkielman aineena oli käsitellä kotikäyttäjän tietoturvaa erään Nordean yksikön kautta. Tutkimuksessa perehdyttiin siihen, mikä on erään Nordean yksikön tietämys tämän ajan käsitteistä, jotka liittyvät oman kotitietokoneeseen kohdistuviin uhkiin sekä mikä oli kohderyhmän suhtautuminen tähän liittyvään roskapostiin. Tutkimuksessa tutkittiin lisäksi, osaako kohderyhmä huolehtia kotikoneensa tietoturvasta. Työ ei ollut toimeksianto.

Verkkorikollisuus on paitsi lisääntynyt myös muuttanut muotoaan. Viitekehyksessä käsiteltiin teoriatasolla haittaohjelmista virusta, matoa, takaovea, troijalaista, rootkitia sekä bottia ja bottiverkkoa. Hyökkäysmalleista olivat tarkasteltavissa roskaposti eli spam sekä palvelunestohyökkäys. Social engineering -hyökkäyksissä käytetään hyväksi lähinnä käyttäjän omaa herkkäuskoisuutta. Näitä ovat phising- eli khalastelu ja pharming. Edellä oleviin liittyy myös torjunta. Siitä käsiteltiin palomuuria, virustentorjuntaohjelmaa, päivityksen merkitystä sekä lyhyesti eri käyttöjärjestelmiä sekä selaimia.

Tutkimus toteutettiin kvantitatiivisena survey-tutkimuksena. Kyselyn kohderyhmässä oli 89 henkilöä. Heille lähetettiin syyskuussa vuonna 2009 Webropolilla toteutettu kyselylomake.

Tutkimustulokset analysoitiin tavallisten käyttäjien ja jonkin verran ammattilaisten vertailuna sekä ikäryhmävertailuna. Rinnakkaisvertailua tietämyksen ja ikäryhmien kesken ei kyetty tekemään pienen kohderyhmän takia. Vastaajien yksilönsuojaa haluttiin suojella. Ammattilaiseksi itsensä luokitellut jätettiin analysoinnista pois.

Tuloksista voitiin päätellä, että kohderyhmä on melko valveutunutta. Phising ei ollut kaikille tuttu käsite, vaikka näin olisi voinut kuvitella johtuen sen liittymisestä tämän alan uutisointiin Nordeasta. Vastaajien suhtautuminen saada pahanlaatuinen virus omalle koneelle oli joko neutraali tai sitten todennäköisyyttä ei pidetty suurena. Tulokset osoittivat, että suurin osa vastaajista näytti poistavan roskapostin avaamatta sitä. Torjunnan osalta kävi ilmi, että kaikilla ei ollut palomuuria. Virustorjuntaohjelma oli lähes kaikilla. Vastaajista kaikki olivat suurimmaksi osaksi ottaneet automaattiset päivitykset käyttöön liittyen virustorjunnan turvapäivityksiin. Roskapostin suodatus oli hoidettu huonommin.

Suosituksena on se, että kaikki käsitteet käydään läpi kohderyhmän kanssa. Hyvä on myös muistuttaa, mikä on roskapostiin suhtautumisen merkitys.

Asiasanat
tietokonevirukset, haittaohjelmat, tietoturva, virustentorjuntaohjelmat

HAAGA-HELIA
ammattikorkeakoulu

Abstract

1 April 2010

Degree programme in Business Information Technology

Author	**Group**
Jaana Laaksonen	TIKO06SI

The title of thesis	**Number of pages and appendices**
Computer security from a home user's perspective	45 + 16

Supervisor
Titta Ahlberg

The purpose of this thesis was to find out whether the target group (i.e. the employees of a business unit at Nordea Bank Finland) knows the concepts of malware and social engineering and related terms that threat computers and how the target group reacts to spam. In addition, the aim was to clarify how well the target group knows computer protection related to data security. The study concentrated on computer security from a home user's perspective.

The thesis was carried out as follows: a Webropol-questionnaire was sent to the target group via e-mail. The target group consisted of 89 people working in one of the units at Nordea Bank Finland. The query included questions about the subject with various alternatives to choose from. Furthermore, it included some open questions. The questions in the query were based on the theoretical part of the thesis. The results were analyzed based on the respondents' level of their previous knowledge of technical issues. The other aspect was to analyze the results comparing different age groups.

The thesis indicated that the target group is aware of the threats of malware. Phising was one of the asked concepts and it should have been known to the bank employees. The results showed that it was not as well-known as predicted. Furthermore, the thesis showed that the opinion of having malware on one's own computer was either neutral or the probability was not regarded as a considerable one. Moreover, the study revealed that the majority of the target group did delete their spam mail without opening it. Additionally, what comes to the data security, not all respondents had a firewall in their computers. However, most of them had some kind of virus protection program.

The thesis concludes that even though the results did not show anything alarming, training should be provided to the target group. Additionally, those employees who do not maintain their own computer should be encouraged to do so.

Key words
computer viruses, malware, data security, computer protection, virus protection programs

Haluan kiittää yksikönjohtaja Taina Seiloa, joka ystävällisesti suostui pyyntööni lähettää kysely-lomake alaisilleen. Haluan myös kiittää kaikkia työkavereita kannustuksesta, mitä olen saanut tämän työn tekemisessä. Jo kysely herätti kiinnostusta aiheeseen.

Sisällys

1 Johdanto 1
2 Verkkorikollisuus 2
2.1 Haittaohjelmat 3
2.1.1 Virus 4
2.1.2 Mato 4
2.1.3 Takaovi 5
2.1.4 Troijalainen 5
2.1.5 Rootkit 6
2.1.6 Botti ja bottiverkko 6
2.2 Hyökkäysmallit 7
2.2.1 Roskaposti eli spam 7
2.2.2 Palvelunestohyökkäys 9
2.2.3 Muut 9
2.3 Social engineering -hyökkäykset 11
2.3.1 Phising 11
2.3.2 Pharming 12
2.4 Tulevaisuus menneen kautta 13
3 Torjunta 15
3.1 Palomuuri 16
3.2 Virustentorjuntaohjelma 16
3.3 Päivittäminen 17
3.4 Käyttöjärjestelmät ja selaimet tietoturvan näkökulmasta 18
3.4.1 Microsoft Windows 18
3.4.2 Linux 19
3.4.3 Macintosh OS 19
3.4.4 Selaimet 20
3.5 Torjunnan tulevaisuus 20
4 Aineisto ja tutkimusmenetelmät 23
4.1 Tutkimusongelmat 23

4.2 Tutkimusmenetelmä 23
4.3 Kohderyhmä 24
4.4 Toteutus 25
5 Tulokset 26
5.1 Vertailua tavallisten käyttäjien ja jonkin verran ammattilaisten välillä 26
5.1.1 Oletko havainnut kotikoneellasi perinteisiä haittaohjelmia (matoja, viruksia, takaovia, troijalaisia) 27
5.1.2 Miten hyvin tunnet seuraavat käsitteet 27
5.1.3 Sinulta kysytään salasanaasi. Kenelle sen antaisit? 28
5.1.4 Tietoisuus pahanlaatuisten virusten esiintymisestä 29
5.1.5 Suhtautuminen roskapostiin 29
5.1.6 Oman tietokoneen suojaus 31
5.1.7 Käytätkö kotikoneessasi roskapostin automaattista suodatusta? 32
5.1.8 Kotikoneen pääasiallinen käyttöjärjestelmä ja sen tietoturvapäivitykset 33
5.1.9 Kohderyhmän kotona käyttämä web-selain ja sen päivitys 34
5.2 Vertailua ikäryhmien välillä 34
5.2.1 Oletko havainnut kotikoneellasi perinteisiä haittaohjelmia (matoja, viruksia, takaovia, troijalaisia) 35
5.2.2 Miten hyvin tunnet seuraavat käsitteet 35
5.2.3 Sinulta kysytään salasanaasi. Kenelle sen antaisit? 37
5.2.4 Tietoisuus pahanlaatuisten virusten esiintymisestä 37
5.2.5 Suhtautuminen roskapostiin 38
5.2.6 Oman tietokoneen suojaus 40
5.2.7 Käytätkö kotikoneessasi roskapostin automaattista suodatusta? 41
5.2.8 Kotikoneen pääasiallinen käyttöjärjestelmä ja sen tietoturvapäivitykset 41
5.2.9 Kohderyhmän kotona käyttämä web-selain ja sen päivitys 42
6 Johtopäätökset ja suositukset 43
6.1 Johtopäätökset 43

6.2 Suositukset 44
7 Yhteenveto 45
Lähteet 46
Liitteet
Liite 1. Kyselylomake 49
Liite 2. Työn esitys 55
Liite 3. Loppuraportti 58

1 Johdanto

Tämä työ on HAAGA-HELIAlle tehty opinnäytetyö. Se noudattaa oppilaitoksen ohjeistusta dokumentoinnin suhteen. Työn aiheena on ollut käsitellä tietoturvaa kotikäyttäjän näkökulmasta. Kotikäyttäjä on kuka tahansa, joka käyttää tietokonetta kotona ja siis joutuu itse miettimään tietoturvaan liittyviä asioita. Koulussa tai työpaikalla tietoturvasta huolehtivat alan ammattilaiset. Useissa yrityksissä ja kouluissa on tietoturvapolitiikka, jossa käydään läpi eri riskitekijöitä liittyen tietoturvaan. Eli jossain muualla kuin kotona tietoturva on ulkoistettu jonkun muun hoidettavaksi. Kun vastuu siirtyy kotiin, myös tietotaidon merkitys kasvaa. Tässä työssä kotikäyttäjä on rajattu työssä käyvään henkilöön, joka käyttää tietokonetta kotona.

Internet sisältää paljon kivaa hyödyllistä ja ei-hyödyllistä tietoa oman maun mukaan. Samalla, kun maailma on tullut sen kautta napin painalluksen ulottuville, myös maailman uhat ovat lähentyneet. Aina välillä kuulee, ettei Suomea kukaan terroristi uhkaa, koska olemme niin kaukana. Näin varmasti voi ollakin. Valitettavasti verkko ei kuitenkaan tunne etäisyyksiä niin kuin karttapallo. Jos koneeni on suojaamaton ja venäläinen rikollinen etsii kohteita, oma koneeni Suomen Espoossa on yhtä suuressa vaarassa kuin yhteistyökumppanini kone Yhdysvaltain Bostonissa.

Tietoturva sinällään pitää sisällään mitä moninaisimpia asioita aina yksityisyyden suojasta haittaohjelmiin, tiedon oikeasta säilyttämisestä tiedon oikeaan tuhoamiseen. Tässä työssä tietoturva jotenkin liittyy siihen, mitä tapahtuu liittyen tietokoneeseen ja siihen ympäröivään maailmaan, jonka hakukone Google on tuonut lähelle.

Tämä työ keskittyy kotikäyttäjän tietoturvaan. Aiheen laajuuden takia työssä käsitellään pääsääntöisesti uhkia, jotka liittyvät verkkorikollisuuteen sekä sen torjuntaan. Tässä esityksessä ei käydä läpi ongelmia, jotka liittyvät verkkokauppaan, tiedon säilyttämiseen ja tiedon tuhoamiseen. Jos nämä mainitaan, ne ovat vain esimerkkejä liittyen itse aiheeseen. On hyvä huomioida, että verkkorikollisuus on sen verran muuttunut, että tiukkoja rajauksia ei voidai tehdä. Työn viitekehykseen on kerätty aineistoa pääsääntöisesti ennen 17.8.2009. Koska työn tekeminen viivästyi, tähän työhön on otettu lisäyksenä mukaan Nordean verkkopankkia koskeva uusi uutinen tammikuulta 2010 jo tutkimuksen kohderyhmän takia sekä muutama uudempi tilastotieto.

Työn tavoitteena on viitekehyksessä esitellä käsitteet liittyen verkkorikollisuuteen ja torjuntaan teoriatasolla sekä kytkeä nämä aiheet tutkimukseen kappaleissa neljä ja viisi. Tutkimuksessa on

tavoitteena eri tutkimusongelmien kautta käydä läpi, mikä on tietyn Nordea Pankki Suomen yksikön henkilöiden tietämys viitekehyksessä esitetyistä asioista. Tutkimus ei ollut Nordean toimeksianto.

Työn tutkimusongelmat on kiteytetty kahteen kohtaan eli 1) Tunteeko kohderyhmä tämän ajan käsitteet, jotka liittyvät omaan kotitietokoneeseen kohdistuviin uhkiin sekä mikä on heidän suhtautumisensa tähän liittyvään roskapostiin? sekä 2) Osaako kohderyhmä huolehtia kotikoneensa tietoturvasta? Edellä kuvattuja ongelmia on analysoitu tutkimuksessa asiaan perehtyneisyyden ja ikäryhmävertailujen kautta.

2 Verkkorikollisuus

Verkkorikollisuus on muuttunut paljon viimeisten vuosien aikana. Kun vuonna 2002 tehtiin tutkimus EU-tasolla verkoista, tietokonemadot olivat voimissaan ja ne tekivät tuhojaan. Nyt nämä ovat lähes kadonneet ja tilalle on tullut tietokoneeseen piiloutuva tuholainen, jonka pääsääntöinen tarkoitus on aiheuttaa tuhoa muille kuin itse tietokoneen käyttäjälle. Vuonna 2000 hakkerit eli scriptikidit olivat voimissaan. Nykyään hakkerit ovat usein osa isompaa organisaatiota, jonka tarkoitus on aiheuttaa taloudellista hyötyä organisaatiolleen. Jokin pieni botti koneessani voi olla osa sadan tuhannen zombie-koneen bottiverkkoa, jonka tarkoitus on hoitaa rahanpesua.

Yhteistä kaikelle on kuitenkin se, että verkkorikollisuus on verkossa tapahtuvaa rikollisuutta, jossa tarvitaan tietokone ja kyberavaruus eli internet. Tähän kuuluu myös kotikäyttäjän harhauttaminen ja huijaaminen verkkoon liittyen. Sitä voi tapahtua missä päin maailmaa tahansa ja sitä voi tapahtua milloin vain. Jos haluaa välttyä tyystin kaikilta uhilta liittyen tähän aiheeseen, on paras olla kiinnittämättä tietokonettaan verkkoon.

Virusten kirjoittaminen on siirtynyt hakkereiden eli nuorehkojen miesten harrastuksesta ammattimaiseksi toiminnaksi. Motiivi on muuttunut huvista ja maineen hankinnasta taloudellisen hyödyn tavoitteluun. Tyypillistä on alihankinnan kaltainen yhteistyö, jossa rikolliset ovat omaksuneet eri rooleja. Rikolliset voivat olla eri puolilla maailmaa, eivätkä he edes tunne toisiaan. Taitava ohjelmoija voi kirjoittaa haittaohjelmia ja myydä niitä edelleen bottiverkkojen ylläpitäjälle. Tämä puolestaan myy bottiverkkonsa palveluja roskapostittajille ja palvelunestohyökkäyksillä yrityksiä uhkaavalle kiristäjälle. Myös luottokortteja ja pankkitilejä kauppaavat tahot myyvät yleensä tietonsa eteenpäin sen sijaan, että käyttäisivät niitä itse. (Suoranta 2008.)

Vaikka rikosten tekijät eivät olisikaan kiinnostuneita tietyn kotikäyttäjän yksittäisestä tietokoneesta, se voidaan valjastaa pahimmillaan rikolliseen toimintaan. Kokonaisvahingot voivat ulottua pitkälle ja aiheuttaa paljon tuhoa. Kotikäyttäjä voi tietämättään olla osallisena esimerkiksi mikroblogi Twitteriä vastaan kohdistetussa palveluhyökkäyksessä.

2.1 Haittaohjelmat

Haittaohjelma on ohjelma, joka tulee tietokoneelle käyttäen hyväkseen tietotokoneen heikkouksia tai käyttäjän hyväuskoisuutta. Sen tarkoitus on joko aiheuttaa haittaa suoraan käyttäjälle tai se voi olla myös niin huomaamaton, ettei käyttäjä huomaa mitään. Haitan kärsivä uhri ei välttämättä ole käyttäjä vaan joku ulkopuolinen taho. Käyttäjän kone on valjastettu johonkin, mitä sen ei pitäisi tehdä. Haittaohjelmien kirjo on kasvanut. Samasta haittaohjelmasta voidaan pakkaamalla ja kryptaamalla tehdä muunnelmia, jotka vaativat uusia tunnisteita. Tietoturvayhtiö F-Secure saa päivittäin noin 25.000 näytettä, joista noin puolet on uusia haittaohjelmia. (Suoranta 2008.) Elämme muuttuvassa toimintaympäristössä.

Haittaohjelmien luokittelu ei ole täysin yksiselitteistä. Joissakin lähteissä madot ja troijalaiset madot luokitellaan viruksiin. Joissakin nämä kaikki luokitellaan erikseen. Tässä esityksessä on päädytty siihen, että madot, virukset ja troijalaiset käsitellään erikseen.

Haittaohjelmien kirjo on kasvanut. Nykyajan haittaohjelmilla voi tehdä yritysvakoilua (vakoiluja näppäimistökaapparit). Tunnettuja nettipalveluita voi kiristää palvelunestohyökkäyksillä. Khalastelu- ym. huijausviestit ovat keino ansaita rahaa. Roskaposti eli jopa miljoonien viestien lähetys voidaan ostaa valmiina, ulkoistettuna palveluna bottiverkon ylläpitäjältä. Tietomurrot yrityksiin voidaan haittaohjelmien avulla kierrättää useiden muiden koneiden kautta ja täten piilottaa jäljet todelliseen lähteeseen. Bottiverkon kautta voidaan salasanalla suojattujen dokumenttien murtaminen hajauttaa tuhansille kotikoneille. Vakoiluohjelmat voivat kerätä surffaustietoja, jolloin voidaan kohdistaa mainonta tehokkaammin. Roskapostittajat keräävät toimivia sähköpostiosoitteita uhrin sähköpostiohjelmista. Haittaohjelmia voidaan käyttää portteina uusien haittaohjelmien syöttämiseen sekä klikkaushuijauksessa voidaan hajauttaa klikkaukset tulemaan eri koneista. Tässä oli lueteltu vain osa haittaohjelmien mahdollisuuksista. (Järvinen 2006, 77-79). Ei ole kovinkaan kauan siitä, kun nigerialaiskirjeet ja lottovoitot olivat tavallisia. Nyt näiden on huomattu lähes hävinneen.

Haittaohjelmat pääsevät tietokoneeseen esimerkiksi sähköpostin liitetiedostona (ohjelmatiedosto suoraan tai linkkinä www-sivulle, jolta varsinainen haittaohjelma latautuu). Käyttöjärjes-

telmän tietoturva-aukkoja käyttävät erityisesti verkkomadot ja muut ohjelmat, jotka pyrkivät levittämään itseään uusiin kohteisiin. Selaimen turva-aukot ovat vaarallisia. Www-sivuilta ladattavat ActiceX-ohjelmat ovat myös riski. Ongelma on myös usein vieraskielinen viesti, johon käyttäjä helposti vastaa ”yes”. Muina kanavina voi mainita p2p-verkot (laittoman jakelun verkot), mp3-soittimien levyt, cd-äänilevy. (Järvinen 2006, 79-82.)

2.1.1 Virus

Virukset ovat ohjelmia, jotka päästessään tietokoneeseen muuttavat alkuperäisiä ohjelmia siten, että alkuperäinen ohjelma saadaan tekemään kopioita viruksesta, joka sitten taas tartuttaa muita ohjelmia. Sanotaan, että sillä on isäntäohjelma. Virus ajetaan samaan aikaan kuin isäntäohjelma. Ensimmäinen virus ilmestyi jo 1980-luvulla (Stallings 2008, 220)

Viruksia luokitellaan kohteensa tai strategiansa mukaisesti. Käynnistyssektorivirukset tarttuvat levykkeiden ja kiintolevyjen aloitussektoreille. Tiedostovirukset tartuttavat itseään muihin ohjelmatiedostoihin. Makrovirukset leviävät niissä ohjelmissa, joissa on kyseinen makro-ohjelmointikieli. Stealth-virus pystyy piiloutumaan virustentorjuntaohjelmilta. Mutaatiovirukset muuntavat tunnistettaan ja tekevät viruksen löytymisen hankalaksi. Vitsivirukset ovat pelkkiä tyhjiä uhkauksia. Huijausvirukset ovat samantapaisia tyhjiä virusvaroituksia. (Flyktman 2006, 298)

Sähköpostivirus on tuoreempi virustyyppi. Ensimmäinen tällainen oli nimeltään Melissa. Se käytti hyväkseen sähköpostin liitteessä olevaa Microsoft Wordin makroa. Makron aktivoitua sähköpostivirus lähetti itsensä jokaiselle, joka oli käyttäjän sähköpostilistalla. Se aiheutti myös vahinkoa käyttäjän koneelle. Uudempaa kehitystä edustaa vuonna 1999 ilmestynyt sähköpostivirus, joka aktivoitui pelkästään sähköpostin avaamisesta. Siinä käytettiin hyväksi Visual Basicin scriptikieltä. (Stallings 2008, 225) Välttämättä sähköpostivirus ei tuhoa mitään, vaan se voi kerätä käyttäjän sähköpostiaineistoa ja lähettää sen eteenpäin.

2.1.2 Mato

Verkkomadot ovat pieniä ohjelmia, jotka leviävät netin välityksellä koneesta toiseen. Ne leviävät itse itseään kopioimalla. Ne eivät siis tarvitse isäntäohjelmaa kuten virukset. Ne aktivoituvat automaattisesti. Morris-mato oli yksi tunnetuimmista madoista. Se julkaistiin vuonna 1988 ja se oli suunniteltu leviämään UNIX-järjestelmissä. Nykyajan matoja edustaa Code Red -mato

vuodelta 2001. Se hyödynsi tietoturva-aukkoa Microsoftin internet-tietoserverissä. (Stallings 2008, 231-3) Sähköpostimadosta on esimerkkinä vuosikymmenen alusta Loveletter-viesti.

Joulukuussa 2008 laskettiin liikkeelle Conficker-verkkomato, jonka tiedetään edelleen olevan voimissaan. McAfee raportoi sen aiheuttamien selainhyökkäysten muuttuneen web-sivuja koskeviksi hyökkäyksiksi. (McAfee 2009, 6.) CERT-FI lähetti toisen vuosineljänneksen aikana vuonna 2009 käyttäjille 22000 Conficker-verkkomatoon liittyvää ilmoitusta. Suomalaisissa verkoissa verkkomadon saastuttamia koneita oli havaittu noin 5300 eri IP-osoitteesta. Ensimmäisellä vuosineljänneksellä vuonna 2009 lähetettiin vastaavasti noin 14000 ilmoitusta, jotka koskivat 3600 eri osoitetta. Madon todettiin myös kopioituneen USB-muistikorteille toukokuussa 2009. (Cert-Fi 2009.)

2.1.3 Takaovi

Takaovi on ohjelma, joka tarjoaa hyökkääjälle avoimen pääsyn järjestelmään. Sen ensi sijaisena tavoitteena on käyttää piilotettua etähallintaohjelmistoa käyttäjän tekemisten seuraamiseen. Täten voidaan kerätä käyttäjän käyttäjätunnuksia ja salasanoja muihin järjestelmiin, joita voidaan käyttää uusiin hyökkäyksiin. (Boström 2003, 48.)

Takaovea hallitseva hyökkääjä voi myös yrittää piileskellä järjestelmässä. Nykyisissä takaovioh-jelmissa on hyökkäysominaisuus, joka voi odottaa bottiverkon ohjaajan komentoa. Tällöin konetta voidaan käyttää zombie-koneena laajamittaiseen hajautettuun palvelunestohyökkäykseen. (Järvinen 2006, 88.)

2.1.4 Troijalainen

Antiikin Kreikan tarustossa Troijan hevosella avattiin Troijan portit, jotta päästiin tekemään tuhoja. Samanlaisen ajattelun mukaan haittaohjelma troijalainen on työkalu, joka avaa portin uhrin koneeseen. Aivan kuin takaovea myös troijalaisen saastuttamaa konetta voi kutsua bottiverkon ohjaaja. Aktivoitunut troijalainen voi myös poistaa ohjelmallisen palomuurin käytöstä. Tällöin avatusta portista voi latautua lukuisia eri ohjelmia, joista joku voi olla troijalainen, joka taas lataa uusia ohjelmia. Lopputuloksena voi olla selaimen kaatuminen. (Järvinen 2006, 83)

Osa troijalaisista antaa sellaisen käsityksen, että ne ovat hyödyllisiä, mutta aiheuttavatkin tuhoa. Esimerkkinä voi olla troijalaisen lähettäminen piilottamalla se maksuttomasti ladattavaan materiaaliin, esimerkiksi näytönsäästäjiin, peleihin tai porno-ohjelmiin, jotka antavat ”maksutto-

man" pääsyn epäilyttävään sisältöön. Troijalainen voidaan lähettää myös sähköpostin liitetiedostoina tai verkkolinkkeinä. Paitsi bottiverkon osana troijalaista käytetään myös pharming-hyökkäyksissä. (Symantec 2009b.)

2.1.5 Rootkit

Rootkit on ohjelmakokoelma, joka asentuu systeemiin mahdollistaakseen ylläpitäjän (tai juuren) pääsyn systeemiin. Yleisesti juureen (root) pääsy mahdollistaa pääsyn kaikkiin niihin toimintoihin ja palveluihin, joita käyttöjärjestelmällä on. Hyökkääjä saa siten systeemin täydellisen hallinnan. Hän voi lisätä tai muuttaa ohjelmia ja tiedostoja, monitoroida prosesseja, lähettää ja saada tietoliikennettä ja saada takaovi-pääsyn käskystä. Osa rootkiteistä selviytyy uudelleenkäynnistyksestä, osa ei. (Stallings s. 242-243.) Rootkitien historia ulottuu Unix-aikaan 1990-luvulle. Windowsissa rootkitit alkoivat yleistyä 2000-luvulla. (Järvinen 2006, 92.)

Rootkit voi asentua troijalaisen välityksellä. Asennus voi tapahtua myös hakkeroinnilla. Tällöin hyökkääjä käyttää toimintoa tunnistaakseen avonaisia portteja tai muita haavoittuvuuksia. Hyökkääjä käyttää salasanan murtoa, haittaohjelmaa tai systeemi haavoittuvuutta saavuttaakseen lopullisen pääsyn ja lopulta juuri-pääsyn. Rootkitiin voidaan lisätä virus, palvelunestohyökkäys tai muun tyyppinen hyökkäys. Rootkit voi asentaa myös näppäimistökuuntelijan. (Stallings 2008, 243.) Kesällä 2008 löydettiin Mebroot-troijalainen, joka piiloutui tietokoneen pääkäynnistyslohkoon ja käynnistyi siten ennen käyttöjärjestelmää. (Suoranta 2008.)

2.1.6 Botti ja bottiverkko

Botti on haittaohjelma, joka antaa hyökkääjälle saastuneen tietokoneen hallinnan. Botit ovat yleensä osa ympäri maailmaa sijoittuneiden saastuneiden tietokoneiden verkkoa, jota kutsutaan bottiverkoksi. Storm-, Kraker- ja Srizbi -haittaohjelmien verkot ovat esimerkkejä bottiverkoista. Niihin kuuluu muutamia satoja tuhansia saastuneita koneita. Saastuneita koneita kutsutaan zombeiksi. Yleensä käyttäjä ei tiedä koneensa olevansa saastunut. Botti piiloutuu saastuneeseen koneeseen ja lähettää tiedon isännälleen. Botit pysyvät piilossa kunnes ne saavat käskyn toimia. (Suoranta 2008.) Etäkontrolliominaisuus erottaa botin madosta. Mato aktivoi itsensä, kun taas botit aktivoidaan jostakin muualta keskitetysti. (Stallings(2008, 241.)

Botteja ja bottiverkkoja voidaan käyttää eri tavoin. Myöhemmin käydään läpi tarkemmin palvelunestohyökkäystä, joka on eräs käyttötapa. Bottiverkon avulla hyökkääjä voi myös lähettää massiivisen määrän roskaposteja. Botti voi käyttää salakuuntelua löytääkseen esimerkiksi käyt-

täjän käyttäjätunnuksia ja salasanoja. Sillä voidaan myös saada tietoon käyttäjän näppäinpainallukset. Bottiverkko voi levittää uusia botteja mahdollistaen näin uusien haittaohjelmien levittämisen. Sitä voidaan käyttää myös mainoslauseiden ja selainapuohjelmien päivittämiseen ja täten taloudellisen hyödyn saavuttamiseen. Bottiverkolla on helppo manipuloida verkkopelejä ja äänestysten tuloksia, koska jokaisella botilla on oma IP-osoite eli jokaisella on täten yksi ääni. (Stallings (2008, 240-1)

Vuonna 2007 raportoitiin yleistyneestä web-hyökkäysten aallosta, jossa käyttäjän koneelle tullaan arvostettujen ja tunnettujen sivustojen kautta. 4.4.2008 Bottiverkkoja hyödyntävä haittaohjelma hyökkäsi Tietokone.fi-sivustolle. Se hyödynsi Internet Explorerin tukemaa ActiveX-tekniikkaa. Esimerkissä web-sovelluksessa oli ohjelmointivirhe ja MS SQ Server -tietokannasta puuttui tietoturvapäivitys. (Lehto 2008.)

Uusia haittaohjelmien valjastamia zombitietokoneita kirjattiin vuonna 2009 toisella neljänneksellä 14 miljoonaa kappaletta. McAfee totesi, että se oli enemmän kuin millään aikaisemmalla neljänneksellä. Hyökkääjien rikollisiin tarkoituksiin käyttämiin bottiverkkohin jäi siis kiinni 150000 tietokonetta päivässä. (IT-viikko 2009b.) Cert.fi-ryhmän mukaan Suomessa on bottiverkkoihin kuuluvia koneita suhteessa hyvin vähän. Kohdennettuja hyökkäyksiä on kuitenkin todettu myös Suomessa. (Suoranta 2008.)

2.2 Hyökkäysmallit

Seuraavassa on lueteltu erilaisia hyökkäysmalleja, joissa joillakin tavoilla aktivoidaan tai saadaan uhrin koneeseen aktivoiduksi haittaohjelma. Tässä työssä on käsitelty erikseen social engineering -hyökkäykset eli niitä ei ole luokiteltu hyökkäysmalleiksi. Näinkin olisi voinut tehdä.

2.2.1 Roskaposti eli spam

Roskaposti eli spam on keino mainostaa erilaisia tuotteita sähköpostitse. Sähköpostilla mainostaminen ei ole kiellettyä. Tietoturvan kannalta ongelma ei olekaan itse mainosviesti vaan niiden yhteys haittaohjelmiin, bottiverkkojen ylläpitäjiin ja luottokorttirikollisten verkostoon. Varastetuilla luottokorttitiedoilla ostetaan laillisesti tavaraa, jonka välittäjät hoitavat rahanpesun. (Hämäläinen 2008.) Valtaosa roskapostista on huijausta. Roskapostiin vastaamisen on todettu lisäävän postin määrään. Välttämättä ei edes ole kysymys vastaamisesta vaan pelkästä katsomisesta. Tämän voi todeta itsekin jonkun manatessa ”vain katsoneensa, mikä se oli”. Miksi ihmiset sitten avaavat roskapostin ja vielä vastaavat siihen?

MAAWG:n (Messaging Anti-Abuse Working Group) teki vuonna 2009 Pohjois-Amerikassa tutkimuksen. Siinä kävi ilmi, että lähes kolmannes kuluttajista myönsi vastanneensa jopa tahallaan sellaiseen sähköpostiviestiin, jota epäilivät roskapostiksi. 80 prosenttia käyttäjistä ei uskonut, että heidän tietokoneensa voisi saastua ns. bottiohjelmalla, joka saa tietokoneen vaikkapa lähettämään roskapostia käyttäjän tietämättä. Tutkimuksen mukaan käyttäjät ovat tietoisia sähköpostin perusuhista, mutta eivät ole tarpeeksi valveutuneita tai varuillaan. (Taloussanomat 2009b.)

Roskapostin kasvu alkoi kesästä 2007. Tutkimukset ovat paljastaneet roskapostitilanteen vain pahentuneen. Tähän on arveltu olevan syynä uudet käyttäjät Kiinassa, Intiassa, Venäjällä ja Brasiliassa. Nämä eivät ilmeisesti hallitse tietoturvaa eivätkä osaa siis varoa netissä. Miljoonia uusia työasemia on saatu kaapattua ja muutettua zombeiksi ympäri maailmaan. (Järvinen 2008.)

Mikä on siis ratkaisu tähän kasvavaan ongelmaan? Roskapostitus on saanut jotkut yritykset miettimään sähköpostin rajoittamista. Sähköpostit voidaan korvata puhelimella ja tekstiviesteillä sekä mesettämällä ja Skypella. Roskapostin lähettäminen ei ole kiellettyä kaikissa maissa. Onkin huomattu, että valta osa viesteistä kierrätetään näiden maiden kautta. (Järvinen 2008.)

Tietoturvayhtiö McAfeen mukaan roskapostin määrä kasvoi huhti-toukokuussa 2009 80 prosenttia ensimmäisestä neljänneksestä. Sen luvuissa koko vuoden 2009 toista neljännestä tarkastellessa sähköpostista roskapostin määrä oli 92 prosenttia eli 150 miljardia roskapostia joka päivä. Tietoturvayhtiö Symantecin mittauksissa roskaposti vastasi kesäkuussa 2009 enimmillään 95 prosenttia kaikista viesteistä. Maailman suurin ohjelmistoyhtiö Microsoft on väittänyt, että jopa yli 97,3 prosenttia sähköpostiliikenteestä oli roskapostia vuoden 2008 lopulla. Alku vuonna 2009 roskapostia syytänyt internet-yhtiö McColon suljettiin. Se aiheutti kuitenkin vain tilapäisen laskun. (IT-viikko 2009b.)

On huomattu, että roskapostin lähetyksissä on piikki erilaisina juhtapäivinä. Myös kuuluisuuksien nimiä on käytetty hyväksi. Esimerkkinä Michael Jacksonin kuolemaan liittyy massasähköpostimato, joka lähetti roskaposteja otsikolla ”Remembering Michael Jackson”. Liitteensä oleva ”Michael Jackson songs and pictures.zip” sisälsi tiedoston nimeltään ”MichaelJacksonsongsandpictures.doc.exe”. Se oli kopio madosta, joka ajettiin käyttäjän koneelle, kun tiedosto avattiin. (Symantec 2009d.)

Symantec raportoi vuonna roskapostittajien käyttäneen Twitteriä syöttinä houkutellakseen viattomia uhreja phishing-ansaan. Siellä liikkui myös massasähköpostimato, joka näytti siltä kuin se olisi lähetetty Twitter-tililtä. Se poikkesi kuitenkin virallisesta Twitter-sanomasta, koska siinä oli pakkaus-tiedosto ”Invitation.Card.zip”, joka on tunnistettu massasähköpostimadoksi W32.AckanttaB@mm. Se kerää @-mail -osoitteita saastuneelta koneelta ja levittää liikuteltaviin ajureihin ja jaettuihin tiedostoihin. Tilastojen mukaan roskaposteja tulee eniten Yhdysvalloista, Brasiliasta ja Etelä-Koreasta. (Symantec 2009d.)

2.2.2 Palvelunestohyökkäys

Palvelunestohyökkäyksen kohteena on yritys. Kotikäyttäjälle koituu lähinnä haittaa, koska hän ei pääse haluamalleen sivustolle. Palvelunestohyökkäyksessä hyökätään verkkoliikennettä, systeemiresursseja sekä sovellusresursseja vastaan. Hyökkääjä ylikuormittaa yritykseen sisään tulevaa liikennettä. Tavoitteena on joko vaikeuttaa yrityksen toimintaa tai kaataa koko sivusto. Alun perin palvelunestohyökkäyksessä hyökkääjä oli mahdollista tunnistaa, koska hän käytti mahdollisesti yhtä lähdepalvelinta. Nykyään hyökkääjä voi myös väärentää lähdeosoitteita. (Stallings 2008, 250.)

Hajautetussa palvelunestohyökkäyksessä hyökkääjä antaa hallinnoimilleen zombie-koneille käskyn lähettää liikennettä kohdettaan vastaan. Hyökkääjä on alun perin saanut tavallisen kotikäyttäjän tietokoneen hallintaansa esimerkiksi asentamalla sinne takaoviohjelman. Zombiekoneiden muodostamia bottiverkkoja voidaan tämän jälkeen käyttää palvelunestohyökkäykseen. Nykyään hyökkääjä voi myös hallinnoida IRCin kautta. (Stallings 2008, 259)

Mikroblogi Twitter oli elokuussa 2009 nurin jonkin aikaa sitä vastaan tehdyn vihamielisen palveluestohyökkäyksen takia. Hyökkäyksellä yritettiin haitata ja estää käyttäjien pääsyä Twitteriin. Myös yhteisöpalvelu Facebookia vastaan tehtiin samana päivänä hyökkäys. Hyökkäykset hidastivat, mutta eivät kataneet sivuston toimintaa. (Iltasanomat 2009.) Twitterillä on noin 44 miljoonaa käyttäjää, joten vaikutukset olivat mittavat. (Taloussanomat 2009a.) Näissä kotikäyttäjä joutui suoraan haitan kärsijäksi.

2.2.3 Muut

Salakuuntelulla (sniffing) pyritään keräämään tietoja jonkin koneen tai jonkin verkon osan liikenteestä. Tietojen keräys voi olla salasanojen ja tilien numeroita. Tietokoneessa voi olla virus,

joka mahdollistaa hyökkääjälle oman yhteyden salakuunteluun. Salakuuntelua voi tapahtua myös verkonkuunteluohjelmalla. (Flyktman 2006, 295.)

Yhteyden kaappaamisessa hyökkääjä ottaa kahden osapuolen välisen tietoliikenneyhteyden hetkellisesti omaan hallintaansa ja pudottaa sinne omia komentojaan. Myös koko yhteys voidaan kaapata, kun olemassa olevaan yhteyteen on saatu ujutettua paketteja. Toinen osapuoli saadaan täten pudotettua kokonaan pois linjoilta. (Boström 2003, 49.)

Näppäimistökaappari on ohjelma, joka kaappaa salasanoja ja käyttäjätunnuksia. Se aktivoituu, kun uhri menee esimerkiksi verkkopankin sivulle. Tällöin ohjelma kaappaa syötetyt tunnukset muistiin ja lähettää ne isännälleen joko IRC-kanavalla tai sähköpostiviestinä. Koska Suomessa käytetään kertakäyttötunnuksia, pankkitunnusten urkinnasta ei ole vaaraa tämän haittaohjelman kohdalla. (Järvinen 2006, 89.)

Modeemikaappauksessa uhrin koneeseen lähetetään haittaohjelma, joka ohjelmoi modeemin tai ISDN-kortin soittamaan ulkomaiseen palvelunumeroon. Käyttäjä ei usein edes huomaa yhteyden uudelleen avausta ulkomaiden kautta. Tässä uhrille pyritään aiheuttamaan taloudellista vahinkoa. On huomattu, että laajakaistan yleistyminen on pienentänyt modeemikaappauksia. (Järvinen 2006, 89-92.)

Vakoilu- ja mainosohjelmia on paljon. Osa on harmittomia ohjelmia, joiden ainoa tehtävä on ohjata www-sivuilla näkyviä mainoksia tai lisätä toimintapalkki selaimeen. Osa on taas tietoja varastavia troijalaisia. Spyware oli alun perin vakoiluohjelma, joka tarkkaili käyttäjän surffausta ja keräsi siitä mainostajaa kiinnostavaa tietoa. Nyt sillä tarkoitetaan kaikkia salaa asentuvia tiedonkeruu- ja mainosohjelmia. (Järvinen 2006, 80.) Kesken surffauksen pidempää aikaa ilmestyvistä samaa tuotetta mainostavista mainosikkunoista yleensä huomaa spyware-tartunnan. Käyttäjä ei kuitenkaan huomaa samalla tapahtuvaa yksityisyyttä vaarantavaa henkilö- ja surffaustietojen keräämistä. (Järvinen 2006, 101.)

Valeturvaohjelmat ovat netistä löytyviä erilaisia apuohjelmia, jotka eivät kaikki ole sitä miltä näyttävät. Eräiden spywaren etsintäohjelmien on huomattu joskus olevan spywarea. Ne voivat kyllä poistaa näön vuoksi levyltä haittaohjelmia, mutta asentavat samalla omat haittaohjelmansa tilalle. (Järvinen 2006, 97.) Yleisesti suositellaan, että turvaohjelma hankitaan niin kutsutuilta tunnetuilta ja siten luotettaviksi tiedetyiltä toimittajilta.

2.3 Social engineering -hyökkäykset

Social engineering -hyökkäyksellä tarkoitetaan käyttäjän harhauttamista ja huijaamista. Siinä ei käyttöjärjestelmällä ja turva-aukoilla ole juuri mitään merkitystä. Näitä ovat phishing- ja pharming -hyökkäykset. Näiden kappaleiden yhteydessä käsitellään myös torjuntaa, koska se ei ole varsinaisesti tietoturvaan liittyvää teknistä torjuntaa.

2.3.1 Phising

Phising eli khalastelu eli kalastelu eli verkkohuijaus tarkoittaa tietojen urkkimista pahaaavistamattomalta käyttäjältä. Termi on yhdistelmä sanoista password ja fishing. Siitä voi jo päätellä että huijarit haluavat tietoonsa paitsi salasanoja myös pankkitilien numeroita, pinkoodeja ja käyttäjätunnuksia. Hyökkäys perustuu täysin käyttäjän huijaamiseen. Tietoja voidaan kalastella paitsi tietokoneella myös esimerkiksi puhelimella. Kanavana on kuitenkin yleensä sähköposti tai väärennetty www-sivu. Sähköpostin saaja saadaan kuvittelemaan olevansa viestin ainoa vastaanottaja. Tosiasiassa sähköpostiviestejä lähetetään miljoonia. Kalastelulla kokeillaan, kuka jää koukkuun. Kalastelijoiden on huomattu käyttävän samoja osoiterekistereitä kuin roskapostittajat. Yleensä viestejä kohdennetaan domain-nimen maakoodin mukaan eli esimerkiksi Suomeen fi-tunnuksen mukaan. (Järvinen 2006, 273-274.)

Suomessa ensimmäiset phising-huijaukset koskivat Nordean asiakkaita vuonna 2005. Viestit olivat englanninkielisiä. Ongelma on se, että viesti tuli pankista, josta on totuttu saamaan aitoa postia. Siihen oli siis tietty herkkyys vastata. (Järvinen 2006, 276.) Huijarit voivat lähettää käyttäjälle viestin uudesta turvaominaisuudesta ja pyytää kirjautumaan linkistä esimerkiksi pankin verkkosivulle ja päivittämään omat yhteystiedot. Kirjautuessaan palveluun käyttäjä luovuttaa tunnuksensa. Käyttäjä ei kuitenkaan huomaa, että pankin verkkosivu onkin kopioitu. (Järvinen 2006, 283-286.)

Tietoturvayhtiö Symantecin kesäkuun 2009 raportin mukaan phishing-hyökkäykset lisääntyivät kuukaudessa 21 prosenttia. Suurin syy kasvuun oli se, että 62 prosenttia hyökkäyksistä oli yksittäisiltä tunnetuilta sivuilta. Facebook oli kohteena toukokuussa 2009. (Symantec 2009c.) Yksi tuoreimmista phising-hyökkäyksistä Suomessa on elokuun 2009 alusta, jolloin sähköposteihin virtasi jälleen Nordean nimissä lähetettyjä huijaussähköposteja. Niissä pyydettiin verkkopankin asiakastunnuksia. Viestit olivat suomenkielisiä, mutta ne oli kirjoitettu erittäin huonolla suomella. (Helsingin Sanomat 2009.)

Viestin aitoutta kannattaa epäillä, jos saa viestin pankilta, jonka asiakas ei ole. Koneellinen kielenkäännös pitäisi myös herättää miettimään. Sivun päiväys ja kellonaika voi olla väärä. Huijaussivun URL-osoite voi olla outo. Lukon kuvaan on totuttu luottamaan, mutta aina se ei tarkoita suojattua yhteyttä. Maakoodi ja epästandardi porttinumero kertovat myös jotain, jos ymmärtää siitä jotain (Järvinen 2006, 286-289.) Viimeksi mainitut voivat toki olla tavalliselle kotikäyttäjälle hankalia huomata.

Phisingista oli liikkeellä kesäkuussa 2009 uudentyyppinen esimerkki Australiasta. Huijarit lähettivät Australian veroviraston nimissä verolomakkeen omilla tiedoillaan. Print-napin painaminen lähetti lomakkeen rikollisille. Hyökkäys tapahtui mm. saksalaisilta ja itävaltalaisilta saastuneilta palvelimilta. (IT-viikko 2009a.)

2.3.2 Pharming

Pharmingissa käyttäjä ohjataan automaattisesti valesivustoon eli käyttäjän ei tarvitse painaa mitään linkkiä. Hän luulee olevansa oikealla rahalaitoksen tai kauppiaan sivulla.. (Symantec 2009b.)

Tavallisimman muodon pharming-hyökkäyksessä on huomattu olevan paikallisen tietokoneen DNS-tietojen (nimipalvelin) myrkytys, jossa tietokone tallentaa kopion aikaisemmin selattujen sivustojen DNS-tiedoista DNS-valimuistiin. Välimuistia voidaan muokata troijalaisen avulla. Kun käyttäjä kirjoittaa selaimeen verkkopankkinsa osoitteen, hänet ohjataankin valesivustoon. Käyttäjä paljastaa samalla kirjautumistietonsa. Harvinaisempi muoto on sivustojen välisessä komentosarjahyökkäyksessä (XSS-hyökkäys). Siinä hakkeri yrittää murtautua aitojen sivustojen ohjelmistokoodiin. Sinne hakkerilla on tavoitteena ujuttaa komentosarja, joka ohjaa sivuston kävijöitä valesivustoon. Sivustoon voidaan esimerkiksi lisätä linkki. Aidon sivuston päälle voi myös avautua valeselainikkuna. Hakkerin syöttämä komentosarja voi myös käyttää hyväkseen selaimen tietoturva-aukkoa ja saastuttaa sivustoa selaavien käyttäjien tietokoneen. (Symantec 2009b.) Yksi ensimmäisistä pharming-hyökkäyksistä tapahtui vuonna 2005. Siinä hyökkääjä kaappasi web-sivun. Sitten hän muutti alkuperäistä sivua siten, ettei sinne päässyt. (Symantec 2009a.) Täten aiheutettiin vahinkoa kyseessä olevan yrityksen liiketoiminnalle.

Parasta torjuntaa pharming-hyökkäystä vastaan on todettu olevan käyttäjätunnusta pyytävän sivuston URL-osoitteen tarkistus, virustorjuntaohjelman pitäminen ajan tasalla, valitsemalla luotettava internet-palvelutarjoaja, ja tarkistamalla sivun voimassaoleva turvasertifikaatti. On myös muistettava, ettei koskaan siirry nettisivulle suoraan sähköpostiviestin, pikaviestin, mai-

nospalkin tai ponnahdusikkunassa annetusta linkistä. Käyttäjätunnusta ja salasanaa ei saa antaa missään nimissä. Varmuuden vuoksi on hyvä tarkistaa pankkitilin ja luottokortin tapahtumat joka kuukausi epäilyttävien tapahtumien varalta. (Symantec 2009b.) Viimeksi mainittu neuvo ei liity vain pharming-hyökkäykseen vaan myös phisingiin.

2.4 Tulevaisuus menneen kautta

Tietoturvayhtiö MacAfeen toisen kvarttaalin raportti vuodelta 2009 osoitti, että kesäkuun 2009 roskapostiluku oli suurin sitten lokakuun 2008. Haittaohjelmista salasanoja varastavan troijalaisen rooli oli noussut. McAfee arvioi, että zombien määrän kasvu ennakoi sitä, että roskapostin ja muiden haittaohjelmien lähettäminen kasvaa. Hyökkääjät johtivat käyttäjät haitalliselle sivulle asettamalla häiritseviä scriptejä koneeseen. Näistä tunnetuimpia on Gumblar. Hyökkääjien arvellaan etsivän uusia keinoja piiloutuakseen. (McAfee 2009, 1-8.). Lähteitä lukiessa ei missään näytä siltä, että tämä kehitys ei pysähdy. Uudet tekniikat mahdollistavat erilaisia oppimisväyliä myös rikollisille.

Jotta kyetään pysymään jotenkin rikollisten jäljillä ja pystyttäisiin jossain vaiheessa tyystin lopettamaan tuo toiminta, erilaisten viranomaisten on ollut pakko ryhtyä toimiin. Yksi esimerkki on internetin osoite- ja verkkotunnushallintoa koordinoiva ICANN sekä tietojen varastelutoiminnan torjumiseen keskittyvä APWG (Anti-phishing Working Group). Ne ovat käynnistämässä hanketta, jossa phishing-toimintaan käytettävät, virheellisillä tiedoilla rekisteröidyt verkkotunnukset saataisiin suljettua jo muutaman tunnin kuluessa havaitun huijauksen raportoinnista. ICANN on tarkentamassa verkkotunnusten rekisteröintipalvelujen tarjoajien valvontaa ja ohjeistusta. Molemmat tahot ovat korostaneet tarvetta tiiviiseen yhteistyöhön erityisesti CERT-FI:n kaltaisten kansallisten CERT-yksiköiden kanssa. Esimerkkinä CERT-FI:n toiminnasta voi mainita apu ulkomaisille viranomaisille selvittää tapaus, johon liittyi pankkitietoja varastava haittaohjelma. Ohjelmaa levitettiin latvialaisen palveluntarjoajan verkko-osoitteiden kautta. Selvitystyön yhteydessä ilmeni, että samaa verkkoa käytettiin useiden eri haittaohjelmien jakelualustana. Tapahtumaketjun lopputuloksena palveluntarjoajan verkko-operaattori katkaisi sen verkkoyhteydet käyttöehtorikkomuksen perusteella. (Cert-Fi 2009.)

Tulevaisuudessa voidaan olettaa, että palvelunestohyökkäyksiä tullaan enenevässä määrin käyttämään erilaisiin poliittisiin tarkoituksiin. Tästä on nähty jo esimerkkejä, kun vuosina 2007 ja 2008 Viron ja Georgian poliittiset levottomuudet näkyivät myös tietoverkoissa. Verkkojen ja tietoyhteiskunnan palveluiden toimintaa häirittiin muun muassa palvelunestohyökkäyksin. Toukokuussa 2009 pidettyjen Iranin presidentinvaalien aikana yhteisö- ja julkaisupalveluista

tuli kanava, jonka kautta yksityishenkilöt välittivät tietoja ja näkemyksiä Iranin tapahtumista vallinneissa poikkeusolosuhteissa. Keskustelupalstoja ja blogisivustoja käytettiin myös vastakkaisten näkemysten levittämisen häirintään. Sivustoilla jaettiin tavallisille tietokoneiden käyttäjille ohjeita siitä, miten he voivat valjastaa työasemansa ja internet-yhteytensä palvelunesto-hyökkäykseen. Toteutetuissa hyökkäyksissä käytettiin varsin vähän bottiverkkoja, ja ne toteutettiin esimerkiksi http-pyyntöjä generoimaan suunniteltujen www-sivustojen avulla. (Cert-Fi 2009.)

Kun tähän asti lukemaansa muistelee, voi huomata, että uhat ovat todella muuttuneet. Kotikäyttäjä on massaa, johon kohdistetaan kolkutuksia etsittäessä suojaamattomia koneita. Kun kyseessä oleva kone on löydetty, se voidaan valjastaa erilaisiin tarkoituksiin. Pahimmillaan kotikäyttäjä huomaa koneensa pimentyneen tai menettäneensä rahansa. Suurempi todennäköisyys näyttää kuitenkin olevan, että hän ei pääse jonkin yrityksen sivustolle ja/tai sitten hänen koneensa on valjastettu hyökkäykseen kyseessä olevaa yritystä vastaan. Kotikäyttäjä voi kuitenkin vaikuttaa omilla toimillaan oman koneensa luvattomaan käyttöön. Ensimmäinen askel on tietoisuus omasta vastuusta. Internet on paitsi tuonut kaikkea mukavaa tietoa omalle kotisohvalle, mutta myös oman vastuun tietokoneen suojauksesta. Suojausta käsitellään seuraavassa kappaleessa.

Tulevaisuus ei siis näytä kovinkaan hyvältä. Arvellaan, että hyökkäykset lisääntyvät mikroblogeihin. Tämän takia näissä on jo tartuttu tähän ongelmaan. Tuorein Nordean verkkopalvelussa pyörinyt haittaohjelma vuodelta 2010 on sen kaltainen uutinen, joita voi odottaa enemmänkin. Siinä Nordean asiakkaita joutui haittaohjelman uhriksi. Haittaohjelma näkyi asiakkaan koneella siten, että Nordean verkkopankin suomenkielinen sisään kirjautumissivu oli muuttunut englanninkieliseksi. Sivulla huomautettiin huoltotoimenpiteistä, jotka kestävät 24 tuntia. Jos asiakas kirjautui verkkopankkiin, pääsi hyökkääjä siirtämään varoja asiakkaalta tämän tietämättä. Haittaohjelmaa ei havaittu muissa pankkikonsernin maissa kuin Suomessa. (Nieminen 2010, A15.) Nordea korvasi asiakkaiden kärsimät tappiot.

Kuten jo todettiin aiemmin, viranomaisten on hyvä lisätä yhteistyötään yhteisen uhan torjuntaan. Valitettavasti tätä ei kaikkialla nähdä samalla tavalla kuin länsimaissa. Brasiliassa toimivalle hakkerille lisätienesti on varmasti tervetullut lisä eikä siellä kyetä näkemään uhkaa samalla tavalla kuin uhan kärsivissä maissa. Tekninen torjunta on suuressa roolissa verkkorikollisuuden torjunnassa. Sitä käsitellään seuraavassa kappaleessa.

3 Torjunta

Tietoturvan päätavoitteet ovat luotettavuus, eheys ja käytettävyys. Luotettavuus liittyy tiedon luotettavuuteen sekä yksityisyyteen. Tiedon luotettavuus takaa sen, että yksityinen ja luottamuksellinen tieto ei paljastu eikä päädy sellaisille henkilöille, joille se ei kuulu. Yksityisyys takaa sen, että yksityiset henkilöt voivat kontrolloida ja vaikuttaa mitä heihin liittyvää tietoa voidaan kerätä ja varastoida ja kenelle tietoa voidaan luovuttaa. Eheyteen kuuluu tiedon eheys ja systeemin eheys. Tiedon eheys takaa, että tieto ja ohjelmat vaihtuvat tietyllä luvallisella tavalla. Systeemin eheys takaa, että systeemi toimii alkuperäisellä tavallaan vapaana tavalliselta ja huomaamattomalta luvattomalla systeemin manipuloinnilta. Käytettävyys takaa, että systeemi toimii tarkasti ja että palvelua ei kielletä luvallisilta käyttäjiltä. (Stallings 2008, 7-8.)

Tietoturvalla tarkoitetaan eri yhteyksissä eri asioita. Joillekin se on vain varmuuskopioiden ottamista. Tämä toki takaa sen, ettei tietoja menetetä lopullisesti, kun jokin haittaohjelma on tuhonnut tietokoneen. Tässä esityksessä on keskitytty verkkorikollisuuteen. Tietoja voidaan menettää muutenkin kuin haittaohjelman tuhoamana. Tiedostoja voidaan poistaa tai tallentaa vahingossa väärin, sähkökatkokset voivat vioittaa auki olleita tiedostoja, ylijännitteet voivat rikkoa laiteosia, tulipalo tai vesivahinko voi aiheuttaa tuhoa, tietokone voidaan varastaa tai voit vain pudottaa tietokoneen. (Flyktman 2006, 292.) Tässä esityksessä ei käsitellä näitä asioita torjunnan kannalta vaan keskitytään verkkorikollisuuteen liittyvään torjuntaan.

Myöhemmin tässä kappaleessa on lueteltu erilaisia teknisiä ratkaisuja, miten suojautua haittaohjelmia ja muuta vastaan. Kuitenkin on muistettava, että osa tietoturvaa on ihmisen rooli. Tietoturvapaketit eivät poista ihmiseen omaan toimintaan liittyviä tietoturvaongelmia. Sen tähden seuraavassa kappaleessa on lueteltu sellaisia keinoja, joita jokainen voi noudattaa. Luettelo on kasattu Petteri Järvisen ajatuksista.

Yes-klikkaus ei ole aina viisasta varsinkaan, jos ei ymmärrä kysymystä. Kun netistä päättää ladata mainostetun turvaohjelman, pitää muistaa, että myös valeturvaohjelmia on olemassa. Lisäohjelmien asennuksessa kannattaa kuunnella muiden käyttäjien suosituksia tai lukea lehdestä lisätietoja. Koneen sammutus ja irrotus verkkoyhteydestä kannattaa, jos tietokone on pidempiä aikoja käyttämättä. Käytettäviin spyware- ja virustorjuntaohjelmiin ei kannata luottaa sokeasti. Tietokoneessa valmiiksi oleva palomuuri ei auta mitään, jos se ei ole käytössä. Käyttöjärjestelmän ja selaimen säännöllisistä päivityksistä kannattaa huolehtia. Selaimen ja sähköpostiohjelman vaihtaminen vähemmän suosittuun kannattaa. Haittaohjelmien tekijät eivät ole vält-

tämättä kiinnostuneita niistä. (Järvinen 2006, 103.). Viimeinen lause ei ole välttämättä absoluuttinen totuus, sillä haittaohjelmia voi löytyä myös muista kuin Microsoftin tuotteista.

3.1 Palomuuri

Palomuurin merkitys on ollut kauan hallitseva torjunnassa. Tämä onkin riittänyt pitkään mutta ei nykyään enää ainoa turvana. Palomuuri suojelee kotikäyttäjän tietokonetta hyökkäyksiltä. Suoja liittyy turva-aukkoihin, joita ei ole päivitetty tai vielä edes löydetty. Palomuuri on erikoistunut yhteyksien käsittelyyn. Se pystyy pitämään yksittäistä työasemaa paremmin kirjaa kaikista yhteyksistä ja havaitsemaan tarkoitukselliset ylikuormitustilanteet, jolloin liikenne kyseisestä IP-osoitteesta pudotetaan kokonaan pois. Vain palomuuri pystyy havaitsemaan tietokoneesta ulospäin lähtevän liikenteen ja tarvittaessa estämään sen. Palomuuri torjuu lähinnä hakkereita. Se ei kuitenkaan estämään käyttäjän toimintaa, jos tämä päättää hyväksyä jonkin haittaohjelman lataamisen. (Järvinen 2006, 104-107.)

Palomuurit ovat joko erillisiä laitteita (rautapalomuurit) tai tietokoneessa toimivia ohjelmia (softapalomuurit). Kotikäyttäjä voi valita jommankumman. Windosw XP:ssä ja Vistassa on oma palomuuri. Sen on todettu täyttävän minimitarpeet. (Järvinen 2006, 116-117.) Myös Linuxissa ja OS X:ssä on vakiona palomuuriohjelma. (Järvinen 2006, 106.) Maksullisten turvaohjelmien lisäksi on tarjolla ilmaisia vaihtoehtoja kuten Comodo Firewall Pro. Koska palomuurin ei yksistään ole todettu riittävän, sen lisäksi yleisesti suositellaan vakoojaohjelmien poistajaa. (Tietokone 2008.)

3.2 Virustentorjuntaohjelma

Virustentorjuntaohjelman hankinta ja sen automaattinen päivitys ovat hyvä turva. Se tutkii taustalla nettiselailua, verkkoliikennettä, tiedostojen käsittelyä eli oikeastaan kaikkea koneen toimintaa. Se hidastaa melkein kaikkea käyttöä, joka on yksi syy, miksi sitä ei välttämättä hankita.. Tyypillisesti turvapaketti hidastaa tietokonetta 5-10 prosenttia. (Kotiranta 2009.) Tämän työn kirjoittaja oli vähällä, ettei poistanut koko F-Securen virustentorjuntaohjelmaa, koska se latautui koneelle niin hitaasti. Ilmeisesti F-Secure teki jonkin parannuksen, koska uusin versio latautuu nopeammin.

Suomessa tarjolla olevista turvapaketeista F-Securen ja Nortonin pakettien osuus on arvion mukaan ollut kummallakin noin kolmanneksen osuus kotipaketeista. Noin viidennes markkinoista on ilmaisilla virustorjuntaohjelmilla ja niiden maksullisilla versioilla. Suomenkielisiä pa-

ketteja on myös Pandalla, McAfeella ja Normanilla. Ne vievät valtaosan lopusta kymmenestä prosentista. Muut tietoturvapaketit ovat englanninkielisiä. Tietoturvapaketit eroavat erilaisten suojauskerrosten mukaan. Eroja on myös lisäominaisuuksista. Monissa paketeissa on varmuuskopiointiohjelma ja tietokoneen tehon viritys. Ilmaisen version ei ole huomattu tarjoavan kaikkia suojauskerroksia. (Kotiranta 2009.)

Kun hankkii tietoturvaohjelmaa, on hyvä varoa valeturvaohjelmaa, josta on jo ollut aiemmin puhetta. Se voi putsata jotain, mutta voi myös tuoda jotain haitallista mukanaan.

3.3 Päivittäminen

Oman tietokoneen päivittäminen on tärkeä osa tietoturvaa ja taistelua erilaisia haittaohjelmia vastaan. Tällä ei tarkoiteta vain käyttöjärjestelmiä vaan myös sovelluksia ja käytettyjä ohjelmia mukaan lukien hankittu virustentorjuntaohjelma. Teknisellä päivittämisellä ei kyetä vaikuttamaan inhimilliseen toimintaan. Omia tietoturvataitoja voi toki päivittää.

Kaikki käyttöjärjestelmät vaativat jatkuvaa päivittämistä. Suositeltavaa on, että päivitykset tehdään kerran viikossa. Jos päivitysautomatiikka on käytössä, tästä ei tarvitse huolehtia itse. Eri käyttöjärjestelmät toimivat hieman eri tavalla. Windowsissa on mahdollisuus käyttää automaattista päivitystä. Macintoshin OS X -käyttöjärjestelmässä päivityksiä ei asenneta automaattisesti vaan käyttäjä saa ilmoituksen saatavissa olevista päivityksistä. Unix-käyttöjärjestelmässä ei ole yhtenäistä tapaa hoitaa päivitystä. (Järvinen 2006, 34-35.)

Päivittäminen ei liity vain tietokoneisiin vaan myös muiden teknisten laitteiden kuten digiboksien päivityksistä on huolehdittava. Tämä johtuu siitä, että tekniset laitteet tuodaan yleensä myyntiin kiireellä ja keskeneräisinä. Kiireen vuoksi niihin jää virheitä, joita joudutaan paikkailemaan jälkikäteen. (Järvinen 2006, 15.) Virheitä ei aina edes huomata heti. Vuonna 2005 käytettiin Windowsissa alun perin kuvatiedostoon upotettua ohjelmakoodia haittaohjelman levittämiseen. Ohjelmakoodi oli tuolloin ollut olemassa jo 15 vuotta ja siirtynyt jopa uuteen versioon. Kyseessä oli ns. nollapäivähyökkäys, johon ei ollut heti saatavilla korjausta. (Järvinen 2006, 23.)

Tavallisessa päivittäisessä käytössä olevissa sovelluksissa voi myös olla ohjelmistovirheitä. Ne on siis hyvä päivittää. Esimerkiksi Office 2003 Excelissä oli bugi, jonka seurauksena satunnaislukufunktio palautti joskus negatiivisia arvoja vastoin määritelmää. On huomattu, että myös muuttunut roskaposti- ja phishing-tilanne vaatii myös sovellusten päivittämistä. Työtiedostot

voivat laukaista ohjelmissa virhetoimintoja ja jopa ladata netistä jonkin haittaohjelman. Näitä virhetoimintoja voidaan käyttää tietoturvahyökkäyksiin jakamalla työtiedostoa, joka aiheuttaa sovelluksessa puskurin ylivuodon. Joissakin tapauksissa hyökkääjä voi saada koneen täysin hallintaansa yhden ainoan työtiedoston avulla. Aukon hyödyntäminen tosin edellyttää, että uhri saadaan lataamaan ja avaamaan tietty työtiedosto. Tiedosto voidaan asettaa esille www-sivulle tai lähettää sähköpostilla sopivasti houkuttelevan saatteen kera. Myös musiikkiohjelman soittolistat voivat olla näin vaarallisia. Vaarallisia turva-aukkoja on löydetty mm. Microsoftin Media Playerista sekä Adobe Acrobat -lukuohjelmasta.(Järvinen 2006, 17-18.)

Arvio on, että kaupallisissa ohjelmissa on yhdestä seitsemään virhettä tuhatta ohjelmariviä kohti. Osa voi aiheuttaa epämääräisiä kaatumisia, osa on täysin huomaamattomia. Valitettavasti osa virheistä on sellaisia, että niiden kautta voidaan aiheuttaa vahinkoa ohjelmalle tai jopa saada ohjelma suorittamaan aivan vierasta koodia. (Järvinen 2006, 23-24.) Näiden päivityksistä huolehtiminen on siis erittäin tärkeää.

3.4 Käyttöjärjestelmät ja selaimet tietoturvan näkökulmasta

Tietoturvan näkökulmasta Windowsiin on tehty eniten hyökkäyksiä. Hyökkääjät ovat kuitenkin enemmänkin yrittäneet maksimoida saamansa hyödyn ja siksi Windows on historiallisesti ollut useammin hyökkäysten kohteena. Windowsilla on ollut suuremmat käyttäjämäärät kuin muilla käyttöjärjestelmillä. Vuoden 2009 tilaston mukaan sen markkinaosuus on 92,2 prosenttia. (Keizer, 2010.) Tämä ei kuitenkaan tarkoita sitä, että ainoastaan Windowsista löytyy tietoturva-aukkoja.

Eri käyttöjärjestelmät ja selaimet voivat tarjota erilaisia tietoturvaratkaisuja. Kuitenkin on muistettava, että riippumatta siitä, mitä käyttöjärjestelmää tai selainta käyttää, on tärkeää muistaa pitää huolta saatavista tietoturvapäivityksistä joko automaattisesti tai manuaalisesti.

3.4.1 Microsoft Windows

Kun Windows vuonna 1985 esiteltiin, tietoturva ei ollut ykkösasia. Tämä voi olla suurin syy Windowsin ongelmiin tietoturva-asioissa. Windows on kuitenkin jokaisessa uudessa versiossaan pyrkinyt vastaamaan ympäröivän toimintaympäristön tietoturvahaasteisiin. Kaikissa Windowseissa on Windows XP:stä lähtien ollut sisäänrakennettuna palomuuri. Kun tähän työhön liittyvään tutkimukseen liittyvä kyselylomake lähetettiin kohderyhmälle, Windows Vista oli viimeisin Microsoftin käyttöjärjestelmä. Tätä työtä kirjoitettaessa on Microsoft julkaissut sekä

selaimestaan että käyttöjärjestelmästään uudet tuotteet. Käyttöjärjestelmässä uusin tuote on Windows 7.

Vistassa on palomuuri sisäänrakennettuna. Microsoftin suositeltavat asetukset sille ovat, että palomuuri on käytössä kaikissa verkkosijainneissa (esim. kotona), että se on käytössä kaikissa verkkoyhteyksissä. Palomuuri torjuu ne sisään tulevat yhteydet, jotka eivät vastaa mitään poikkeusta. Jos tietokoneessa on jo jokin toinen palomuuri, suosituksena on se, että käytetään vain yhtä palomuuria, koska toinen voi sotkea toisen toimintaa. (Microsoft 2010.)

Vistasta alkaen Windowsissa on ollut Windows Defender, joka on Windowsin oma ohjelma vihamielisiä ohjelmia vastaan. Defender ei kuitenkaan ole virustentorjuntaohjelma. Se on siis hankittava erikseen. Defender muun muassa ilmoittaa, kun jokin haittaohjelma pyrkii koneelle. Tämän työn kirjoittajalla on tästä omakohtaisia kokemuksia.

3.4.2 Linux

Linus Torvaldsin vuonna 1991 kehittämä Linux on maailman suosituin vapaasti käytettävä käyttöjärjestelmä. Ubuntu on Linuxista täysin vapaa versio. Red Hat Enterprise Linux on kaupallisesti tuettu. Linuxissa on rakennettuna palomuuri. Erilaisia virustorjuntaohjelmia on saatavilla myös Linux-versioihin.

Historiallisesti Linux ei ole ollut niin haavoittuva viruksille kuin muut käyttöjärjestelmät. Tämä ei johdu siitä, että Linux olisi turvallisempi. Virus-kirjoittajat haluavat kuitenkin maksimoida tuoton. Windows on siis suuremman käyttäjämääränsä takia ollut suuremman uhan kohteena. Palvelunestohyökkäys, Web-sovellus haavoittuvuudet ja rootkit-hyökkäykset ovat olleet perus-Linuxin yleisimmät haavoittuvuudet. (Stallings 2008, 700-1.)

On arveltu, että Linux-virusten suosio kasvaa käyttöjärjestelmän suosion kasvun mukana. Linux-käyttäjä on myös yhtä vaarassa inhimillisille virheilleen. Jos hän hyväksyy luvattoman ohjelma, siinä ei Linuxin turvallisuus paljon auta.

3.4.3 Macintosh OS

Mac OS on Applen kehittämä käyttöjärjestelmä. Markkinoille se tuli vuonna 1984 Macintosh-koneissa. Mac OS X on siitä uudempi versio. Tietoturvan näkökulmasta Macia on perinteisesti pidetty turvallisena käyttöjärjestelmänä. Siinä on sisäänrakennettu palomuuri. Siihen on myös

mahdollisuus saada virustentorjuntaohjelma. Vaikka Mac koetaankin turvalliseksi, ESET:in (Edge Research and Communications Inc.) tekemässä tutkimuksessa amerikkalaisista Mac-käyttäjistä moni verkkorikollisuuteen liittyvistä tappioista on liittynyt phisingiin. Eli riippumatta käytettävästä käyttöjärjestelmästä käyttäjää voidaan huijata. Samaisessa tutkimuksessa kävi ilmi, että 57 prosenttia Mac-käyttäjistä katsoi olevan turvallista käyttää konetta ilman mitään virustentorjuntaohjelmaa. Vastaava luku PC-käyttäjissä oli 27 prosenttia. (ESET Threat Blog 2009.)

3.4.4 Selaimet

Missä on vika, kun Saksan ja Ranskan tietoturvaviranomaiset saivat tammikuussa 2010 suosittelemaan jonkin muun valmistajan selaimen käyttöä väliaikaisesti? Syynä tähän oli Internet Explorerissa paljastuvien tietoturva-aukkojen paljastuminen. (Pullinen 2010, A8.) Tietoturva on siis mitä suurimmassa määrin ei ainoastaan käyttöjärjestelmiin liittyvä ongelma vaan se liittyy myös selaimiin.

Windows-käyttöjärjestelmän mukana tulee oletuksena Microsoftin oma selain Internet Explorer. Tästä on uusin versio Internet Explorer 8. Jos käyttäjällä on ollut automaattinen päivitys, uusin versio päivittyi automaattisesti. Uusi selain ei kuitenkaan takaa turvallista oloa, sillä uusiin versioihin voi melkein heti tulla korjausversioita. Näin tapahtuikin, sillä Googlea vastaan tehtiin hyökkäys selaimesta löydetyn aukon avulla. Microsoftin selain on suosituin käytössä olevista. Aivan kuin käyttöjärjestelmäpuolella hyökkääjä saa hyödyn maksimoitua, kun hän kohdistaa hyökkäyksen suosituimpaan selaimeen. Tämän takia nimenomaan IE on ollut hyökkääjien kohde.

Mozilla Firefox, Opera ja Safari ovat ilmaisia selaimia. Varsinkin Firefoxin suosio on kasvanut, koska IE:stä on löytynyt haavoittuvuuksia. Vaikka Safari on myös Applen tuote, sitä voi käyttää myös Windows-käyttöjärjestelmän kanssa.

3.5 Torjunnan tulevaisuus

Mikä on tietoturvan tulevaisuus? Jos isoon yritykseen voidaan tehdä keskitetty palvelunesto-hyökkäys huolimatta resursseista, joita panostetaan tietoturvaan, miten yksityinen kotikäyttäjä voi selvitä siitä, ettei hänen koneensa ole osa zombie-koneiden verkostoa. Viitekehyksen toisessa kappaleessa luotiin katsaus siihen muutokseen, mitä haittaohjelmissa on tapahtunut. Ehkäpä kotikäyttäjä on siinä mielessä turvatummassa asemassa kuin ennen, sillä hänen konettaan

halutaan käyttää salaa eikä välttämättä haluta tuhota tiedostoja. Kotikäyttäjälle se, ettei hän pääse palvelunestohyökkäyksen kohteena olevalle sivustolle, on lähinnä haitta. Yritykselle siitä taas koituu joskus taloudellista tappiota ja imagon menetystä.

Koska kuitenkin kotikäyttäjän konetta käytetään välillisesti hyökkäyksiin, on ollut pakko miettiä erilaisia ratkaisuja. Näyttää siltä, että nykyajan tietotokoneissa tietoturvapaketti on melkein osa sen varustetasoa. Jotkut eivät kuitenkaan ota sitä käyttöön, koska se hidastaa tietokoneen käyttöä. Kun joku tekee päätöksen kävellä päin punaista valoa vastoin liikennesääntöjä, miten tähän voidaan puuttua muuten kuin sakottamalla. Pitäisikö kotikäyttäjää sakottaa siitä, että hän ei halua noudattaa tietoturvan perusohjeita. En ole kuullut, että kukaan olisi esittänyt tätä. Ratkaisu voikin olla siinä, että viedään tietoturvan miettimispäätös kotikäyttäjältä kokonaan pois.

Tietoturva ei ole pelkkää tekniikkaa. Niin kauan kuin joku haluaa ostaa internetistä esimerkiksi viagraa, rikolliset saavat kotikäyttäjä-uhrinsa verkkoonsa. Rikollisen nettisivun lataus johtaa kotikäyttäjän tietokoneen tutkintaan. Aukkoja löytyy helposti etenkin selainten lisäosista, sillä niitä ei päivitetä automaattisesti. Tuossa ei auta se, että Windows on tehnyt töitä tietoturvan parantamiseksi. Tilaston mukaan nettiselaimista löytyi vuonna 2008 kymmeniä kriittisiä turva-aukkoja, mutta selainten lisäosissa niitä oli satoja. Kun turva-aukko löytyy, siihen tarjoutuu juuri tuohon aukkoon sopiva haittaohjelma. Haittaohjelmilla on kyky muuntautua. Aiempi virustunniste ei välttämättä tunnista hieman muutettua haittaohjelmaa. (Kotiranta 2009.) Eli mitä tehdä? Kieltää Viagra? Tuskin onnistuu.

Tuholaisten määrä nousi vuonna 2008 miljoonaan. Sitä edellisenä vuonna nousu oli puoleen miljoonaan. Tuhansien uusien virustunnisteiden syöttäminen koneille ja haittaohjelmien jatkuva muuttuminen on ongelma. Yhä useammin koneelle yrittävä tuholainen ei olekaan ennestään tunnettu, eikä sitä varten ole vielä tehty virustunnistetta. Turvapakettien onkin ollut pakko siirtyä yhä tiukempiin ennakoiviin suojauksiin, jotka etsivät tietokoneelta haitallista toimintaa. Tämä on osoittanut hankalaksi, koska monesti on ollut esimerkiksi vaikea erottaa asennusohjelmaa viruksesta. Testeissä esimerkiksi Norton erehtyi luulemaan Ontrack Eraser -ohjelman asennusohjelmaa Adware.Rabio-haittaohjelmaksi. (Tietoturva nousee pilviin 2009.) On siis ollut pakko keksiä jotain.

Eräänä ratkaisuna on pidetty tietoturvan siirtämistä pilveen. Puhutaan Pilti-it:stä. Se sisältää muutakin kuin tietoturvaan liittyviä asioita. Tietoturvan näkökulmasta haittaohjelmien tietokanta on siinä internetissä eikä tietoturvayhtiöiden tarjoamana käyttäjän koneella. Mallissa tietoturvapaketti tarkistaa mahdollisen haitallisen ohjelman virustunnisteen ensimmäiseksi inter-

netistä. Nettipalvelussa voi säilyttää miljoonia virustunnisteita. Uusi virustunniste on heti kaikkien käytettävissä. Nyt lataus on voinut kestää pahimmillaan tunteja. Käyttäjän koneen virustietoa käytettäisiin vain, jos internet ei toimi. (Kotiranta 2009.)

Internetissä voidaan myös ylläpitää valkoisia listoja, jossa on toinen lista puhtaiksi ja asiallisiksi tiedetyistä ohjelmista. Täten turvalliseksi tiedettyjä tiedostoja ei tarvitse tutkia. Valkoinen lista parantaa myös tietoturvaa. Kun väärät hälytykset eivät enää uhkaa valkoisella listalla olevia ohjelmia, voidaan suojaukset säätää tiukemmalle ja turvan taso nousee. Tähän asti käytetyt valkoiset listat ovat olleet suppeita. Netissä listan pituudella ei ole mitään rajaa ja sitä voidaan päivittää reaaliajassa. Symantec on kehittänyt valkoisista listoista version, jossa käytetään apuna käyttäjäkunnalta automaattisesti kerättävää tietoa. Suomessa tarjolla olevat F-Secure, McAfee, Panda ja Symantec ovat myös kehityksessä. Pilvi-it keventää tietoturvapaketteja. Tekniikkaa käytetään myös internet-varmuuskopioinnissa. (Kotiranta 2009.)

4 Aineisto ja tutkimusmenetelmät

Kuten johdannossa todettiin, tutkimuksessa on tavoitteena eri tutkimusongelmien kautta käydä läpi, mikä on tietyn Nordean yksikön henkilöiden tietämys viitekehyksessä esitetyistä aiheista.

4.1 Tutkimusongelmat

Tutkimusongelmat voi kiteyttää kahteen kohtaan eli

1) Tunteeko kohderyhmä tämän ajan käsitteet, jotka liittyvät omaan kotitietokoneeseen kohdistuviin uhkiin sekä mikä on heidän suhtautumisensa tähän liittyvään roskapostiin?
2) Osaako kohderyhmä huolehtia kotikoneensa tietoturvasta?

Edellä kuvattuja ongelmia analysoidaan tutkimuksessa asiaan perehtyneisyyden ja ikäryhmävertailujen kautta.

4.2 Tutkimusmenetelmä

Tutkimus toteutettiin kvantitatiivisena survey-tutkimuksena. Siinä pyrittiin noudattamaan kvantitatiivisen tutkimuksen keskeisiä periaatteita, jotka ovat: johtopäätökset aiemmista tutkimuksista, aiemmat teoriat, hypoteesien esittäminen, käsitteiden määrittely, havaintoaineiston tulee soveltua määrälliseen mittaamiseen, aineiston saattaminen tilastollisesti käsiteltävään muotoon sekä päätelmien teko havaintoaineiston tilastolliseen analysointiin perustuen. (Hirsjärvi, Remes, Sajavaara 136, 2007) Tutkimustuloksia oli tarkoitus vertailla käyttäen khiin neliö -riippumattomuustestiä. Se on kuitenkin tarkoitettu suurten otosten tilastolliseen analysointiin. Sitä ei myöskään voi tehdä, jos tulosjoukossa on vähemmän kuin viisi yksilöä. Tämän testin tuloksissa oli useammassa kohdassa vähemmän kuin viisi yksilö. Testaus ei siis olisi antanut oikeaa kuvaa. (Tietojen arvioiminen.)Tulosten analysoinnissa on siis käytetty pelkästään prosenttilukujen vertailua.

Kohderyhmää oli tarkoitus verrata MAAWGin (Messaging Anti-Abuse Working Group) tutkimukseen ”A Look at Consumers’ Awareness of Email Security and Practises or ”Of Course, I Never Reply to Spam - Except Sometimes””. Tutkimus tehtiin Yhdysvalloissa ja Kanadassa vuonna 2008-9. Analysointivaiheessa huomattiin, että kohderyhmä ei ollutkaan

vertailukelpoinen. Tuo kohderyhmä sisälsi huomattavan määrän sellaisia henkilöitä, joilla oli vain kotisähköposti. MAAWGin tutkimusta on täten pidetty lähdemateriaalina kysymysten laadinnassa.

Tutkimusongelmaan yksi on pyritty hankkimaan vastaus kysymyksillä 6 ”Oletko havainnut kotikoneellasi perinteisiä haittaohjelmia (matoja, viruksia, takaovia, troijalaisia”, kysymyksellä 8 ”Miten hyvin tunnet seuraavat käsitteet (phising/khalastelu, pharming, bottiverkko, rootit, palvelunestohyökkäys)”, kysymyksellä 10 ”Oletko tietoinen pahanlaatuisista viruksista, jotka voivat ottaa haltuusi tietokoneesi tietämättäsi ja siten käyttää konettasi roskapostin lähettämiseen?”, kysymyksellä 11 ”Miten arvioit arvoasteikolla 5-1, että voit saada pahanlaatuisen viruksen koneeseesi?”, kysymyksellä 12 ”Oletko saanut työsähköpostiisi roskapostia?”, kysymyksellä 13 ”Oletko saanut kotisähköpostiisi roskapostia?”, kysymyksellä 14 ”Mitä eri toimenpiteitä olet tehnyt kotikoneellesi saamallesi roskapostille?” sekä kysymyksellä 15 ”Jos olet klikannut linkkiä tai vastannut sähköpostiin, jota olet epäillyt roskapostiksi, mitä toimenpiteitä olet tehnyt?”.

Tutkimusongelmaan kaksi on pyritty hankkimaan vastaus kysymyksillä 16 ”Millä tavalla olet suojannut tietokoneesi”, kysymyksellä 17 ”Kuka hoitaa kotikoneesi virustorjunnan turvapäivitykset”, kysymyksellä 18 ”Käytätkö kotikoneessasi roskapostin automaattista suodatusta?”, kysymyksellä 19 ”Mikä on koneesi pääasiallinen käyttöjärjestelmä?”, kysymyksellä 20 ”Kuinka usein käyttämäsi käyttöjärjestelmän uudet tietoturvapäivitykset tarkistetaan?”, kysymyksellä 21 ”Mitä web-selainta/selaimia käytät kotona?” sekä kysymyksellä 22 ”Kuinka usein päivität selainta”.

4.3 Kohderyhmä

Tähän tutkimukseen on kohderyhmä valittu Nordeasta, koska Nordea on tämän tutkimuksen tekijän työpaikka. Ryhmän katsottiin soveltuvan hyvin vastaamaan kysymyksiin tavallisen kotikäyttäjän tietoturvasta. Pankkilaisia kohderyhmä edustaa hyvin, koska miehiä on vähemmän kuin naisia. Tietotekniikan ammattilaisia ryhmässä on vain muutama.

Kohderyhmäksi pyydettiin ja saatiin yksikkö, jossa on kolme erilaista osastoa, jotka jakautuvat tiimeihin. Kohderyhmässä oli tutkimusajankohtana töissä 89 henkilöä. Tutkimuksen tekijä esitteli tekemänsä kyselyn pääpiirteet johtoryhmän kokouksessa 2.9.2009 ja sai lopullisen hyväksynnän kohderyhmän käyttöön.

Nordeassa otettiin muutama kuukausi sitten otettu käyttöön uudet tietoturva-asetukset, jotka estävät pääsyn tietyille internet-sivuille kuten pelisivuille. Muuten Nordeassa ei ole rajoitettu pääsyä internetiin. Ohjeistus on kuitenkin se, että internetistä saa etsiä vain työhön liittyviä tietoja. Nordean sähköpostijärjestelmä on Microsoft Outlook. Jokaisella on Nordean antama sähköpostiosoite. Nordeassa on käytössä roskapostisuodatin, joka ilmoittaa roskapostikansioon siirretystä viestistä.

4.4 Toteutus

Webropol on internetin välityksellä toimiva kysely- ja tiedonkeruusovellus, jonka käyttöön tarvitaan käyttövaltuudet. (Webropol.) Tutkimuksessa käytetty kyselylomake toteutettiin anonyymina verkkokyselynä Webropolin avulla. Ajankäytön takia haastattelututkimusta ei voitu harkita. Webropol tuottaa suoraan valmiita raportteja. Niistä voi tehdä ristiin ajoja joko suoraan tai manuaalisesti.

Kyselylomakkeen taustatiedoissa eli ensimmäisessä osassa kysyttiin henkilön ikää sekä sukupuolta sekä sähköpostista. Jos henkilöllä ei ollut käytössä internet-yhteyttä kotona, vastaajan ei tarvinnut vastata mihinkään muihin kysymyksiin. Toisessa osassa kysymykset liittyivät haittaohjelmiin sekä roskapostiin. Kolmannessa osassa kysymykset liittyivät käyttöjärjestelmiin sekä tietoturva-asetuksiin. Kyselylomake oli suunniteltu vastaamaan viitekehyksen rakennetta.

Kysymyksistä osa oli valintakysymyksiä ja osa monivalintakysymyksiä. Muutamassa avoimessa kysymyksessä vastaajalle annettiin mahdollisuus itse kertoa. Tähän ei kuitenkaan ollut mitään pakkoa. Kyselylomake on esitetty liitteessä 1. Kysymysten tuloksia käsiteltiin tulosten esittelyssä prosenttilukuina ja kokonaislukuina. Luku 10,5 on pyöristetty ylöspäin lukuun 11. Tämä on voinut joissakin tuloksien esittelyssä johtaa siihen, että yhteenlaskettu prosenttimäärä on 101 tai 99 riippuen pyöristyksestä.

Webropol-verkkokysely lähetettiin sähköpostitse kohderyhmälle 8.9.2009 Kun muistutus lähti 17.9.2009, vastausprosentti oli 64. Kyselyn viimeinen vastauspäivä oli 18.9.2009, josta tutkimuksen tekijä poikkesi yhden vastaajan osalta yhden päivän. Lopullinen vastausprosentti oli 76 prosenttia eli 68 vastaajaa. Näistä miehiä oli 12 ja naisia 56. Alle 30-vuotiaita oli 19, 35 - 44 -vuotiaita 12, 45 - 55 -vuotiaita 20 ja yli 55-vuotiaita 17.

5 Tulokset

Tutkimuksessa tutkittiin ryhmää vertailuna tavallisten käyttäjien ja jonkin verran ammattilaisten välillä. Vertailua tehtiin myös ikäryhmävertailuna. Vastaajista ammattilaisia kertoi olevan 6 prosenttia vastaajista. Tavallisia käyttäjiä oli 54 prosenttia vastaajia ja loput 40 prosenttia oli jonkin verran ammattilaisia. Ammattilaisten osuus on jätetty käsittelemättä tutkimustulosten analysoinnissa. Vaikka heidän osuutensa oli pieni, heidän todettiin väärentävän tuloksia.

Koska miesten osuus oli niin paljon pienempi kuin naisilla, tutkimuksessa ei tehdä vertailua eri sukupuolien välillä.

5.1 Vertailua tavallisten käyttäjien ja jonkin verran ammattilaisten välillä

Tavallisista käyttäjistä 87 prosenttia oli naisia ja jossakin määrin ammattilaisista naisia oli 82 prosenttia.

TAULUKKO 1: Ikäryhmäjakautuma tavallisten ja jonkin verran ammattilaisten mukaan todellisina lukuina

	alle 35	35-44	45-55	yli 55
Ei	9	3	11	14
Jossakin määrin	8	9	8	2
Yhteensä	17	12	19	16

Ikäryhmäjakautumasta voidaan huomata, että jossakin määrin ammattilaisista alle 44-vuotiaita on 66 prosenttia ja yli 45-vuotiasta 68 prosenttia on tavallisia käyttäjiä.

Internet-yhteys oli kotona tavallisista käyttäjistä 92 prosentilla ja jossakin määrin ammattilaisilla kaikilla. Seuraavat kysymykset suunnattiin niille, joilla oli internet-yhteys kotona.

5.1.1 Oletko havainnut kotikoneellasi perinteisiä haittaohjelmia (matoja, viruksia, takaovia, troijalaisia)

TAULUKKO 2: Vastaukset kysymykseen perehtyneisyyden mukaan.

	en	kyllä	en osaa sanoa
Tavallinen käyttäjä	47 %	47 %	6 %
Jossakin määrin perehtynyt	52 %	44 %	8 %
Yhteensä	49 %	46 %	5 %

Prosenttiluvuista kyetään huomaamaan, että eroja ei juuri näyttäisi olevan.

Kysyttäessä kuvailua näistä 81 prosenttia antoi jonkin vastauksen. Vastaus liittyi 40 prosenttisesti troijalaiseen ja 23 prosenttisesti virukseen. Yksi vastaajista kuvaili laajasta ongelmasta, johon olivat sekoittuneet troijalaiset, virukset sekä tunnuksen kaapparit. Tarkemmat kuvaukset ovat kysymyslomakkeen kohdassa seitsemän liitteessä 1.

5.1.2 Miten hyvin tunnet seuraavat käsitteet

Kohderyhmältä kysyttiin käsitteiden (phising, pharming, bottiverkko, rootit ja palvelunesto-hyökkäys) tuntemista. Seuraavissa taulukoissa käsitellään erikseen jokaisen käsitteen tuntemista perehtyneisyyden mukaan.

TAULUKKO 3: Phising eli khalastelu -käsitteen tunteminen perehtyneisyyden mukaan

	hyvin	jonkin verran	en lainkaan
Tavallinen käyttäjä	44 %	32 %	24 %
Jossakin määrin perehtynyt	85 %	7 %	7 %
Yhteensä	62 %	21 %	16 %

TAULUKKO 4: Pharming-käsitteen tunteminen perehtyneisyyden mukaan

	hyvin	jonkin verran	en lainkaan
Tavallinen käyttäjä	0 %	12 %	88 %
Jossakin määrin perehtynyt	0 %	15 %	85 %
Yhteensä	0 %	13 %	87 %

TAULUKKO 5: Bottiverkko-käsitteen tunteminen perehtyneisyyden mukaan

	hyvin	jonkin verran	en lainkaan
Tavallinen käyttäjä	0 %	12 %	88 %
Jossakin määrin perehtynyt	0 %	15 %	85 %
Yhteensä	0 %	13 %	87 %

TAULUKKO 6: Rootit-käsitteen tunteminen perehtyneisyyden mukaan

	hyvin	jonkin verran	en lainkaan
Tavallinen käyttäjä	0 %	9 %	91 %
Jossakin määrin perehtynyt	4 %	37 %	59 %
Yhteensä	2 %	21 %	77 %

TAULUKKO 7: Palvelunestohyökkäys-käsitteen tunteminen perehtyneisyyden mukaan

	hyvin	jonkin verran	en lainkaan
Tavallinen käyttäjä	3 %	32 %	65 %
Jossakin määrin perehtynyt	29 %	52 %	19 %
Yhteensä	15 %	41 %	44 %

Kun tarkastellaan tuloksia perehtyneisyyden mukaan, huomataan, että phising eli khalastelu tunnetaan käsitteenä kaikkein parhaiten. Muista käsitteistä palvelunestohyökkäys on tutumpi kuin pharming, bottiverkko tai rootit.

5.1.3 Sinulta kysytään salasanaasi. Kenelle sen antaisit?

TAULUKKO 8: Salasanan antaminen perehtyneisyyden mukaan.

	IT-tukihenkilö	pomo	perheen jäsen	paras ystävä	joku muu	en kenellekään
Tavallinen käyttäjä	6 %	0 %	12 %	3 %	0 %	82 %
Jossakin määrin perehtynyt	7 %	0 %	4 %	0 %	4 %	85 %
Yhteensä	7 %	0 %	8 %	2 %	2 %	83 %

Salasanan antaminen jollekin muulle on aina turvallisuusriski vaikkakin kyseessä olisi perheen jäsen. Prosenttiluvuista voidaan päätellä, että suurin osa ei antaisi salasanaansa kenellekään.

5.1.4 Tietoisuus pahanlaatuisten virusten esiintymisestä

Seuraavissa taulukoissa käsitellään kohderyhmän tietoisuutta pahanlaatuisten virusten esiintymisestä perehtyneisyyden mukaan sekä arviota saada tuollainen virus omaan koneeseen.

TAULUKKO 9: Tietoisuus pahanlaatuisista viruksista, jotka voivat ottaa haltuunsa tietokoneesi tietämättäsi ja siten käyttää konettasi roskapostin lähettämiseen perehtyneisyyden mukaan.

	en	kyllä
Tavallinen käyttäjä	15 %	85 %
Jossakin määrin perehtynyt	7 %	93 %
Yhteensä	12 %	89 %

Tuloksista voidaan päätellä, että kummassakin ryhmässä tietoisuus on korkea.

TAULUKKO 10: Arvio arvoasteikolla 5-1 saada pahanlaatuinen virus koneelle perehtyneisyyden mukaan.

	5	4	3	2	1
Tavallinen käyttäjä	0 %	24 %	44 %	21 %	12 %
Jossakin määrin perehtynyt	7 %	15 %	33 %	30 %	15 %
Yhteensä	3 %	20 %	39 %	25 %	13 %

Kysymyksessä arvoasteikon numero viisi ilmaisi erittäin suurta todennäköisyyttä saada pahanlaatuinen virus koneelle. Arvoasteikon numero yksi ilmaisi epätodennäköisyyttä saada pahanlaatuinen virus koneelle. Tuloksesta on vaikea nähdä todellisia eroja. Prosenttilukuja tarkastellessa näyttää siltä, että vastaajien suhtautuminen on joko neutraali tai sitten todennäköisyyttä ei pidetä suurena.

5.1.5 Suhtautuminen roskapostiin

Seuraavissa taulukoissa käsitellään kohderyhmän suhtautumista roskapostiin perehtyneisyyden mukaan sekä eri toimenpiteitä, mitä he ovat tehneet saamalleen roskapostille. Ensin luodaan katsaus, onko kohderyhmä saanut roskapostia työsähköpostiinsa ja kotisähköpostiinsa.

TAULUKKO 11: Roskapostia työsähköpostiin saaneet perehtyneisyyden mukaan

	en	kyllä	en osaa sanoa
Tavallinen käyttäjä	47 %	53 %	0 %
Jossakin määrin perehtynyt	44 %	52 %	4 %
Yhteensä	46 %	53 %	2 %

TAULUKKO 12: Roskapostia kotisähköpostiin saaneet perehtyneisyyden mukaan

	en	kyllä	en osaa sanoa
Tavallinen käyttäjä	29 %	62 %	9 %
Jossakin määrin perehtynyt	22 %	78 %	0 %
Yhteensä	26 %	69 %	5 %

Ne, jotka kertoivat saaneensa kotisähköpostiinsa roskapostia, vastasivat myös jatkokysymyksiin liittyen kotikoneelle tulleeseen roskapostiin.

TAULUKKO 13: Tehdyt toimenpiteet kotikoneelle saamalle roskapostille perehtyneisyyden mukaan

	Olen painanut roskapostipainiketta tai siirtänyt ko.kansioon	Olen poistanut avaamatta	Olen avannut ja lukenut ennen poistamista	Olen raportoinut siitä palveluntuottajalle	Olen raportoinut siitä sähköpostioperaattorille	Olen vaihtanut sähköpostiosoitteeni	En ole tehnyt mitään
Tavallinen käyttäjä	43 %	91 %	5 %	0 %	5 %	0 %	5 %
Jossakin määrin perehtynyt	38 %	91 %	10 %	10 %	5 %	5 %	0 %
Yhteensä	41 %	91 %	7 %	5 %	5 %	2 %	2 %

Tähän kysymykseen vastaaja pystyi valitsemaan useamman kuin yhden vaihtoehdon. Tämä estää vertailun tekemisen seuraavassa kappaleessa esitettyihin lukuihin, jos siihen tuntee kiinnostusta. Suurin osa vastaajista kuitenkin näyttää poistaneen roskapostin avaamatta sitä.

TAULUKKO 14: Tehdyt toimenpiteet, jos on klikannut linkkiä tai vastannut sähköpostiin, jota epäillyt roskapostiksi, perehtyneisyyden mukaan.

	Kiinnostus tuotteeseen/ palveluun	Kiinnostus nähdä, mitä tapahtuu	Tein virheen	En ole klikannut linkkiä tai vastannut roskapostiin	En osaa sanoa
Tavallinen käyttäjä	5 %	0 %	19 %	76 %	0 %
Jossakin määrin perehtynyt	0 %	10 %	5 %	86 %	5 %
Yhteensä	2 %	5 %	12 %	81 %	2 %

Tuloksista suurin osa ei ollut klikannut linkkiä tai vastannut roskapostiin. Melkoisen moni tunnusti tehneensä virheen klikatessaan linkkiä.

5.1.6 Oman tietokoneen suojaus

Seuraavissa taulukoissa käydään läpi kohderyhmän oman tietokoneen suojaus perehtyneisyyden mukaan sekä kuka hoitaa heidän kotikoneensa virustorjunnan päivitykset.

TAULUKKO 15: Oman tietokoneen suojaustavat perehtyneisyyden mukaan.

	palomuuri	virusten torjunta ohjelma	haittaohjelmien poisto-ohjelma	jotenkin muuten	en käytä mitään suojausta
Tavallinen käyttäjä	68 %	91 %	38 %	3 %	0 %
Jossakin määrin perehtynyt	78 %	100 %	63 %	11 %	0 %
Yhteensä	72 %	95 %	49 %	7 %	0 %

Kysymyksessä annettiin vastaajalle mahdollisuus valita useampi vaihtoehto. Jossakin määrin perehtyneissä näyttää siltä, että kaikilla on jokin virusten torjuntaohjelma. Tarkempi tarkastelu kokonaismäärästä paljasti, että vain yhdellä vastaajista oli pelkästään haittaohjelmien poisto-ohjelma. Vastaajista kahdella oli ainoana vaihtoehtona palomuuri. Kymmenellä oli vain virustorjuntaohjelma. 24 vastaajaa oli suojannut kaikilla kolmella vaihtoehdolla. 17 oli suojannut palomuurin ja virustorjuntaohjelman yhdistelmällä. Vapaassa kommenttiosuudessa eräs vastaaja totesi käyttävänsä Firefoxia, koska oli huomannut sen tuovan vähemmän roskapostia.

Tähän kysymykseen liittyen kysyttiin minkä nimisiä suojausohjelmia vastaajilla on. Suurimmalla osalla oli F-Secure. Muita olivat Norton, Avasti, Antitrust, sekä Elisan tietoturvajärjestelmä.

TAULUKKO 16: Kotikoneen virustorjunnan turvapäivitysten hoitaminen perehtyneisyyden mukaan

	En käytä virustorjuntaohjelmaa	Päivitän itse tarvittaessa	Joku muu päivittää tarvittaessa	En päivitä virustorjuntaohjelmaa	Päivittyy automaattisesti
Tavallinen käyttäjä	3 %	12 %	27 %	0 %	59 %
Jossakin määrin perehtynyt	0 %	15 %	15 %	0 %	70 %
Yhteensä	2 %	13 %	21 %	0 %	64 %

Kummassakin ryhmässä näyttää siltä, että vastaajat ovat suurimmaksi osaksi ottaneet käyttöön turvapäivitysten automaattisen päivityksen. Niiltä, jotka kertoivat jonkun muun päivittävän tarvittaessa, ei kysytty, kuka tuo päivittäjä on.

5.1.7 Käytätkö kotikoneessasi roskapostin automaattista suodatusta?

TAULUKKO 17: Kotikoneen roskapostin automaattinen suodatus perehtyneisyyden mukaan.

	Olen määritellyt sähköpostiohjelmaani omat suodatussäännöt	Käytän suodatukseen erillistä apuohjelmaa	Operaattori siivoaa roskapostin jo postipalvelimella	En	En osaa sanoa
Tavallinen käyttäjä	21 %	3 %	27 %	18 %	32 %
Jossakin määrin perehtynyt	41 %	7 %	11 %	30 %	11 %
Yhteensä	30 %	5 %	20 %	23 %	23 %

Tuloksista huomattiin, että verrattuna tavallisiin käyttäjiin jossakin määrin perehtyneet olivat enemmän määritelleet sähköpostiohjelmaansa omia suodatussääntöjä. Prosenttilukuja tarkkaillen moni tavallisista käyttäjistä ei osannut vastata tähän kysymykseen. Monella ei myöskään ollut mitään automaattista suodatusta.

5.1.8 Kotikoneen pääasiallinen käyttöjärjestelmä ja sen tietoturvapäivitykset

Seuraavissa taulukoissa kerrotaan kohderyhmän käyttämä pääasiallinen käyttöjärjestelmä perehtyneisyyden mukaan sekä kuinka usein uudet tietoturvapäivitykset tarkistetaan.

TAULUKKO 18: Kotikoneen pääasiallinen käyttöjärjestelmä perehtyneisyyden mukaan

	Vista	Muu Windows	Macintosh OS	Linux	joku muu
Tavallinen käyttäjä	29 %	59 %	9 %	3 %	0 %
Jossakin määrin perehtynyt	30 %	67 %	0 %	0 %	4 %
Yhteensä	30 %	62 %	5 %	2 %	2 %

Tutkimuksessa kävi ilmi, että Linuxin osuus oli vähäinen. Kysymyksessä kysyttiin pääasiallista käyttöjärjestelmää. Mikä olisi ollut tulos, jos kaikkia käytettäviä käyttöjärjestelmiä olisi kysytty, ei kyetä toteamaan.

TAULUKKO 19: Kohderyhmän käyttämän käyttöjärjestelmän uusien tietoturvapäivitysten tarkistamistiheys perehtyneisyyden mukaan.

	automaattinen	viikoittain	kuukausittain	harvemmin	ei koskaan	en osaa sanoa
Tavallinen käyttäjä	71 %	6 %	6 %	0 %	0 %	18 %
Jossakin määrin perehtynyt	70 %	0 %	7 %	4 %	4 %	15 %
Yhteensä	71 %	3 %	7 %	2 %	2 %	16 %

Tuloksissa voidaan huomata prosenttiosuuksia tarkastellen, että käyttöjärjestelmän uudet tietoturvapäivitykset tarkistetaan suurimmaksi osaksi automaattisesti kummassakin ryhmässä.

5.1.9 Kohderyhmän kotona käyttämä web-selain ja sen päivitys

Seuraavista taulukoista selviää kohderyhmän kotona käyttämä web-selain sekä sen päivittämistiheys perehtyneisyyden mukaan.

TAULUKKO 20: Web-selainten käyttö kotona perehtyneisyyden mukaan.

	Internet Explorer	Mozilla Firefox	Google Chrome	Opera	Safari	Joku muu
Tavallinen käyttäjä	71 %	53 %	12 %	3 %	6 %	0 %
Jossakin määrin perehtynyt	78 %	63 %	7 %	7 %	0 %	0 %
Yhteensä	74 %	57 %	10 %	5 %	3 %	0 %

Kysymyksessä vastaajilla oli mahdollisuus valita useampia vaihtoehtoja.

TAULUKKO 21: Selaimen päivittämistiheys perehtyneisyyden mukaan.

	viikoittain	kuukausittain	harvemmin	en koskaan	en osaa sanoa
Tavallinen käyttäjä	18 %	15 %	24 %	3 %	41 %
Jossakin määrin perehtynyt	11 %	30 %	37 %	4 %	19 %
Yhteensä	15 %	21 %	30 %	3 %	31 %

Tuloksista voidaan huomata ”en osaa sanoa”-vastaajien suuri määrä. ”En koskaan”-vastaajia oli prosentuaalisesti vähän. Molemmissa ryhmissä kuitenkin yli kolmannes päivittää selaimen kuukausittain tai viikoittain.

5.2 Vertailua ikäryhmien välillä

Seuraavaksi on tehty vertailua eri ikäryhmien välillä. Mukana ei ole ammattilaisiksi itsensä luokitelleet. Tutkimuksessa oli myös tarkoitus tehdä ristikkäistutkimusta perehtyneisyyden ja ikäryhmien välillä. Kohderyhmä oli kuitenkin liian pieni tähän, jotta tuloksia olisi kyetty esitellä vaarantamatta vastaajien identiteettiä.

Ikäryhmässä alle 35-vuotiaat oli kaikilla vastaajilla sähköpostiosoite sekä töissä että kotona. Vastaajista ikäryhmässä yli 55-vuotiaat 13 prosentilla ei ollut internet-yhteyttä kotona. Vastaava

luku 45-55-vuotiaissa oli 5 prosenttia. Muissa ikäryhmissä kaikilla oli internet-yhteys. Niille, joilla ei ollut internet-yhteyttä, ei suunnattu seuraavia kysymyksiä.

5.2.1 Oletko havainnut kotikoneellasi perinteisiä haittaohjelmia (matoja, viruksia, takaovia, troijalaisia)

TAULUKKO 22: Vastaukset kysymykseen ikäryhmittäin mukaan.

	en	kyllä	en osaa sanoa
alle 35 v	29 %	59 %	12 %
35-44 v	58 %	42 %	0 %
45-55 v	44 %	56 %	0 %
yli 55 v	71 %	21 %	7 %

Prosenttilukuja tarkasteltaessa huomattiin, että yli 55-vuotiaista melkein kolme neljännestä ei ollut havainnut perinteisiä haittaohjelmia kotikoneella.

5.2.2 Miten hyvin tunnet seuraavat käsitteet

Kohderyhmältä kysyttiin käsitteiden (phising, pharming, bottiverkko, rootit ja palvelunesto-hyökkäys) tuntemista. Seuraavissa taulukoissa käsitellään erikseen jokaisen käsitteen tuntemista ikäryhmittäin mukaan.

TAULUKKO 23: Phising-käsitteen tunteminen ikäryhmittäin

	hyvin	jonkin verran	en lainkaan
alle 35 v	59 %	18 %	23 %
35-44 v	92 %	8 %	0 %
45-55 v	56 %	33 %	11 %
yli 55 v	50 %	21 %	29 %

TAULUKKO 24: Pharming-käsitteen tunteminen ikäryhmittäin

	hyvin	jonkin verran	en lainkaan
alle 35 v	0 %	18 %	82 %
35-44 v	0 %	25 %	75 %
45-55 v	0 %	7 %	94 %
yli 55 v	0 %	7 %	93 %

TAULUKKO 25: Bottiverkko-käsitteen tunteminen ikäryhmittäin

	hyvin	jonkin verran	en lainkaan
alle 35 v	0 %	36 %	65 %
35-44 v	0 %	8 %	92 %
45-55 v	0 %	0 %	100 %
yli 55 v	0 %	7 %	93 %

TAULUKKO 26: Rootit-käsitteen tunteminen ikäryhmittäin

	hyvin	jonkin verran	en lainkaan
alle 35 v	0 %	47 %	53 %
35-44 v	8 %	17 %	75 %
45-55 v	0 %	11 %	89 %
yli 55 v	0 %	7 %	93 %

TAULUKKO 27: Palvelunestohyökkäys-käsitteen tunteminen ikäryhmien mukaan

	hyvin	jonkin verran	en lainkaan
alle 35 v	12 %	65 %	24 %
35-44 v	17 %	42 %	42 %
45-55 v	17 %	33 %	50 %
yli 55 v	14 %	13 %	74 %

Kun tarkastellaan tuloksia ikäryhmien mukaan, huomataan, että phising eli khalastelu tunnetaan käsitteenä kaikkein parhaiten. Muista käsitteistä palvelunestohyökkäys on tutumpi kuin pharming, bottiverkko tai rootit. Alle 35-vuotiaiden ryhmässä kuitenkin huomataan, että bottiverkko ja rootit ovat käsitteinä tutumpia kuin muille.

5.2.3 Sinulta kysytään salasanaasi. Kenelle sen antaisit?

TAULUKKO 28: Salasanan antaminen ikäryhmittäin.

	IT-tukihenkilö	pomo	perheen jäsen	paras ystävä	joku muu	en kenelle kään
alle 35 v	6 %	0 %	6 %	6 %	6 %	82 %
35-44 v	17 %	0 %	8 %	0 %	0 %	75 %
45-54 v	0 %	0 %	6 %	0 %	0 %	94 %
yli 55 v	7 %	0 %	14 %	0 %	0 %	79 %

Prosenttiosuuksia katsoen huomataan, että erot ovat pienet. Joku on kuitenkin valmis antamaan salasanansa jollekin.

5.2.4 Tietoisuus pahanlaatuisten virusten esiintymisestä

Seuraavissa taulukoissa käsitellään kohderyhmän tietoisuutta pahanlaatuisten virusten esiintymisestä ikäryhmittäin sekä arviota saada tuollainen virus omaan koneeseen.

TAULUKKO 29: Tietoisuus pahanlaatuisista viruksista, jotka voivat ottaa haltuunsa tietokoneesi tietämättäsi ja siten käyttää konettasi roskapostin lähettämiseen perehtyneisyyden mukaan.

	en	kyllä
alle 35 v	6 %	94 %
35-44 v	17 %	83 %
45-54 v	17 %	83 %
yli 55 v	7 %	93 %

Prosenttiosuuksia katsoen huomataan, että ikäryhmissä 35-54 -vuotiaat tietämys näyttäisi olevan heikompi.

TAULUKKO 30: Arvio todennäköisyydestä saada pahanlaatuinen virus koneelle ikäryhmittäin.

	5	4	3	2	1
alle 35 v	0 %	18 %	47 %	12 %	24 %
35-44 v	0 %	17 %	42 %	33 %	8 %
45-54 v	6 %	33 %	28 %	22 %	11 %
yli 55 v	7 %	7 %	43 %	36 %	7 %

Kysymyksessä arvoasteikon numero viisi ilmaisi erittäin suurta todennäköisyyttä saada pahanlaatuinen virus koneelle. Arvoasteikon numero yksi ilmaisi epätodennäköisyyttä saada pahanlaatuinen virus koneelle. Prosenttiosuuksia tarkastellen kaikkien vastaukset ovat neutraaleja. 45-54 -vuotiaiden ryhmässä näyttäisi siltä, että arvio todennäköisyydestä on suurempaa.

5.2.5 Suhtautuminen roskapostiin

Seuraavissa taulukoissa käsitellään kohderyhmän suhtautumista roskapostiin ikäryhmittäin sekä eri toimenpiteitä, mitä he ovat tehneet saamalleen roskapostille. Ensin luodaan katsaus, onko kohderyhmä saanut roskapostia työsähköpostiinsa ja kotisähköpostiinsa.

TAULUKKO 31: Roskapostia työsähköpostiin saaneet ikäryhmittäin

	en	kyllä	en osaa sanoa
alle 35 v	59 %	35 %	6 %
35-44 v	17 %	83 %	0 %
45-54 v	44 %	56 %	0 %
yli 55 v	57 %	43 %	0 %

TAULUKKO 32: Roskapostia kotisähköpostiin saaneet ikäryhmittäin

	en	kyllä	en osaa sanoa
alle 35 v	6 %	94 %	0 %
35-44 v	25 %	67 %	8 %
45-54 v	39 %	50 %	11 %
yli 55 v	36 %	64 %	0 %

Ne, jotka kertoivat saaneensa kotisähköpostiinsa roskapostia, vastasivat myös jatkokysymyksiin liittyen kotikoneelle tulleeseen roskapostiin.

TAULUKKO 33: Tehdyt toimenpiteet kotikoneelle saamalle roskapostille ikärymittäin.

	Olen painanut roskapostipainiketta tai siirtänyt ko.kansioon	Olen poistanut avaamatta	Olen avannut ja lukenut ennen poistamista	Olen raportoinut siitä palveluntuottajalle	Olen raportoinut siitä sähköpostioperaattorille	Olen vaihtanut sähköpostiosoitteeni	En ole tehnyt mitään
alle 35 v	63 %	81 %	13 %	6 %	6 %	6 %	6 %
35-44 v	50 %	88 %	0 %	13 %	13 %	0 %	0 %
45-54 v	11 %	100 %	11 %	0 %	0 %	0 %	0 %
yli 55 v	22 %	100 %	0 %	0 %	0 %	0 %	0 %

Tähän kysymykseen vastaaja pystyi valitsemaan useamman kuin yhden vaihtoehdon. Tämä estää vertailun tekemisen seuraavassa kappaleessa esitettyihin lukuihin, jos siihen tuntee kiinnostusta. Tuloksista voidaan huomata, että suurin osa on poistanut roskapostin avaamatta sen.

TAULUKKO 34: Tehdyt toimenpiteet, jos on klikannut linkkiä tai vastannut sähköpostiin, jota epäillyt roskapostiksi, ikäryhmittäin..

	Kiinnostus tuotteeseen/ palveluun	Kiinnostus nähdä, mitä tapahtuu	Tein virheen	En ole klikannut linkkiä tai vastannut roskapostiin	En osaa sanoa
alle 35 v	6 %	13 %	19 %	69 %	0 %
35-44 v	0 %	0 %	0 %	88 %	13 %
45-54 v	0 %	0 %	22 %	78 %	0 %
yli 55 v	0 %	0 %	0 %	100 %	0 %

Prosenttiosuuksia tarkkaillen voidaan huomata, että suurin osa ei ollut klikannut linkkiä tai vastannut roskapostiin.

5.2.6 Oman tietokoneen suojaus

Seuraavissa taulukoissa käydään läpi kohderyhmän oman tietokoneen suojaus ikäryhmittäin sekä kuka hoitaa heidän kotikoneensa virustorjunnan päivitykset.

TAULUKKO 35: Oman tietokoneen suojaustavat ikäryhmittäin.

	palomuuri	virusten torjunta ohjelma	haittaohjelmien poisto-ohjelma	jotenkin muuten	en käytä mitään suojausta
alle 35 v	94 %	88 %	65 %	0 %	0 %
35-44 v	58 %	100 %	42 %	8 %	0 %
45-54 v	67 %	100 %	61 %	6 %	0 %
yli 55 v	64 %	93 %	21 %	14 %	0 %

Tuloksista voidaan huomata, että kaikilla 35-54 -vuotiailla on kotitietokoneen suojauksena jokin virusten torjuntaohjelma. Ilman suojausta ei ole kenenkään kone. Alle 35-vuotiaissa kiinnittyy huomio korkeaan palomuurin osuuteen verrattuna muihin ikäryhmiin.

TAULUKKO 36: Kotikoneen virustorjunnan turvapäivitysten hoitaminen ikäryhmittäin.

	En käytä virustorjunta ohjelmaa	Päivitän itse tarvittaessa	Joku muu päivittää tarvittaessa	En päivitä virustorjuntaohjelmaa	Päivittyy automaattisesti
alle 35 v	6 %	18 %	12 %	0 %	65 %
35-44 v	0 %	17 %	8 %	0 %	75 %
45-54 v	0 %	0 %	28 %	0 %	72 %
yli 55 v	0 %	21 %	36 %	0 %	43 %

Jos verrataan edelliseen taulukkoon, virustorjuntaohjelman käytön luvut eivät täsmää alle 35-vuotiaiden ja yli 55-vuotiaiden ryhmissä. Nämä eivät siis näytä olevan vertailukelpoiset. Niiltä, jotka kertoivat jonkun muun päivittävän tarvittaessa, ei kysytty, kuka tuo päivittäjä on.

5.2.7 Käytätkö kotikoneessasi roskapostin automaattista suodatusta?

TAULUKKO 37: Kotikoneen roskapostin automaattinen suodatus ikäryhmittäin.

	Olen määritellyt sähköpostiohjelmaani omat suodatussäännöt	Käytän suodatukseen erillistä apuohjelmaa	Operaattori siivoaa roskapostin jo postipalvelimella	En	En osaa sanoa
alle 35 v	24 %	6 %	30 %	24 %	18 %
35-44 v	33 %	8 %	0 %	42 %	17 %
45-54 v	28 %	6 %	28 %	22 %	17 %
yli 55 v	36 %	0 %	14 %	7 %	43 %

Prosenttiosuuksia tarkastellen voidaan huomata, että monella ei ole minkäänlaista roskapostin automaattista suodatusta. Etenkin yli 55-vuotiaista moni ei myöskään osannut vastata tähän kysymykseen.

5.2.8 Kotikoneen pääasiallinen käyttöjärjestelmä ja sen tietoturvapäivitykset

Seuraavissa taulukoissa kerrotaan kohderyhmän käyttämä pääasiallinen käyttöjärjestelmä perehtyneisyyden mukaan sekä kuinka usein uudet tietoturvapäivitykset tarkistetaan.

TAULUKKO 38: Kotikoneen pääasiallinen käyttöjärjestelmä ikäryhmittäin.

	Vista	Muu Windows	Macintosh OS	Linux	joku muu
alle 35 v	35 %	47 %	12 %	6 %	0 %
35-44 v	17 %	83 %	0 %	0 %	0 %
45-54 v	28 %	67 %	0 %	0 %	6 %
yli 55 v	36 %	57 %	7 %	0 %	0 %

Tuloksista voidaan huomioida, että muiden kuin Microsoftin käyttöjärjestelmien käyttö on harvinaisempaa. Kysymyksessä kysyttiin pääasiallista käyttöjärjestelmää. Mikä olisi ollut tulos, jos kaikkia käytettäviä käyttöjärjestelmiä olisi kysytty, ei kyetä toteamaan. Se ei ole yllätys, että muiden kuin Microsoftin käyttöjärjestelmien käyttö näyttää olevan yleisempää alle 35-vuotiaiden ryhmässä.

TAULUKKO 39: Kohderyhmän käyttämän käyttöjärjestelmän uusien tietoturvapäivitysten tarkistamistiheys ikäryhmittäin.

	automaattinen	viikoittain	kuukausittain	harvemmin	ei koskaan	en osaa sanoa
alle 35 v	53 %	6 %	12 %	0 %	6 %	24 %
35-44 v	67 %	0 %	0 %	8 %	0 %	25 %
45-54 v	89 %	0 %	6 %	0 %	0 %	6 %
yli 55 v	71 %	7 %	7 %	0 %	0 %	14 %

Tuloksia voidaan huomioida, että alle 45-vuotiaista moni ei osannut vastata tähän kysymykseen.

5.2.9 Kohderyhmän kotona käyttämä web-selain ja sen päivitys

Seuraavista taulukoista selviää kohderyhmän kotona käyttämä web-selain sekä sen päivittämistiheys ikäryhmittäin.

TAULUKKO 40: Web-selainten käyttö kotona ikäryhmittäin.

	Internet Explorer	Mozilla Firefox	Google Chrome	Opera	Safari	Joku muu
alle 35 v	47 %	82 %	0 %	6 %	12 %	0 %
35-44 v	100 %	42 %	25 %	0 %	0 %	0 %
45-54 v	78 %	50 %	6 %	6 %	0 %	0 %
yli 55 v	79 %	50 %	14 %	7 %	0 %	0 %

Tuloksista voidaan huomioida se, että alle 35-vuotiaiden ikäryhmässä Firefoxin käyttö oli suurempaa kuin Internet Explorerin. Vastaajalla oli mahdollisuus valita useampi vaihtoehto.

TAULUKKO 41: Selaimen päivittäminen ikäryhmittäin.

	viikoittain	kuukausittain	harvemmin	en koskaan	en osaa sanoa
alle 35 v	12 %	41 %	18 %	0 %	29 %
35-44 v	0 %	25 %	42 %	8 %	25 %
45-54 v	17 %	17 %	33 %	6 %	28 %
yli 55 v	29 %	0 %	29 %	0 %	43 %

Tuloksista voidaan huomata ”en osaa sanoa”-vastaajien suuri määrä.

6 Johtopäätökset ja suositukset

Tutkimuksen tavoitteena oli kytkeä tutkimus esitettyyn viitekehykseen verkkorikollisuudesta ja siihen liittyvästä torjunnasta. Kohderyhmänä oli eräs Nordea Pankki Suomen yksikkö. Tutkimus ei ollut toimeksianto. Tutkimustulosten perusteella kohderyhmä jaettiin kolmeen ryhmään tietotekniikka/tietoliikenne-tietämyksen mukaan. Ammattilaisiksi itsensä luokitelleet jätettiin tulosten analysoinnissa käsittelemättä. Analysoinnissa verrattiin tavallisten käyttäjien ja jonkin verran ammattilaisten tietämystä sekä tehtiin vertailua eri ikäryhmien välillä. Rinnakkaisvertailua tietämyksen ja ikäryhmien kesken ei kyetty tekemään pienen kohderyhmän takia. Vastaajien yksilönsuojaa haluttiin suojella. Tutkimustuloksia on seuraavaksi käsitelty tutkimusongelmien kautta.

6.1 Johtopäätökset

Työlle oli asetettu kaksi tutkimusongelmaa. Tässä kappaleessa on käsitelty tutkimusongelman ”Tunteeko kohderyhmä tämän ajan käsitteet, jotka liittyvät omaan kotitietokoneeseen kohdistuviin uhkiin sekä mikä on heidän suhtautumisensa tähän liittyvään roskapostiin?” tuloksia. Seuraavassa kappaleessa on käsitelty tutkimusongelman ”Osaako kohderyhmä huolehtia kotikoneensa tietoturvasta?” tuloksia. Ensimmäisen tutkimusongelmaan liittyen tutkimustuloksista voidaan päätellä, että vaikka kohderyhmä onkin melko valveutunutta, sieltä löytyy muutama yllättävä tieto. Tutkimuksen tekijälle oli yllätys, että Nordeassakin paljon esillä ollut phising- eli khalastelu ei ollut kaikille tuttu. Käsitteiden tuntemisessa kuitenkin kyettiin huomaamaan, että alle 35-vuotiaiden ryhmässä bottiverkko ja rootit olivat tutumpia käsitteitä kuin muille ikäryhmille. Tietenkin tässä on pakko todeta, että tärkeämpää kuin tuntea käsite, on tietää, miten välttää se. Vastaajien suhtautuminen saada pahanlaatuinen virus koneelle oli joko neutraali tai sitten todennäköisyyttä ei pidetty suurena. Salasanan oli joku valmis antamaan jollekin. Tämän voi katsoa olevan huolestuttavaa, vaikka kyseessä olisikin perheen jäsen tai IT-tukihenkilö. Roskapostin suurin osa vastaajista näytti poistavan avaamatta sitä. Niistä, jotka olivat klikanneet roskapostilinkkiä tai vastanneet roskapostiin, melkoisen moni tunnusti tehneensä virheen klikatessaan linkkiä. Ikäryhmävertailu ei paljastanut mitään muuta erikoista huomioitavaa tulosten analysoinnissa.

Työn toinen tutkimusongelma oli, osaako kohderyhmä huolehtia kotikoneensa tietoturvasta. Tuloksista kävi ilmi, että kaikilla ei ollut palomuuria käytössä. Alle 35-vuotiaiden ikäryhmässä kuitenkin kyettiin huomaamaan, että palomuurin korkea osuus korostui verrattuna muihin

ikäryhmiin. On huomioitavaa, että jossakin määrin perehtyneiden ryhmässä kaikilla ja tavallisten käyttäjien ryhmässä lähes kaikilla oli virustentorjuntaohjelma. Virustentorjuntaohjelma oli 35-54 -vuotiaiden ikäryhmissä kaikilla ja muillakin oli korkeat osuudet. Kaikki vastaajat olivat suurimmaksi osaksi ottaneet käyttöön automaattiset päivitykset käyttöön liittyen virustorjunnan turvapäivityksiin. Yllättävän monet eivät käyttäneet minkäänlaista roskapostin automaattista suodatusta. Yli 55-vuotiaiden ikäryhmässä hieman alle puolet ei osannut vastata tähän kysymykseen. Päivitykset olivat melko hyvin hallinnassa, vaikkakaan tästä ei selainten osalta saanut hyvää kokonaiskuvaa, koska niin moni ei osannut vastata tähän kysymykseen. Kuitenkin voidaan todeta, että yli 55-vuotiaiden ryhmässä liki kolmannes päivitti selaimen viikoittain.

6.2 Suositukset

Viimeisin Nordean verkkopankkiasiakkaita koskettanut uutinen näkyi myös osalle tämän tutkimuksen kohderyhmän henkilöille lisääntyneenä työnä. Pitäisin itse tärkeänä, että haittaohjelmiin ja torjuntaan liittyvä käsitteistö käydään läpi joko tämän esityksen pohjalta tai sitten organisaation riskienhallintaosaston virallisena esityksenä. Täten kasvatetaan sitä tietoisuutta, jota arvioitiin myös tutkitussa kysymyksessä. Työn tekijällä ei ole tarkoitus herättää turhia pelkotilanteita varsinkaan sen takia, että tutkimuksesta ei paljastunut suuria ongelmia. Tämän työn lukeminen on hyvä alku ja varmasti auttaa ymmärtämään paremmin, mitä ympäröivässä verkkomaailmassa tapahtuu. Tätä selkeyttämään on viitekehyksessä esitetty erilaisia esimerkkejä tapauksista. Liitteessä 2 on kooste tästä työstä hyödynnettäväksi mahdollisessa esityksessä.

Paitsi, että jokainen on vastuussa oman tietokoneensa tietoturvasta, on myös tärkeää, että jokainen meistä huolehtii, että roskapostiliikenne saadaan loppumaan. Uteliaisuus on paikallaan tietyssä tilanteessa. Jos riskinä on joutuminen lisääntyvässä määrin roskapostittajien jakelulistalle, suosittelisin roskapostin pikaista poistamista avaamatta sitä. Ja pitää muistaa, ettei ole kovinkaan tehokasta, jos suurin osa saapuneesta sähköpostista on jotain muuta kuin sitä toivottua.

7 Yhteenveto

Tässä työssä on käyty läpi teoriaa, joka liittyy verkkorikollisuuteen sisältäen sekä perinteiset että uudemmat haittaohjelmat sekä hyökkäysmallit. Työssä on myös esitetty katsaus edellä mainittuihin liittyvään torjuntaan. Historiallisesti kehitys on ollut huimaa. Verkkorikollisuus on muuttunut rikollisuudeksi, jossa ei enää haluta aiheuttaa vain haittaa, vaan halutaan osoittaa tietyn vallan käytön kautta voimansa mahdollisen taloudellisen hyödyn saavuttamiseksi. Tietoturva on yrityksissä tietoturva-asiantuntijoiden käsissä. Kotona tietoturva on enemmän tai vähemmän asiantuntevien henkilöiden käsissä. Jokaisen on hyvä ymmärtää syyt, miksi oma tietokone kannattaa suojata. On myös hyvä huomioida, että torjunta ei enää ole vain pelkkää tekniikkaa. Se sisältää myös hyväuskoisten yksityisten ihmisten harhauttamisen riippumatta heidän tietotaidostaan.

Pilvi-it on uudistuksena mielenkiintoinen. Eri asia on sitten, milloin voimme lukea, että haittaohjelman kirjoittaja on päässyt murtautumaan sen sisältämään virustietokantaan ja muuttanut sitä aiheuttaen suuren katastrofin. Kuulostaa vähän siltä, että ”munien laittamisesta yhteen koriin” ei hyvää seuraa. Tietoturvayhtiöt ovat kuitenkin yhdessä linjassa tämän näkemyksen takana, joten toivottavasti mitään ei tapahdu. Pilvi-it on tätä aikaa. Se pitää sisällään paljon muuta kuin tietoturvaan liittyvää. Näyttää siltä, että olemme kaikki kohta ”pilvessä”.

Lähteet

Boström, M. 2003. Kotimikron tietoturva. Gummerus Kirjapaino Oy. Jyväskylä.

Cert-Fi. Tietoturvakatsaus 2/2009. Luettavissa: http://www.cert.fi/katsaukset/2009/tietoturvakatsaus_22009.html. Luettu: 9.8.2009.

ESET Threat Blog. 2009. Luettavissa: http://www.eset.com/threat-center/blog/2009/11/16/once-upon-a-cybercrime Luettu 14.2.2010.

Flyktman, R. 2006. PC tehokäytössä. Gummerus Kirjapaino Oy. Jyväskylä.

Iltasanomat. Twitter ja Facebook joutuivat nettihyökkäyksen kohteeksi. Luettavissa: http://www.iltasanomat.fi/uutiset/ulkomaat/uutinen.asp?id=1717516. Luettu: 7.8.2009.

IT-viikko 2009a. Tulosta-nappi teki kepposet. Luettavissa: http://www.itviikko.fi/tietoturva/2009/07/14/tulosta-nappi-teki-tepposet/200916285/7. Luettu: 31.7.2009.

IT-viikko 2009b. 150 miljardia roskapostiviestiä päivässä. Luettavissa: http://www.itviikko.fi/tietoturva/2009/07/30/roskapostilla-menee-nyt-lujempaa-kuin-koskaan/200917349/7. Luettu: 30.7.2009

Järvinen, P. 2006. Paranna tietoturvaasi. WF Bookwell. Porvoo.

Järvinen, P. Uudet aseet roskapostin torjuntaan. Luettavissa: http://www.tietokone.fi/lukusali/artikkelit/2008tk09/roskaposti.htm. Luettu: 22.7.2009.

Helsingin Sanomat. Nordea-huijausviestejä virtaa taas sähköposteihin. 5.8.2009.

Hämäläinen, P. Roskapostin ekosysteemi. Luettavissa: http://www.tietokone.fi/lukusali/artikkelit/2008tk04/kytkentoja.htm. Luettu: 22.7.2009.

Keizer, G. Windows market share slide resumes. Computerworld. 3.1.2010. Luettavissa: http://www.computerworld.com/s/article/9142978/Windows_market_share_slide_resumes?taxonomyId=89&pageNumber=1 Luettu 14.2.2010.

Kotilainen, S. Tietoturva nousee pilviin. Luettavissa: http://www.tietokone.fi/lukusali/artikkelit/2009tk01/ttpaketit.htm. Luettu: 17.7.2009

Lehto, T. 2008. Verkkorikollinen kaappaa sivusi. Luettavissa: http://www.tietokone.fi/lukusali/artikkelit/2008tk06/kaappaus.htm. Luettu: 22.7.2009.

MAAWG. A Look at Consumers' Awareness of Email Security and Practices or "Of Course, I Never Reply to Spam - Except Sometimes". Luettavissa: http://www.maawg.org/about/publishedDocuments/2009_MAAWG-Consumer_Survey.pdf. Luettu: 16.7.2009.

McAfee Threats Report: Second Quarter 2009. Luettavissa: http://www.mcafee.com/us/local_content/reports/6623rpt_avert_threat_0709.pdf Luettu 9.8.2009.

Microsoft. 2010. Palomuuri: usein kysyttyjä kysymyksiä. Luettavissa: http://windows.microsoft.com/fi-FI/windows-vista/Firewall-frequently-asked-questions Luettu 14.2.2010.

Nieminen, M. Nordean asiakkaita joutui haittaohjelman uhriksi. Helsingin Sanomat. 17.1.2010.

Pullinen, J. Haittaohjelman saastuttama kone on monesti menetetty. Helsingin Sanomat 25.1.2010.

Stallings, W. 2008. Computer Security: Principles and Practice. Pearson Education, Inc. United States of America.

Suoranta, L. 2008. Verkkorikos kannattaa. Luettavissa: http://www.tietokone.fi/lukusali/artikkelit/2008tk14/verkkorikos.htm. Luettu: 17.7.2009.

Symantec 2009a. Online Fraud: Pharming. Luettavissa: http://www.symantec.com/norton/cybercrime/pharming.jsp. Luettu: 4.8.2009.

Symantec 2009b. Pharming on phishing-huijausta kehittyneempi ja vaikeammin havaittava hyökkäysmuoto. Luettavissa: http://www.symantec.com/fi/fi/norton/library/familyresource/article.jsp?aid=article1_08_06. Luettu: 7.8.2009.

Symantec 2009c. State of Phishing, A Monthly Report. Report #21. Symantec. July 2009 Luettavissa: http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_phishing_report_07-2009.en-us.pdf. Luettu: 4.8.2009.

Symantec 2009d. State of Spam. A Monthly Report. Report # 31. Symantec. July 2009. Luettavissa: http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_07-2009.en-us.pdf. Luettu: 4.8.2009.

Taloussanomat 2009a. Krakkerit sulkivat Twitterin. Luettavissa: http://www.taloussanomat.fi/informaatioteknologia/2009/08/06/krakkerit-sulkivat-twitterin/200917756/12. Luettu: 7.8.2009.

Taloussanomat 2009b. Jenkit paljastavat: Vastaamme tahallamme roskaposteihin. Luettavissa: http://www.taloussanomat.fi/tyo-ja-koulutus/2009/07/16/jenkit-paljastavat-vastaamme-tahallamme-roskaposteihin/200916436/139. Luettu: 16.7.2009.

Tietojen arvioiminen. 3.8.2007. http://www2.uiah.fi/projects/metodi/088.htm#khii. Luettu: 25.1.2010.

Tietokone. Turvallisin järjestelmä? Luettavissa: http://www.tietokone.fi/lukusali/artikkelit/2008tk04/kolu_wiio.htm. Luettu: 22.7.2009.

Webropol. Luettavissa: http://w3.webropol.com/finland. Luettu: 22.8.2010.

Kyselylomake

Hei!

Olen viimeisen kolmen vuoden ajan opiskellut ammattikorkeakoulussa tietojenkäsittelyä. Nyt on tullut aika tehdä opinnäytetyö. Tässä tulee sinun roolisi. Lähetän sinulle nyt kyselylomakkeen, jonka toivon sinun täyttävän. Tähti kysymyksen perässä kertoo, onko se pakollinen.

Eli autathan minua valmistumaan koulusta ja vastaat kyselyyn. Käsittelen tulokset anonyymisti.

tv.
Jaana

1) Sukupuoli
- o nainen
- o mies

2) Ikä
- o alle 35-vuotias
- o 35- 44 vuotta
- o 45 - 55 vuotta
- o yli 55-vuotias

3) Oletko ammattisi, opintojesi tai harrastustesi kautta tietotekniikan tai tietoliikenteen "ammattilainen"?
- o ei, olen tavallinen tietokoneen käyttäjä
- o kyllä, ainakin jossakin määrin
- o kyllä olen
- o joku, muu mikä? _____

4) Onko sinulla sähköpostiosoite töissä tai kotona tai molemmissa?
- o vain töissä
- o sekä töissä että kotona
- o vain kotona
- o en osaa sanoa

5) Onko sinulla internet-yhteys kotona?
- o kyllä
- o ei

6) Oletko havainnut kotikoneellasi perinteisiä haittaohjelmia (matoja, viruksia, takaovia, troijalaisia)

- o en
- o kyllä en osaa sanoa

7) Voitko kuvailla millaisia_____

(vastauksia kuvauksiin:

- Käytän virustorjuntaohjelman lisäksi haittaohjelmien poisto-ohjelmaa (AWC) joka tuntuu löytävän aina välillä jotain poistettavaa koneelta. En ole kiinnittänyt huomiota ohjelmien nimiin/laatuun.
- Monta vuotta sitten koneelleni tarttui mato CD:n autorun.exe:n kautta. Lisäksi erilaisia trackereita esiintyy ajoittain.
- en tiedä
- Muistuu mieleen vain Troijan hevonen... ja jotain herjoja esim. HO Object COM device Objects..."tietokone on suljettava..."
- viruksia)

8) Miten hyvin tunnet seuraavat käsitteet

	hyvin	jonkin verran	en lainkaan
phising, khalastelu			
pharming			
bottiverkko			
rootit			
palvelunestohyökkäys			

9) Sinulta kysytään salasanaasi. Kenelle sen antaisit?

- o IT-tukihenkilölle
- o pomolleni
- o perheeni jäsenelle
- o parhaalle ystävälleni
- o jollekin muulle, kenelle?
- o en kenellekään

10) Oletko tietoinen pahanlaatuisista viruksista, jotka voivat ottaa haltuusi tietokoneesi tietämättäsi ja siten käyttää konettasi roskapostin lähettämiseen?

- o en
- o kyllä

11) Miten arvioit arvoasteikolla 5-1, että voit saada pahanlaatuisen viruksen koneeseesi?

	5	4	3	2	1	
erittäin todennäköis-tä						epätodennäköistä

12) Oletko saanut työsähköpostiisi roskapostia?

- o en
- o kyllä en osaa sanoa

13) Oletko saanut kotisähköpostiisi roskapostia?

- o en
- o kyllä
- o en osaa

14) Mitä eri toimenpiteitä olet tehnyt kotikoneellesi saamallesi roskapostille?

- o olen painanut joko roskapostipainiketta tai siirtänyt roskapostikansioon
- o olen poistanut sen avaamatta
- o olen avannut ja lukenut sen ennen poistamista
- o olen lähettänyt sen internet-palveluntuottjalle
- o olen raportoinut siitä sähköpostioperaattorille
- o olen vaihtanut sähköpostiosoitteeni
- o olen käyttänyt en tilaa -linkkiä
- o jotain muuta
- o en ole tehnyt mitään

15) Jos olet joskus klikannut linkkiä tai vastannut sähköpostiin, jota olet epäillyt roskapostiksi, mitä toimenpiteitä olet tehnyt?

- o kiinnostus tuotteeseen/palveluun
- o kiinnostus nähdä mitä tapahtuu
- o tein virheen
- o lähetin viestin poistaa minut jakelusta tai valittaakseni
- o en ole klikannut linkkiä tai vastannut roskapostiin
- o en osaa sanoa
- o joku muu, mikä _____

16) Miten eri tavoin olet suojannut tietokoneesi?

- o palomuuri
- o virustentorjuntaohjelma
- o haittaohjelmien poisto-ohjelma
- o jotenkin muuten, miten? _____
- o en käytä mitään suojausta

17) Minkä nimisiä ohjelmia sinulla on (esim. F-Secure)

vastauksia tähän kysymykseen:

- AVG, AWC
- F-Secure
- BitDefender Quick Scan, CCleaner, LavaSoft AdAware, Vistan omat Defender + Firewall ovat myös käytössä.
- Antitrust
- Norman

18) Kuka hoitaa kotikoneesi virustorjunnan turvapäivitykset?

- o en käytä virustentorjuntaohjelmaa
- o päivitän itse virustentorjuntaohjelmaa tarvittaessa
- o joku muu päivittää virustentorjuntaohjelman tarvittaessa
- o en päivitä virustentorjuntaohjelmaa
- o virustentorjuntaohjelma päivittyy automaattisesti
- o en osaa sanoa

19) Käytätkö kotikoneessasi roskapostin automaattista suodatusta?

- o kyllä, olen määritellyt sähköpostiohjelmaani omat suodatussäännöt
- o kyllä, käytän roskapostin suodatukseen erillistä apuohjelmaa
- o operaattori siivoaa roskapostin jo postipalvelimella
- o en
- o en osaa sanoa

20) Mikä on koneesi pääasiallinen käyttöjärjestelmä?

- o Microsoft Windows Vista
- o Microsoft Windows, muu kuin Vista
- o Macintosh OS
- o Linux
- o joku muu, mitä? _____
- o en osaa sanoa

21) Kuinka usein käyttämäsi käyttöjärjestelmän uudet tietoturvapäivitykset tarkistetaan?

- o käyttöjärjestelmä tarkistaa automaattisesti
- o viikoittain
- o kuukausittain
- o harvemmin
- o ei koskaan
- o en osaa sanoa

22) Mitä web-selainta/selaimia käytät kotona?

- o Internet Explorer
- o Mozilla Firefox
- o Google Chrome
- o Opera
- o Safari
- o joku muu, mikä? _____
- o en osaa sanoa

23) Kuinka usein päivität selainta?

- o viikottain
- o kuukausittain
- o harvemmin
- o en koskaan
- o en osaa sanoa

Kiitos vastaamisesta! Kyselyssä on voinut edetä vain, jos vastaajalla on internet käytössä kotona.?

Jos sinulla on jotain kommentoitavaa kyselystä, voit sen tehdä alla olevaan tilaan.

- Tsemppiä lopputyön kanssa!
- Tsemppiä opinnäytetyön tekoon!
- Microsoft päivittää selaimen tietyin välein automaattisesti.
- Menestystä opintoihisi ja hyvää syksyä!
- Useasti virustorjuntaohjelmat väittävät jotain tiedostoja viruksiksi joita ne ei kuitenkaan ole, ehkä vain epäilyttäviä. Tämä saattaa johtaa harhaan monet käyttäjät.

Työn esitys

Verkkorikollisuus

- verkossa tapahtuva rikollisuus
- tietokone, internet

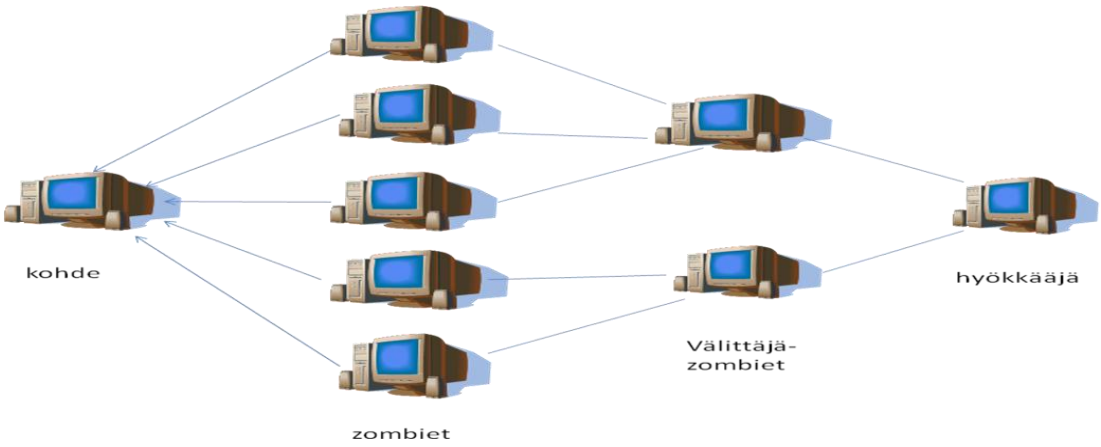
Haittaohjelmat

- ohjelma, joka tulee tietokoneelle käyttäen hyväkseen tietokoneen heikkouksia tai käyttäjän hyväuskoisuutta
- virus: ohjelma, jotka päästessään tietokoneeseen muuttaa alkuperäisiä ohjelmia, siten, että alkuperäinen ohjelma saadaan tekemään kopioita viruksesta. Tarvitsee isäntäohjelman.
- mato: ohjelma, joka leviää internetin välityksellä koneesta toiseen. Leviää itse itseään kopioimalla.
- takaovi: ohjelma, joka tarjoaa hyökkääjälle avoimen pääsyn järjestelmään.
- troijalainen: työkalu, joka avaa portin uhrin koneeseen.
- rootkit: ohjelmakokoelma, joka asentuu systeemiin mahdollistaakseen ylläpitäjän pääsyn systeemiin
- botti ja bottiverkko: haittaohjelma, joka antaa hyökkääjälle tietokoneen hallinnan. Bottiverkko on saastuneiden tietokoneiden eli zombie-koneiden verkko

Hyökkäysmallit

- roskaposti eli spam: käyttäjälle riesa
- palvelunestohyökkäys: katso alla oleva kuva hajautetusta palvelunestohyökkäyksestä

Hajautettu palvelunestohyökkäys:



Social engineering -hyökkäykset

- phising eli khalastelu eli verkkourkinta: huijarit haluavat käyttäjän salasanat
- pharming: käyttäjä ohjataan valesivustoon

Torjunta

- palomuuri: erikoistunut yhteyksien käsittelyyn
- virustentorjuntaohjelma: tutkii taustalla nettiselailua, verkkoliikennettä, tiedostojen käsittelyä
- päivittäminen: käyttöjärjestelmä, selain, ohjelma

Miten saat haittaohjelmat koneelle ja pääset bottiverkkoon:

- Älä suojaa tietokonettasi millään tavalla
- Kun saat viestin, ”haluatko haittaohjelman koneelle”, vastaa riemuiten ”yes”.
- Hyväksy kaikki kiva, mitä roskapostista tulee.
- Surffaa kaikilla epämääräisillä sivuilla.

Seuraus----------> Olet osa bottiverkkoa ja pääset osalliseksi esimerkiksi Facebookin kaatoon osana palvelunestohyökkäystä. On myös mahdollista, että pääset osaksi jännittävää rikollismaailmaa, jossa harjoitetaan rahanpesua ja kaikkea muuta ”kivaa”.

Haluatko olla osa bottiverkkoa ??????????

Toivottavasti et!

Toimi siis seuraavasti (Petteri Järvisen mukaan)

- Yes-klikkaus ei ole aina viisasta varsinkaan, jos ei ymmärrä kysymystä.
- Kun netistä päättää ladata mainostetun turvaohjelman, pitää muistaa, että myös vale-turvaohjelmia on olemassa.
- Lisäohjelmien asennuksessa kannattaa kuunnella muiden käyttäjien suosituksia tai lukea lehdestä lisätietoja. Harkintaa kannattaa käyttää.
- Koneen sammutus ja irrotus verkkoyhteydestä kannattaa, jos tietokone on pidempiä aikoja käyttämättä.
- Käytettäviin spyware- ja virustorjuntaohjelmiin ei kannata luottaa sokeasti.
- Tietokoneessa valmiiksi oleva palomuuri ei auta mitään, jos se ei ole käytössä.
- Käyttöjärjestelmän ja selaimen säännöllisistä päivityksistä kannattaa huolehtia.
- Selaimen ja sähköpostiohjelman vaihtaminen vähemmän suosittuun kannattaa. Haittaohjelmien tekijät eivät ole välttämättä kiinnostuneita niistä.

Tutkimustuloksia:

- vertailu tavallisiksi käyttäjiksi ja jonkin verran ammattilaisiksi luokiteltujen mukaan
- vertailu ikäryhmien kesken (alle 35-v, 35-44v, 45-54v, yli 55-v)

LOPPURAPORTTI

TAUSTAA

Projektin tekijä työskentelee rahoituslaitoksessa. Aina välillä uutisoidaan siitä, kuinka verkkopankin käyttäjiltä on pyydetty pankkitunnuksia kalastus tarkoituksessa. Tämä on saanut tekijän kiinnostumaan tietoturva-asioista ja lukemaan alan kirjallisuutta. Valitettavasti HAAGA-HELIA ei kyennyt tarjoamaan iltaopiskelijalle tähän syventäviä opintoja. Toinen tekijää kiinnostava asia on ihmisnäkökulma tietoturva-asioihin.

Projekti ei liity mihinkään laajempaan kehittämiskokonaisuuteen. Sillä ei ole myöskään toimeksiantajaa.

Projektin tekijä haluaa aiheellaan herätellä tutkimuksen kohderyhmän miettimään tietoturva-asioita ja rohkaisemaan etsimään lisätietoa. Vasta opinnäytetyöhön liittyvä tutkimus osoittaa, jos niissä paljastuu olevan puutteita.

SAAVUTETUT TULOKSET

Projektin tavoitteena oli projektisuunnitelman mukaan tuottaa opinnäytetyö sekä kyselylomake. Nämä kyettiin tuottamaan. Lisäksi tuotettiin ”Työn esitys”, jota ei oltu luokiteltu projektin tavoitteeksi.

Projektia ei kyetty saattamaan loppuun alkuperäisen aikataulun mukaisesti 9.12.2009 eli projektin laadullista alkuperäistä tavoitetta ei kyetty toteuttamaan. Opinnäytetyön ohjauskokouksessa 30.11.2009 sovittiin uusi aikataulu, jonka mukaan työn piti valmistua 18.2.2010. Tästäkään ei kyetty pitämään kiinni vaan sovittiin epävirallisessa kokouksessa työn viivästymisestä vielä kuukauden verran eli työn valmistumiseksi sovittiin 11.3.2010. Tästä jouduttiin myös tinkimään ja työ on nyt menossa arviointiin 1.4.2010.

Projektin laadunvarmistus on varmennettu eri edistymisraporteissa, virallisissa ohjauskokouksissa sekä lukemattomissa epävirallisissa tapaamisissa. Ohjaaja on valvonut, että opinnäytetyö täyttää HAAGA-HELIAn opinnäytetyön tekemiselle asetetut tavoitteet. Näitä ovat tukeneet eri tapaamiset.

PROSESSI, TYÖN ETENEMINEN

Projekti alkoi aihe-ehdotuksella sekä aloituskokouksella 4.6.2010. Projektisuunnitelma hyväksyttiin samassa kokouksessa. Siinä sovittiin, että työ valmistuu 9.12.2009. Työn edistymistä seurattiin edistymisraporttien avulla. Virallisia seurantakokouksia oli kolme, joten edistymisraportteja tehtiin kolme:

seurantajakso	ohjauskokous
4.6.2009 - 17.8.2009	19.8.2009
20.8.2009 - 9.10.2009	12.10.2009
10.10.2009 - 19.11.2009	30.11.2009

Tämän lisäksi pidettiin epäviralliset kokoukset 26.8.2009, 2.9.2009, 20.1.2010, 28.1.2010 sekä 17.2.2010. Näistä kokouksista ei tehty pöytäkirjoja.

Ensimmäinen seurantajakso kattoi ajanjakson, jolloin työn tekijä tutustui viitekehykseen tulevaan teoriamateriaaliin. Tuossa jaksossa projektipäälliköllä oli kesäloma, jolloin ajankäyttö sujui odotetusti eli ongelmia ei ilmaantunut.

Toinen seurantajakso kattoi kyselylomakkeen tekemisen Webropolilla sekä lähettämisen eteenpäin. Ongelmia aiheutti se, että tulosten vertailu oli alun perin sovittu tehtäväksi liian vanhaan tutkimukseen. Aika oli kiireistä, koska projektipäällikkö teki opinnäytetyötä töiden ohessa. Työn tekeminen vaikeutui huomattavasti. Alkoi myös näyttää todennäköiseltä, että töissä alkava projekti sotkee asetettua aikataulua. Työn analysointi aiheutti ongelmia.

Kolmas seurantajakso oli opinnäytetyön tekemisen masentavin. Mikään ei tuntunut onnistuvan. Uusi vertailuryhmä ei ollut vertailukelpoinen, joten työn luonnetta piti muuttaa. Kävi melko nopeasti selväksi, että työn valmistuminen 10.12.2009 mennessä ei tule onnistumaan. 30.11.2009 pidetyssä ohjauskokouksessa muutettiin aikataulua.

Projektipäällikkö piti melkein puolentoista kuukauden tauon työn tekemisessä. Tämä selkeytti ajatuksia. Ohjaajalla oli tässä myös suuri merkitys. Häneltä löytyi aikaa ja kärsivällisyyttä ohjata projektipäällikön vaikean ajan yli.

Joulun jälkeen työ käynnistyi uudelleen. Pienten vastoinkäymisten jälkeen opinnäytetyö on arvioitavana 1.4.2010. Loppukokousta ei pidetty vaan ohjaaja hyväksyi työn sähköpostitse 18.3.2010.

KUSTANNUKSET

Projektille ei ollut tehty erillistä kustannusarviota, koska projekti ei edellyttänyt välineiden hankintaa tai ulkopuolisen työvoiman käyttöä. Oman työtunnin hinnaksi oli arvioitu 0 euroa. Projekti ei poikennut arviosta. Siinä käytettiin projektin tekijän omia tiloja sekä Haaga-Heliassa olevia työtiloja. Kustannukset muodostuivat jälkimmäisen osalta laskennallisesti Haaga-Helian tila- ja välinebudjetista. Koska käyttöoikeus Webropoliin saatiin koulun kautta, myöskään tämä ei aiheuttanut projektin tekijälle erillisiä kustannuksia.

RESURSSIEN KÄYTTÖ

Projektipäällikkö oli resursoinut työhön 400 tuntia. Tuosta toteutui 74 prosenttia.

	projektin alusta		
	suunniteltu	toteutunut	
Henkilö/ tehtävä	tuntia	tuntia	%
Jaana Laaksonen	400	301	75
Yhteensä	**400**	**301**	**75**

Ero johtui siitä, että viitekehyksen lukemiseen oli resursoitu enemmän tunteja kuin mitä siihen loppujen lopuksi kului. Lähteinä käytettiin melko paljon internet-lähteitä, koska projektipäällikkö halusi työhönsä uusinta tietoa. Näiden lähteiden lukeminen nopeutti materiaalin keräämistä. Tutkimuksen tekemiseen kului jonkin verran enemmän tunteja kuin mitä oli alun perin resurssoitu. Tämä johtui ongelmista sekä kyselylomakkeen teossa että tutkimustulosten analysoinnissa ja kirjoittamisessa. Ylitys resursseissa oli 10 prosenttia.

KOKEMUKSET, OPPIMISKOKEMUKSET

Kokemukset opinnäytetyö-projektista olivat myönteiset. Vaikka aikataulu ei täysin pitänyt, oli viisasta asettaa uusi aikataulu, jotta tulos pystyi täyttämään sekä HAAGA-HELIAn opinnäytetyölle asetetut tavoitteet että projektipäällikön omat tavoitteet.

EHDOTUKSET JATKOTOIMENPITEIKSI

Projektipäällikön toive on, että vaikka opinnäytetyö ei ollut toimeksianto, siitä voi olla hyötyä työnantajalle. Koska projektipäällikkö on ollut työnantajan ulkoisten opintojen tuen piirissä, hän on saanut muutaman opintovapaan. Kun työ on valmis, työnantaja on myös kiinnostunut arkistoimaan sen. Opinnäytetyön liitteenä on ”Työn esitys”, josta on toivottavasti apua jossakin yksikön sisäisessä koulutuksessa.

SUOSITUKSET TOIMINTATAPOJEN MUUTTAMISEKSI

Projektipäällikkö ei ehkä ollut kovinkaan ihastunut, että opinnäytetyötä piti toteuttaa projektimuotoisena. Varsinkin alussa aika, jonka kulutti projektisuunnitelman tekemiseen, olisi heti halunnut käyttää varsinaisen viitekehyksen keräämiseen. Projektipäällikkö toki ymmärtää, ettei tämä kritiikki poista projektimuotoisuutta tulevista töistä. Iltaopiskelijalle tämä oli enemmänkin aikataulukysymys kuin vastenmielisyys projekteihin.

Olen kiitollinen ohjaajalleni Titta Ahlbergille, jolta löytyi runsaasti kärsivällisyyttä ohjatessaan opinnäytetyötäni. Hänen roolinsa korostui, koska opinnäytetyöni ei ollut toimeksianto. Olenkin kiitollinen, että HAAGA-HELIA on mahdollistanut sen, että työt voidaan tehdä ilman toimeksiantoa, vaikka se sitoo enemmän ohjaajan resursseja.