Petri Lahti

MAKSULLISTEN JA ILMAISTEN VIRUSTORJUNTAOHJELMIEN SUOJAUKSEN TEHOKKUUDEN VERTAILU

Insinöörityö
Kajaanin ammattikorkeakoulu
Tekniikan ja liikenteen ala
Tietotekniikan koulutusohjelma
Kevät 2014

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ
TIIVISTELMÄ

Koulutusala Tekniikka ja liikenne	Koulutusohjelma Tietotekniikka
Tekijä(t) Lahti Petri	
Työn nimi Maksullisten ja ilmaisten virustorjuntaohjelmien suojauksen tehokkuuden vertailu	
Vaihtoehtoiset ammattiopinnot Tietoturvateknologia	Toimeksiantaja Kajaanin ammattikorkeakoulu
Aika Kevät 2014	Sivumäärä ja liitteet 31

Opinnäytetyön tavoitteena oli verrata maksullisten ja ilmaisten virustorjuntaohjelmien suojauksen tehokkuutta ja ottaa selvää, kummat suojaisivat konetta paremmin. Aihe liittyy tietoturvaan, joka voidaan määritellä viidellä käsitteellä: luottamuksellisuus, eheys, käytettävyys, kiistämättömyys ja pääsynvalvonta. Käsitteillä pyritään esittelemään tietoturva mahdollisimman kattavasti.

Virustorjuntaohjelmat suojaavat haittaohjelmilta, jotka yrittävät levitä koneesta toiseen internetin kautta. Päästessään koneelle ne saattavat aiheuttaa uhrilleen vahinkoa. Yleisimpiä haittaohjelmia ovat troijalaiset ja Bot-verkot. Nykyään tietokoneissa täytyy olla myös palomuuri, joka estää epäilyttävän liikenteen tietokoneen lähiverkon ja internetin väliltä. Muita hyödyllisiä ohjelmia ovat etsintäohjelmat ja selainlaajennukset.

Työssä testattiin kolmea ilmaista ja kolme maksullista virustorjuntaohjelmaa. Testattavat ohjelmat olivat F-Secure Internet Security 2014, Norton Internet Security 2014, Kaspersky PURE 3.0, Avast! Free Anti-Virus, Avira Free Anti-Virus ja Microsoft Security Essential. Testaus tapahtui Oracle VM VirtualBox -ohjelman kautta ajettavassa virtuaalisessa tietokoneessa. Testausten jälkeen verrattiin saadut tuloksia keskenään. Vertailussa ilmeni, ettei ilmaisten ja maksullisten ohjelmien suojauksen tehokkuudessa suuria eroja. Norton, Kaspersky ja Microsoft Security Essential torjuivat parhaiten testivirukset. Kuitenkin ilmaisilla ohjelmilla pystyy turvaamaan helposti kotikäyttöisen tietokoneen, mutta käyttäjän kannattaa ensiksi varmistua ohjelman luotettavuudesta.

Kieli	Suomi
Asiasanat	Tietoturva, virustorjuntaohjelma, virtuaalinen kone, ohjelmistotestaus
Säilytyspaikka	☐ Verkkokirjasto Theseus ☐ Kajaanin ammattikorkeakoulun kirjasto

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

THESIS ABSTRACT

School School of Engineering	Degree Programme Information Technology
Author(s) Lahti Petri	
Title Comparison of Protection Effectiveness between Paid and Free Anti-virus Programs	
Optional Professional Studies Data Security Technology	Commissioned by Kajaani University of Applied Sciences
Date Spring 2014	Total Number of Pages and Appendices 31

The aim of this thesis was to compare the protection effectiveness of paid and free anti-virus programs and find out which one is better for protecting computers. The topic is related to information security, which can be defined with five concepts: confidentiality, integrity, availability, non-repudiation, and access control. The aim is to present the concepts of security as comprehensively as possible.

Anti-virus software protects against malware that tries to spread from one computer to another through the Internet. When malware gets into a computer, it may cause damage to it. The most common types of malware are Trojans and Bot networks. Nowadays computers must also have a firewall that blocks suspicious traffic between the computer's local network and the Internet. Other useful programs are malware scanners and browser extensions.

Three paid and three free anti-virus programs were used in the tests. The programs were tested with F -Secure Internet Security 2014, Norton Internet Security 2014, Kaspersky PURE 3.0, Avast! Free Anti- Virus, Avira Free Anti-Virus and Microsoft Security Essentials. The testing took place in a virtual computer executed by Oracle VM VirtualBox. After the testing the results were compared with each other. The comparison showed that there were no major differences between the free and paid programs in protection. Norton, Kaspersky and Microsoft Security Essential were the best for rejecting the test viruses. However, you can secure a home computer with free software, but the user should first ascertain the reliability of the program.

Language of Thesis	Finnish
Keywords	data security, anti-virus, virtual machine, software testing
Deposited at	☐ Electronic library Theseus ☐ Library of Kajaani University of Applied Sciences

ALKUSANAT

Kiitän Raili Simanaista, Jukka Heinoa ja Eero Soinista rakentavasta ja avustavasta ohjauksesta.

Kiitokset myös Ismo Talukselle työni aiheen ehdottamisesta.

Sekä kiitokset luokkatovereilleni ja perheelleni, jotka tukivat ja kannustivat työni aikana.

SISÄLLYS

1 JOHDANTO

Tietokoneet ja internet ovat osa meidän arkista elämäämme. Netin kautta pystymme hoitamaan asioita helposti kotoa käsin, kuten laskujen maksamiset ja kaupassa käynti. Tietokoneiden ja internetin yleisyys on tuonut mukanaan myös uuden alueen rikollisuudelle. Nettihuijaamisen lisäksi ohjelmoinnista kiinnostuneet ovat alkaneet kehitellä ohjelmia, joilla voi aiheuttaa haittaa muille. Näitä on alettu kutsua yleiseltä nimeltä haittaohjelmiksi.

Haittaohjelmia vastaan on kehitetty ohjelmia, kuten palomuurit ja virustorjuntaohjelmat, joilla pystytään tunnistamaan uhat ennen kuin ne pääsevätkään koneeseen. Virustorjuntaohjelmien päämääränä on suojata lähiverkko, tietokone ja sen käyttäjän tiedot. Virustorjuntaohjelmia löytyy monena erilaisena versiona, joista osa on kohdistettu suojaamaan esimerkiksi isojen yritysten sisäisiä verkkoja. Virustorjuntaohjelmat ovat vuosimaksullisia sovelluksia, mutta nykyään ohjelmia löytyy myös ilmaisina. Tavallista koneen käyttäjää varmasti houkuttaa ilmainen virustorjuntaohjelma rahansäästön takia, mutta kykenevätkö ilmaiset ohjelmat olemaan yhtä turvallisia kuin maksulliset?

Opinnäytetyöni tavoite oli ottaa selvää, kumpi virustorjuntaohjelma versioista suojaa konetta paremmin. Työni aihetta ehdotti Kajaanin ammattikorkeakoulun opettaja Ismo Talus, joka halusi saada kyseiseen aiheeseen vastauksen. Opinnäytetyössä tutustutaan haittaohjelmiin, virustorjuntaohjelmiin ja haittaohjelmien torjuntaohjelmiin. Käytännön osassa testataan kolmea ilmaista ja kolmea maksullista virustorjuntaohjelmaa. Lopuksi vertaan testeistä saatuja tuloksia keskenään ja arvioin, mitä niistä voi päätellä. Verrattavina ohjelmina ovat Avast! Free Anti-Virus, Microsoft Security Essential, Avira Free Anti-Virus, F-Secure Internet Security 2014, Norton Internet Security 2014 ja Kasperesky.

2 TIETOTURVAN PERUSTEET

Tietoturvasta puhuttaessa varmasti monelle tulee mieleen varmuuskopioinnit, virukset tai hakkerit, jotka ovat oikeastaan vain yksi osa koko aihetta. Yrityksissä tämä tarkoittaa muun muassa henkilöstö-, palkka- tai tuotetietoja. Yksittäisen henkilön kohdalla suojattavat tiedot ovat pankki- ja luottokorttitiedot. Henkilötietojen suojaamisesta puhuttaessa käytetään myös nimeä tietosuoja. [1, s. 21.]

2.1 Tietoturvallisuuden määritelmä

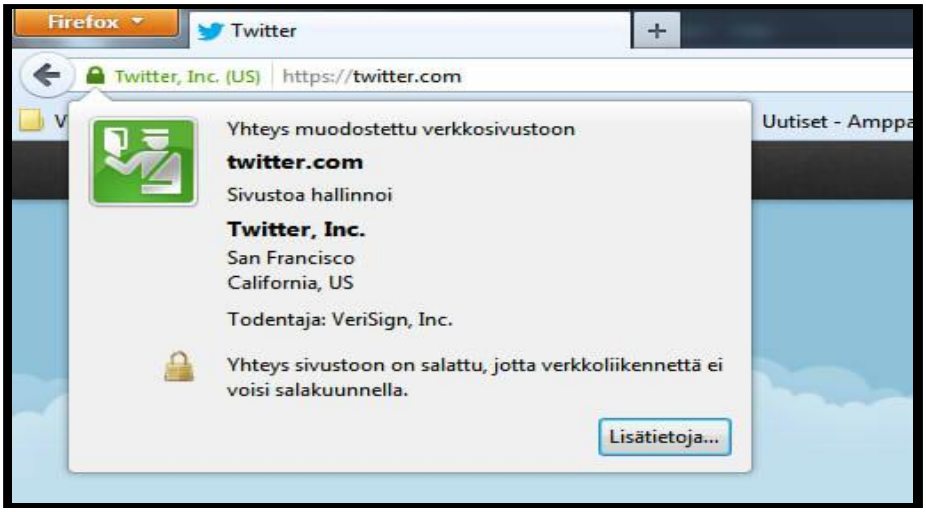
Tietoturvallisuuden määritelmä koostuu käsitteistä, jotka ovat tietoturvaan liittyviä perusvaatimuksia. Kolme ensimmäistä käsitettä ovat luottamuksellisuus, eheys ja käytettävyys. Nämä kolme käsitettä tunnetaan tietoturvan klassisena määrityksenä [2, s. 4]. Nykyisin klassista määritelmää pidetään suppeana, jonka takia on olemassa laajennettu määritelmä. Laajennetun tietoturvallisuuden määritelmässä kolmen käsitteen lisäksi on mukana kiistämättömyys ja pääsynvalvonta.[2, s. 5]

Luottamuksellisuudella tarkoitetaan, että tieto on vain siihen oikeutettujen käytössä [2, s. 4]. Esimerkiksi yrityksissä vain henkilöt, jotka ovat vastuussa yhtiön palkkatiedoista, pääsevät käsiksi yhtiön palkkatietoihin [3, s. 387]. Yrityksissä käyttöjärjestelmiin asetetaan henkilön tunnistus, joka toimii henkilökohtaisilla käyttäjätunnuksilla ja salasanoilla. Tällä tavalla voidaan määritellä henkilöiden käyttöoikeudet. [2, s. 4]. Yksittäisen henkilön kohdalla luottamuksellisuus on käytössä esimerkiksi sähköpostiviesteissä. Lähetetty viesti muutetaan salausmenetelmillä sellaiseen muotoon, ettei kukaan muu kuin viestin vastaanottaja voi lukea sitä. [3, s. 387.]

Eheys määrittelee, että tiedon tai palvelun sisältö ei saa olla muuttunut minkään tahallisen taikka tahattoman virheen takia. [1, s. 22]. Esimerkiksi sähköpostiin kiinnittynyt virus on myös tahallinen lisäys viestiin, mikä rikkoo viestin eheyden. Tietokoneita pyritään suojaamaan erilaisilla sovelluksilla, joilla voidaan estää tai korjata virheitä. [3, s. 387.]

Käytettävyydellä tarkoitetaan tietoa tai palvelua, joka on saatavilla riittävän nopeasti kaikille ja oikeassa muodossa [2, s. 4]. Nettisivut perustuvat käytettävyyteen. Nettisivun palvelimen tulee olla päällä vuorokauden ympäri, jotta käyttäjät voivat käydä sivulla. Kun palvelimelle tulee ongelma, käyttäjät eivät enää pääse sivulle ja saatavuus rikkoutuu. Palvelimelle myös voidaan tehdä palvelunestohyökkäys, jolla saadaan palvelimen hidastumaan taikka jumittumaan.

Kiistämättömyydellä halutaan varmistaa että tiedon, henkilön tai palvelun aitous on todistettavissa. Tätä valvotaan esimerkiksi henkilö-, järjestelmä- sekä nettisivun tunnistuksella. [1, s. 27.] Esimerkiksi alla olevassa kuvassa on esitelty salatun sivun tyyli Firefoxissa. Kuvassa näkyy myös sivun sertifikaatti eli varmenne, jonka saa esille napsuttamalla osoiterivillä olevaa lukon kuvaa (kuva 1). Sertifikaatti on kolmannen osapuolen hyväksymä todiste sivun aitoudesta. [3, s. 406.]



Kuva 1. Firefoxin kautta esiteltävä Twitterin sertifikaatti

Pääsynvalvonnalla pyritään rajaamaan, ketkä kykenevät käyttämään järjestelmää ja kuinka paljon. Suurissa yrityksissä on rajattu, kuinka paljon ominaisuuksia koneissa on käytössä jokaiselle työntekijälle.[3, s. 389]. Rajoituksina voi olla internetin selaaminen taikka tietokoneen asetusten muuttaminen. Yrityksissä on yleensä myös omat turvahenkilöt, jotka voivat antaa työntekijöille oikeuksia päästä käsiksi joihinkin sovelluksiin tai tiedostoihin.[2, s. 5.]

2.2 Tietoturvan osa-alueet

Tietoturvallisuus yleensä jaetaan moneen osaan, jotta niiden toteuttaminen olisi helpompaa. [2, s. 10] Tämän avulla yrityksissä voidaan myös jakaa vastuuta tietoturvallisuuden ylläpitoon. Yleisemmin käytetty jako on seuraava: Hallinnollinen tietoturva, henkilöturvallisuus, fyysinen tietoturva, ohjelmisto- ja tietoaineistoturvallisuus.

Hallinnollisella turvallisuudella pyritään tuottamaan tietoturvan valvontaa, sen kehittämistä ja johtamista yrityksissä. [3, s. 386.] Pienissä yrityksissä pyritään luomaan työntekijöiden kanssa yhteiset säännöt, kuinka pitää tietoturvaa yllä. Isoissa yrityksissä on olemassa oma osasto, joka hoitaa yrityksen tietoturvallisuuden ylläpidon. [2, s. 10.]

Henkilöturvallisuudessa tavoitteena on opastaa ja kouluttaa yrityksen työntekijät toimimaan Sääntöjen mukaisesti [3, s. 386]. Työntekijöiden pääsyä yrityksen tietoihin rajoitetaan ja valvotaan. Huonosti opastettu työntekijä saattaa olla tietoturvariski, koska hän ei saata tietää taikka ymmärtää tietoturvasääntöjä.[2, s. 11.] Pahimmassa tapauksessa työntekijä saattaa vaarantaa yhtiön tietojärjestelmän, mistä seuraa suuret tappiot yritykselle.

Fyysisellä tietoturvalla pyritään suojaamaan tietokone sen ulkopuolisilta uhilta. Työympäristössä tämä tarkoittaa tietokoneen sijaintia ja sen sisälle pääsyä. Esimerkiksi työntekijän ollessa ruokatauolla koneen tulisi olla lukitun oven takana tai vähintään vaatia käyttäjänsä salasanaa. Muutoin koneella saattaa käydä ulkopuolinen henkilö, joka voi päästä käsiksi yhtiön salaisiin tietoihin tai asentaa haittaohjelman. [2, s. 11.]

Kotikoneissa fyysinen turvallisuus keskittyy tietokoneen käyttäjän kavereihin ja perheen jäseniin. Perheellisessä kodissa kaikki perheen jäsenet käyvät koneella netissä ja saattavat asentaa myös pelejä.[1, s. 50.] Varsinkin lasten kanssa pitää olla tarkkana, koska he eivät ymmärrä tietoturvallisuuden monimutkaisuutta. He voivat olettaa koneen suojaavan heitä kaikelta, mitä internetistä tulee koneelle. Tämän takia jokaiselle perheen jäsenelle on kannattavaa vähintään asettaa omat käyttäjätilit, joiden käyttöä voidaan rajata.

Ohjelmistoturvallisuuden tavoitteena on pitää huolta, että ohjelmistot ovat sopivia vaadittuun käyttötarkoitukseen ja että ne eivät ole ristiriidassa minkään toisen ohjelmiston kanssa [2, s. 11]. Ohjelmistoturvallisuudella myös estetään koneisiin asennettujen ohjelmien laiton kopiointi [1, s. 113]. Netissä liikkuu paljon ihmisiä, jotka mielellään lataavat ilmaisen kopion markkinoidusta ohjelmistosta. Ohjelmiston voi saada asennettua toiselle koneelle, jos vain tietää siihen rekisteröidyn käyttäjätunnuksen ja sarjakoodin. Ohjelmistoturvallisuus perustuu laitteiden, esimerkiksi tietokoneiden ja tulostimien käyttöön ja niiden huoltoon. Laitteistojen kuluessa niissä pyritään ennaltaehkäisemään laitevikoja, joista käyttäjät voisivat jopa loukkaantua. [2, s. 12.]

Kotikoneet keräävät sisälleen paljon pölyä, joka kannattaa puhdistaa ajoittain. Pölyt tunkeutuvat tietokoneen pienen komponenttien väliin hidastaen konetta. Pahimmassa tapauksessa koneeseen kertynyt pöly saattaa syttyä tuleen ja rikkoa koneen komponentit, jolloin kone on käyttökelvoton.

Tietoaineistoturvallisuuden päämääränä on käytettyjen koneiden, levyjen, kovalevyjen ja levykkeiden oikeanlainen käyttö ja tuhoaminen [1, s. 113]. Kotikäyttöisiin koneisiin tämä vaikuttaa myös varmuuskopioinnilla. Varmuuskopiointi on tärkeiden tiedostojen kopiointia esimerkiksi siirrettävään kiintolevyyn, jolloin varmuuskopioidut tiedostot olisivat tallessa, vaikka tietokone särkyisi.

Yrityksissä tämä on tärkeää, koska näihin laitteisiin on tallennettu arkaluonteista tietoa, mikä voi aiheuttaa yritykselle tappioita joutuessaan vääriin käsiin. Tämän takia koneet, levyt ja paperit pyritään pitämään piilossa pääsyvalvonnan takana, jotta vain niihin oikeutetut pääsisivät käsittelemään niitä. Poistaessaan tietoaineistoa yritykset yleensä valitsevat yksityisen yrityksen, joka on erikoistunut tuhoamaan tallennuslaitteita.

3 VIRUSTORJUNTA JA HAITTAOHJELMAT

Yleensä puhuttaessa virustorjunnasta monelle tulee mieleen, että kyseessä olisi vain virustorjuntaohjelma ja palomuuri. Todellisuudessa virustorjunnalla tarkoitetaan kaikkia koneeseen hankittavia ohjelmia, joilla luodaan suojaus haittaohjelmia vastaan. Toisin sanoen virustorjunta on laaja käsite, johon kuuluu paljon muitakin ohjelmia ja työkaluja kuin palomuuri ja virustorjuntaohjelma.

3.1 Virustorjuntaohjelmat ja palomuurit

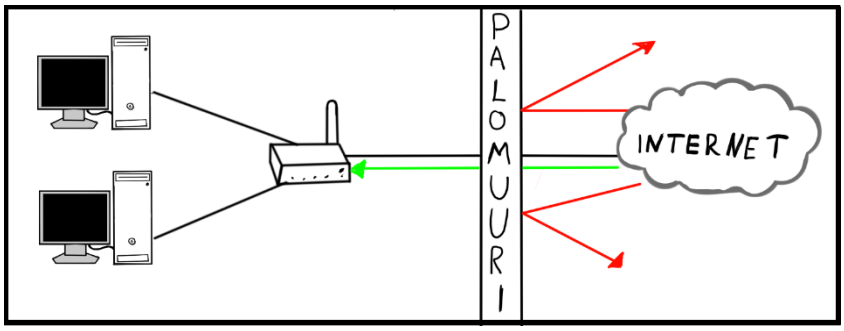
Nimi ”virustorjuntaohjelma” on käännetty nimestä anti-virus, joka tarkoittaa viruksen vastaista. Ohjelmat valvovat konetta ja estävät haittaohjelmia tekemästä ilkivaltaa koneelle. Virustorjuntaohjelmia voi asentaa Windows-käyttöjärjestelmän lisäksi Linux-, Mac-käyttöjärjestelmille ja nykyään myös älypuhelimille ja tableteille.

virustorjuntaohjelmat toimivat kahdella tavalla. Käyttäjä voi myös halutessaan käynnistää ohjelman skannauksen, jolla ohjelma etsii haittaohjelmia. Toinen tapa on reaaliaikainen virustorjunta, millä ohjelma tarkistaa itsekseen koneelle tulleita tiedostoja. Virustorjuntaohjelmat tunnistavat haittaohjelmia virustunnisteiden avulla. Virustunniste on tavallaan digitaalinen allekirjoitus, joka viittaa yksittäiseen haittaohjelmaan. Tarkistuksessa virustorjunta käy jokaisen tiedoston läpi vertaamalla virustunnistetietokantaansa. Virustorjuntaohjelmat eivät voi tunnistaa haittaohjelmia, joita ei ole listattu virustunnistetietokantaan. [2, s. 135.] Tämän takia virustorjuntaohjelmat kannattaa päivittää säännöllisesti.

Virustorjuntaohjelmat ovat yleensä vuosimaksullisia. Hinnat vaihtelevat kahdenkymmenen ja sadan euron välillä. Hintaan vaikuttaa se, mitä ominaisuuksia tulee ohjelman mukana. Ohjelmia voi ostaa netistä tuotteen tekijöiden omilta kotisivuilta tai tietokoneliikkeistä. Internetoperaattoritkin voivat tarjota virustorjunnan heidän kauttaan, jolloin käyttäjän ei tarvitse huolehtia virustorjuntaohjelman päivittämisestä. Valmiiksi rakennetuissa tietokonepaketeissa tulee yleensä mukana myös vuodeksi virustorjuntaohjelma, joka sisältyy koneen hintaan.

On myös olemassa ilmaisia virustorjuntaohjelmia. Nämä ovat ladattavissa netistä ja sisältävät vain tärkeimmät toiminnot koneen suojaamiseen. Ilmaisilla virustorjuntaohjelmilla pystyy hyvin suojaamaan kotikoneen taikka kahdesta neljään koneen lähiverkon. [4, s. 204.] Ilmaisen ohjelman riskinä on se, ettei voi tietää, toimiiko ohjelma niin kuin se väittää. Huonon ohjelman valitessaan ei voi syyttää ketään muuta kuin itseään. Ilmaisista ohjelmista on olemassa myös vuosimaksulliset versiot, joissa tulee mukana lisää hyödyllisiä toimintoja, kuten palomuuri.

Virustorjuntaohjelman lisäksi koneessa täytyy olla myös asennettuna palomuuri. Palomuuri on lähiverkon ja internetin välissä oleva portti, joka valvoo sen läpi kulkevaa liikennettä [3, s. 403]. Ohjelma ei päästä epäilyttävää liikennettä sisälle taikka ulos koneesta kuvan 2 mukaisesti. Palomuureilla voi myös rajata käyttäjien netti selaamista. Koneeseen asennettavat ohjelmapalomuurit ovat tunnetuimpia, ja ne on tarkoitettu yleisimmin kotikoneiden ja pienyritysten käyttöön. Ohjelmapalomuureja löytyy virustorjuntaohjelmien tapaan maksullisina ja ilmaisina ohjelmina. Nykyisissä Microsoft Windows -käyttöjärjestelmissä on oma palomuuri, jonka voi asettaa päälle tai pois. Windowsin palomuuri käynnistetään automaattisesti, ellei koneessa ole erillistä palomuuria. [5, s. 106–107.]



Kuva 2. Palomuuri kotiverkossa

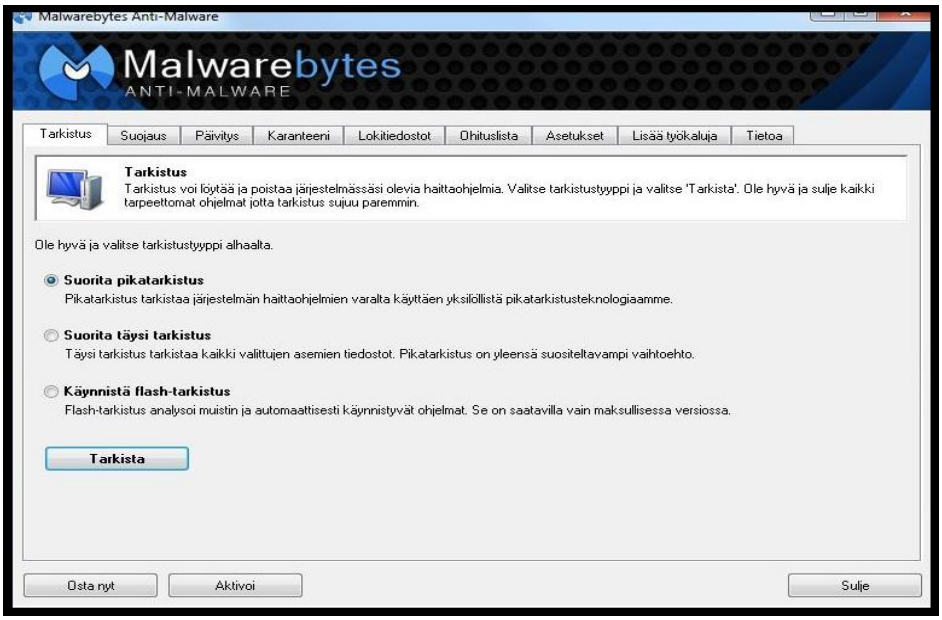
Palomuurisovellusten lisäksi on olemassa laitepalomuureja. Laitepalomuurit on suunniteltu yrityskäyttöön, koska niillä pystyy turvaamaan yritysten sisäisiä lähiverkkoja. Laite asetetaan lähiverkon ja Internetin väliin, jolloin se valvoo lähiverkkoon tulevaa liikennettä. Laitepalomuurit ovat turvallisempia kuin palomuurisovellukset, mutta ovat huomattavasti kalliimpia [5, s. 109–110].

3.2 Muita koneen suojausohjelmia

Virustorjuntaohjelman ja palomuurin lisäksi on olemassa lukuisia sovelluksia, joilla voi parantaa koneen suojausta. Nämä ohjelmat saattavat myös suojata koneen hyvin ilman muita ohjelmia tai päinvastaisesti tarvitsevat virustorjuntaohjelmien tukea. Näihin ohjelmiin kuuluvat muun muassa etsintäohjelmat ja selainlaajennukset.

Haittaohjelmien torjuntaohjelmat, kuten anti-malware ja anti-spyware, toimivat samankaltaisesti kuin virustorjuntaohjelmat. Ohjelmat eivät sisällä yhtä paljoa toimintoja kuin virustorjuntaohjelmat, mutta saattavat pystyä korjaamaan haittaohjelmien aiheuttamia vahinkoja [6, s. 103]. Etsintäohjelmat on tarkoitettu varmistamaan, onko koneessa haittaohjelmia, joita virustorjuntaohjelma ei ole huomannut. [5, s. 85–86.] Ohjelmat ovat enimmäkseen ilmaisia, mutta niistä on myös maksulliset versiot. Maksulliset versiot päivittyvät useammin ja toimivat paljon enemmän virustorjuntaohjelmien tavalla.

Esimerkiksi alla olevassa kuvassa on esillä Malwarebytes Anti-Malware. Ohjelma on ilmainen, mutta maksullinen versio sisältää reaaliaikaisen suojauksen, Flash-muistin tarkistuksen ja automaattisen ohjelman päivityksen (kuva 3).



Kuva 3. Malwarebytes Anti-Malwaren päävalikko

Nykyään virustorjuntaohjelmien mukana tulee selainlaajennus, jolla turvataan käyttäjän surffaaminen Internetissä. Esimerkiksi Avast Online Security kertoo, onko nettisivu turvallinen. Käyttäjän ollessa turvalliseksi todetulla sivulla Avastin logossa näkyy vihreä merkki. Turvallisille nettisivuille vievien linkkien perässä taas näkyy vihreä merkki.

Samankaltainen selainlaajennus on MyWot, jolla käyttäjä näkee sivujen luotettavuuden. Nimi tulee sanoista My Web Of Trust. MyWot kerää käyttäjiltään tietoja nettisivuista ja näyttää tulokset nettiosoitteen vieressä. Ohjelma käyttää liikennevalojen värejä esittämään sivujen luotettavuuden. Vihreä on hyvä, keltainen kohtalainen ja punainen huono [4, s. 69].

Kuva 4. Kajaanin AMK:n sivujen maine MyWotin mukaan

MyWotin kotisivujen kautta voi katsoa minkä tahansa sivun maineen. Esimerkiksi MyWotin käyttäjien mielestä Kajaanin AMK:n kotisivu on luotettava ja lapsiystävällinen, kuten ylhäällä olevasta kuvasta näkee (kuva 4). Käyttäjien avulla kerätty tieto nettisivujen luotettavuudesta sisältää omat vaaransa. On mahdotonta tietää, kuinka moni käyttäjistä on arvioinut sivuja vakavasti tai tahallisesti antanut sivulle huonon arvioinnin. Eli MyWot on hyvä selainlaajennus, mutta siihen ei kannata täysin luottaa.

3.3 Haittaohjelmat

Haittaohjelmat ovat pieniä ohjelmia, joiden tarkoituksena on levitä mahdollisimman moneen koneeseen. Ne leviävät tyypillisesti internetin kautta, mutta ne voidaan tuoda koneeseen myös koneen ulkopuolelta esimerkiksi USB-muistitikulla. Haittaohjelmat voivat aiheuttaa pilailuun tarkoitettuja viestejä tai animaatioita tai oikeasti aiheuttaa haittaa koneelle. [3, s. 410]

Ensimmäinen PC:n haittaohjelma oli virus nimeltä (c)Brain, joka löydettiin vuonna 1986 [3, s. 411]. (c)Brain levisi levykkeiden mukana koneesta toiseen, joissa se muutti kiintolevyjen nimeksi ”(c)Brian”.[1, s. 250] Internetin yleistymisen jälkeen virusten ja muiden haittaohjelmien määrä kasvoi huomattavasti. Haittaohjelmat esiintyvät yleisimmin PC:llä, mutta niiden määrä on alkanut kasvaa Linux ja Mac-käyttöjärjestelmissä.

Haittaohjelmien tekijöistä käytetään yleensä nimitystä ”hakkeri”. Hakkerit voivat olla nuoria opiskelijoita tai tietokoneista kiinnostuneita henkilöitä. Esimerkiksi Ilta-Sanomissa oli uutinen, jossa Runescape-nettipelissä käyttäjätunnuksia ja salasanoja varastelleeksi haittaohjelman tekijäksi oli paljastunut 11-vuotias kanadalainen poika. Hän oli vain varastanut tileistä pelin sisäistä valuuttaa, mutta hän olisi halutessaan pystynyt myös näkemään käyttäjätilien luottokorttitiedot. [7.]

Suurin syy haittaohjelmien tekoon on raha. Rikolliset ostavat haittaohjelmia omaan käyttöönsä. He maksavat näistä ohjelmista hyvin, koska niillä hankittava voitto voi olla paljon suurempi kuin ohjelmasta pyydetty hinta. Suosituimpia ovat vakoiluohjelmat ja helposti levitettävät haittaohjelmat, kuten nollapäiväaukon kautta leviävät haittaohjelmat. [5, s. 77–78.]

3.4 Miten haittaohjelmat pääsevät koneeseen?

Varmasti jokainen tietokoneen käyttäjä on saanut vähintään yhden tai useamman haittaohjelman tietokoneellensa. Lähes jokaisella haittaohjelmalla on oma tapa levitä. Jotkut ohjelmat leviävät itsestään, mutta toiset taas vaativat tietokoneen käyttäjän toimia levitäkseen.

Haittaohjelmat voivat piiloutua myös sähköpostiviesteihin, jotka yrittävät esittää olevansa esimerkiksi pankin virheilmoituksia tai ystävien hätäviestejä. Paras tapa tunnistaa haitalliset viestit on ottaa selvää, onko lähettäjä varmasti lähettänyt viestin. Sähköpostit pystyvät torjumaan suuren osan haitallisista posteista, mutta yksikään niistä ei ole täysin luotettavia.[5, s. 79] Haittaohjelmia löytyy nykyään myös käytetyimmistä sosiaalisista medioista, kuten Twitteristä ja Facebookista. Nämä palvelut ovat ihanteellisia paikkoja levittää haittaohjelmia, koska suurin osa niiden käyttäjistä ei ehkä ymmärrä tietokoneen toimintoja saati tietoturvansa perään.

Haittaohjelmat saattavat esittää olevansa selainlaajennuksia, esimerkiksi työkalurivejä. Nämä haittaohjelmat ovat hyvin vaikeita poistaa. Netistä onneksi löytyy lukuisia ohjeita, kuinka haitallinen liitännäinen poistetaan pysyvästi koneelta. Esimerkiksi hyvin haitallinen työkalurivi Snap.do. Työkalurivi muuttaa väkisin selaimen aloitussivun ja hakukoneen omakseen. Snap.do on myös yksi hankalimmista poistaa, koska pelkkä ohjelman poistaminen ei auta. Käyttäjän pitää poistaa snap.do itse menemällä jokaisen koneelle asennetun selaimen sisäisiin tiedostoihin ja palauttaa ne oletusasetuksiin. Vasta sen jälkeen työkalurivi on poistettu koneelta.

3.5 Haittaohjelmien tyyppejä

Nykyään netissä liikkuu paljon erilaisia haittaohjelmia, joista jokainen toimii hiukan eri tavalla. Haittaohjelmat on määritelty useaan eri ryhmään, mikä perustuu muun muassa niiden käyttäytymiseen ja leviämistapoihin.

Bot-verkko on nykyään yksi yleisimmistä haittaohjelmatyypeistä. Bot-verkot ovat tietokoneen ja sen verkkoyhteyden hallintaan suunniteltuja haittaohjelmia. Bot-verkon saastuttamat ”zombie”-koneet liitetään osaksi hyökkääjän hallitsemaa verkkoa. Bot-verkon uhriksi joutunut kone toimii normaalisti, mutta internetyhteys saattaa olla aiempaa hitaampi. Bot-verkot sisältävät tuhansia zombie-tietokoneita ympäri maailman. [3, s. 396.] Zombie-koneita käytetäänkin laittomiin tarkoituksiin, kuten haittaohjelmien ja roskapostin levittämiseen, sosiaalisten medioiden tilien murtautumiseen sekä palvelunestohyökkäyksiin [4, s. 179].

Troijalaiset tai Troijan hevoset on toinen yleisimmistä haittaohjelmatyypeistä. Ne naamioivat itsensä hyödyllisiksi ohjelmiksi päästäkseen uhrin koneeseen. Ohjelma toimii täysin käyttäjän huomaamatta, ja niitä käytetään avaamaan aukko palomuuriin, jotta muita haittaohjelmia pääsee sisään. [4, s. 178.] Uusia troijalaisperheeseen tulleita ovat pankkitroijalaiset, jotka huomaamattomasti tekevät pankkisiirtoja ulkomaisiin tileihin uhriensa pankkitileiltä. Ne osaavat myös peittää jälkensä, jolloin niiden uhrit eivät pysty näkemään pankkisiirtoja muuten kuin tiliotteen kautta. Löydettyjä pankkitroijalaisia ovat Zeus, SpyEye, Carberp, Gozi ja Patcher. [8.]

Troijalaisten mukana saattaa tulla muitakin haittaohjelmia, kuten adwaret ja spywaret. Spywaret vakoilevat koneen käyttöä. Ohjelmat seuraavat käyttäjien surffaamista netissä, minkä avulla ne laittavat adwaret esittämään oikeanlaisia mainoksia. [5, s. 80] Adwaret eivät ole suoranaisesti haittaohjelmia, mutta niitä voidaan käyttää myös nettihuijauksissa. Ne tuovat ajoittain ponnahdusikkunoita, jotka sisältävät mainoksia. Adwaret saattavat tulla myös oikeiden hyötyohjelmien kautta. Tällöin mainoksilla pyritään maksamaan ohjelmasta koituvia kuluja. [5, s. 100.]

Muita tunnettuja haittaohjelmatyyppejä ovat muun muassa tietokonevirukset ja madot. Tietokonevirukset olivat aluksi yleisimpiä haittaohjelmia, mutta nykyään niiden leviäminen on alkanut olla huomattavasti vähentymään päin. Tietokonevirukset leviävät esimerkiksi sähköpostin liitetiedostona tai USB-muistitikun mukana. Ne vaativat koneen käyttäjän toimia aktivoituakseen. Käynnistyessään virukset voivat muun muassa hidastaa koneen toimintaa, poistaa ja turmella tiedostoja. Pahimmassa tapauksessa virus saattaa poistaa tietokoneen BIOS-muistin, jonka takia kone ei saata enää käynnistyä. Madot taas ovat itsestään leviäviä haittaohjelmia, mutta ovat vähentyneet huomattavasti palomuurien ansiosta. Madot pääsevät myös koneen sisälle piilottamalla kopion itsestään tiedostoon tai sähköpostiviestin liitetiedostoon. Koneeseen päästyään mato saastuttaa koneen ja levittää kopioita itsestään eteenpäin esimerkiksi sähköpostin kautta. [4, s. 178].

4 TESTAUSYMPÄRISTÖN RAKENTAMINEN

Aluksi täytyi testata virustorjuntaohjelmia, jotta kyettiin vertaamaan niitä keskenään. Pyrittiin testaamaan, kuinka hyvin jokainen virustorjuntaohjelma kykeni tunnistamaan haittaohjelmia. Valittiin kuusi testattavaa virustorjuntaohjelmaa, joista kolme oli maksullisia ja kolme ilmaisia.

4.1 Testausympäristön suunnittelu

Aluksi suunniteltiin sopiva testausympäristö, jossa pystyttiin testaamaan virustorjuntaohjelmia. Testi tapahtui tietokoneessa, joten testissä käytettävän ympäristön tuli olla eristettynä muista mahdollisista tietokoneista ja lähiverkoista, koska testauksen aikana saatettiin käsitellä haittaohjelmia. Testausympäristön piti myös olla korjattavissa, vaikka haittaohjelmat sattuisivat saastuttamaan sen kelvottomaksi.

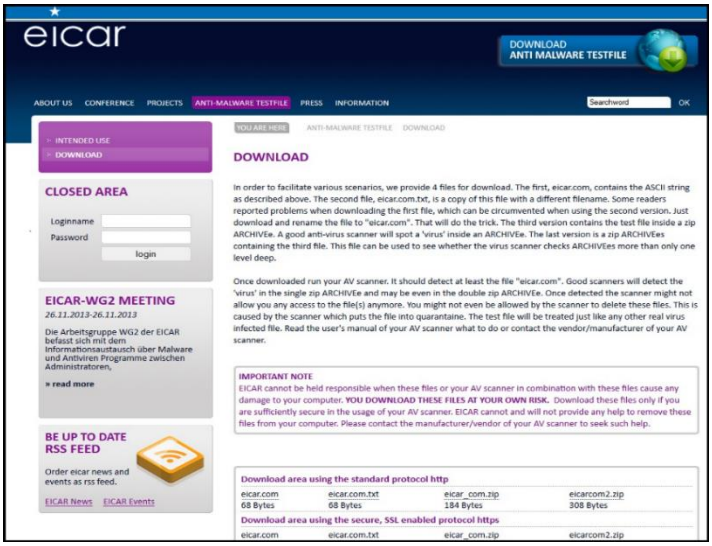
Näillä perusteilla testausympäristöksi valittiin virtuaalikone, joka on nimensä mukaisesti koneen sisällä virtuaalisesti ajettava tietokone. Virtuaalikoneet toimivat kuin oikeat tietokoneet, eivätkä ne kommunikoi isäntäkoneen kanssa ilman erillistä lupaa. Tällä tavalla haittaohjelmat eivät vahingossa siirry oikeaan koneeseen. Vahinkojen sattuessa virtuaalikoneen pystyy nopeasti korjaamaan tai luomaan kokonaan uudestaan. Käytetiin virtuaalikoneen luomiseen Oracle VM VirtualBoxia, koska ohjelmaan oli tutustuttu jo aikaisemmin.

Virtuaalikoneen käyttöjärjestelmäksi valittiin Windows 7, joka on käytetyin Windows-käyttöjärjestelmä [9]. Haittaohjelmathan suunnitellaan hyökkäämään käytetyimpiin ohjelmiin ja käyttöjärjestelmiin, jotta mahdollisimman moni jäisi niiden uhriksi. Windows 7:n asennuslevy pystyttiin lataamaan Microsoft DreamSparkista. Microsoft DreamSpark on alusta, josta koulujen oppilaat ja opettajat voivat hankkia Microsoftin tuotteita oppimistarkoitukseen. Kajaanin ammattikorkeakoulun opiskelijoille tuotteet ovat ilmaisia, mutta suurimman osan lisenssit toimivat vain kaksi vuotta.

4.2 Testitapausten suunnittelu

Suojaustason testaus täytyi tehdä enemmän kuin yhdellä tavalla, jotta saataisiin tarkempia tuloksia. Ensimmäisenä ajatuksena oli testata virustorjuntaohjelmat bigvirusback.zip:n avulla. Nimensä mukaisesti bigviruspack.zip sisälsi lähemmäksi 7000 virusta. Ikävä kyllä zip-tiedoston mukana tuli mato, joka ilmestyi myös isäntäkoneeseenkin. Mato oli ilmeisesti huomannut nettilinjan ”jakautuvan” kahteen erilliseen koneeseen ja päätynyt kopioimaan itsensä toiseenkin suuntaan. Isäntäkoneessa oleva Avast Free Anti-Virus onneksi huomasi häirikön ja esti sen toiminnan. Myös virtuaalikoneeseen asennettu F-Secure Internet Security 2014 pysäytti madon. Tarkistettiin isäntäkone vielä Malwarebytes Anti-Malware ohjelmalla, joka löysi madon jättämän kopion ja poisti sen. Tämän jälkeen päädyttiin isäntäkoneen turvallisuuden nimissä käyttämään pelkästään testiviruksia.

Etsittiin netistä sopivia testiviruksia ja löydettiin tietoturvaan erikoistuva organisaatio nimeltä EICAR. Yhtiön nimi on lyhenne sanoista **European Institute for Anti-virus Research**. EICAR on perustettu vuonna 1991, ja sen työhön kuuluu haittaohjelmien tutkiminen ja tietoturvauhkien torjuminen. EICAR:lla on testivirus, jota käytettiin tässä työssä. Testivirus on turvallinen tapa testata viruksentorjuntaohjelmaa. Sivu, joka näkyy kuvassa 5, esittelee toisen kahdesta tavasta testata virustorjuntaohjelmaa. Testivirus voidaan luoda itse testitiedostoon tai ladata se EICAR:n sivuilta. [10.]

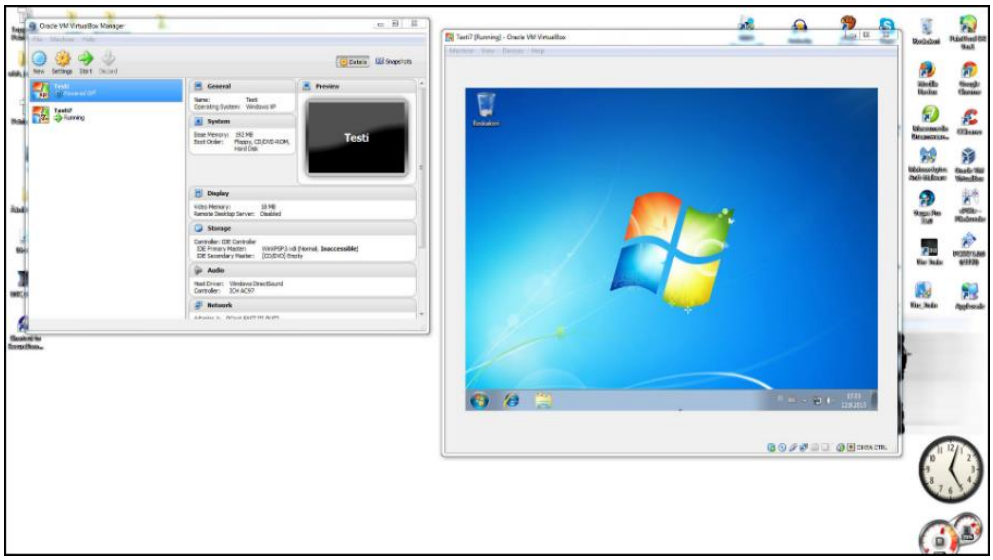


Kuva 5. EICAR:n testivirusten lataussivut

4.3 Oracle VM VirtualBox ja sen käyttöönotto

Oracle VM VirtualBox on ohjelma, jolla pystyy luomaan ja ajamaan virtuaalitietokoneita. Virtuaalikoneita voi olla monta samanaikaisesti luotuna, ja jokaisessa voi olla asennettuna eri käyttöjärjestelmä. VirtualBox toimii Windowsin lisäksi Linux- ja Mac-käyttöjärjestelmissä. Luodessa virtuaalikonetta käyttäjän pitää valita, minkä käyttöjärjestelmän haluaa asentaa virtuaalikoneeseen, mitkä osat isäntäkoneesta kommunikoivat sen kanssa ja kuinka paljon muistia varataan isäntäkoneesta siihen.

Tämän jälkeen käyttäjän tulee asettaa muistien määrät ja minne virtuaalikoneen tiedosto asennetaan. Virtuaalikoneen tiedostot voidaan asentaa halutessaan koneelle, levylle tai jopa muistitikulle. Sen koko riippui käyttöjärjestämästä, esimerkiksi Windows XP tarvitsee 192 Mt RAM-muistia ja Windows 7 tarvitsikin samaa muistia 512 Mt. Ohjelma myös suositteli virtuaaliasemalle varattavan n. 25 Gt muistitilaa. Ohjelma ei suoraan ota sille annettua muistitilaa käyttöönsä, vaan käyttää mahdollisimman vähän tilaa. Virtuaalikoneen koko kasvaa sitä mukaa, kun siihen tallennettiin lisää ohjelmia tai tiedostoja. Kuva 6 esittää, miltä käynnistetty Oracle VM VirtualBox näyttää.



Kuva 6. Oracle VM VirtualBox on käynnissä.

4.4 Valmistelut testausta varten

Ennen testitapauksia täytyi varmistaa, että jokainen testauskerta pystyttiin tekemään mahdollisimman samalla tavalla. Testausympäristössä tuli olla valmiina kaikki tarvittavat työkalut, jotta testaus pystyttiin suorittamaan alusta loppuun myös ilman ongelmia.

Loin uuden virtuaalikoneen Oracle VM VirtualBoxin avulla. Annoin virtuaalikoneen nimeksi ”testikone” ja käyttöjärjestelmäksi valittiin Windows 7. Asetin virtuaalikoneen RAM-muistiksi 512 Mt, ja luotiin uusi virtuaalinen kiintolevyn, johon varattiin 25 Gt muistia isäntäkoneesta. Annettiin VirtualBoxin tallentaa virtuaalikoneen kovalevyn VDI-tiedostona. Laitettiin muistin käytön asetukselle Dynamically allocated, minkä avulla ohjelma käyttää tallentamiseen vain tarvitun muistimäärän.

Tämän jälkeen avattiin virtuaalikoneen ja aloitettiin Windows 7 Professional N:n asennus. Asennettiin käyttöjärjestelmä oletusasetuksilla virtuaalikoneeseen. Asennuksen jälkeen annettiin käyttäjän nimeksi testaaja, jonka mukaan ohjelma automaattisesti nimesi koneen Testaaja-PC:ksi. Annettiin käyttöjärjestelmälle lupa päivittää itsensä automaattisesti ja nettiympäristöksi valittiin kotiryhmä. Lopuksi Windows 7 päivitti itsensä ja käynnisti itsensä uudelleen. Windows 7 Professional N:n asennuksen jälkeen asennettiin virtuaalikoneelle Google Chrome.

Tämän jälkeen otettiin snapshot virtuaalikoneen tilasta, jotta pystyttiin palauttamaan testausten jälkeen virtuaalikone takaisin samaan tilaan. Painoin virtuaalikoneen ikkunassa olevaa ”Machine”-nappia, josta avautui lista. Listasta valittiin toiminto ”Take Snapshot”, jolloin virtuaalikone muuttui kuvan 7:n mukaisesti harmaaksi ja pyysi nimeämään sen. Annettiin ohjelman tallentaa snapshot nimellä ”snapshot 1”.

5 TESTAUKSEN SUORITUS

Ennen testauksen suorittamista käynnistettiin Oracle VM VirtualBox ja varmistettiin kaiken olevan kunnossa. Tämän jälkeen aloitettiin testaus määriteltyjen ohjeiden mukaisesti, mutta varauduttiin mahdollisiin yllättäviin ongelmiin.

5.1 Ohjelmien asentaminen

Kirjattiin ohjelmien asennuksien kulku ennen varsinaista testausta. Asennuksen aikana kiinnitettiin huomiota sen helppokäyttöisyyteen, sekä mitä muita ohjelmia asentui virustorjuntaohjelman mukana.

F-Secure Internet Security 2014

Kokeiluversion lataamislinkki oli helppo löytää. Linkki oli iso painike tuoteselostuksen alta, jossa luki isoilla ”kokeile ilmaiseksi”. Tämä oli mukava yllätys, koska aikaisempien kokeiluversioiden linkit olivat hyvin pieniä. Valitessamme kokeiluversion F-Secure pyysi kirjoittamaan nimen ja sähköpostin. Tämän jälkeen F-Secure lähetti kyseiseen sähköpostiin linkin, jolla pystyi lataamaan ohjelman kokeiluversion.

Asennuksen aikana kysyttiin, haluttiinko käyttää reaaliaikaista suojausverkkoa, joka oli netin kautta toimiva nettisuoja. Kieltäydyttiin ottamasta verkkosuojaa, jonka jälkeen ohjelma alkoi asentaa F-Securea. Asennettaessa F-Securea tapahtui virhe, jonka takia F-Securen Computer Security ei asentunut koneelle ollenkaan. Poistettiin asennus ja kokeilin asentaa ohjelman uudelleen. Tällä kertaa ohjelma asentui oikein, jolloin pystyttiin aloittamaan testaaminen.

F-Secure Internet Security sisälsi kaksi erillistä ohjelmaa: Computer ja Internet Security, joihin pääsi F-Securen päävalikosta. Kumpikin ohjelma on ostettavissa erikseen, jos tietää tarvitsevansa vain toista näistä kahdesta ohjelmasta.

Norton Internet Security 2014

Nortonin tuotteiden testiversiot oli listattu omalle valikolle, joka avautui viemällä hiiri sivun valikossa olevaan ”Ladattava Sisältö” -painikkeen päälle. Tämä avasi listan, josta pystyi valitsemaan mieleisensä version Nortonista. Valittiin testattavaksi ohjelmaksi Norton Internet Security 2014. Tuotetta painamalla selain meni tuotteen omalle sivulle, josta pystyi lataamaan kokeiluversion. Norton ei pyytänyt mitään henkilökohtaisia tietoja, vaan antoi heti ladata kokeiluversion koneelle.

Asennusohjelmasta pystyi asettamaan ohjelman kielen, mutta ei kysytty haluttiinko muokata asennusta. Asennuksen muokkaaminen löytyikin asennuksen aloitusikkunasta, jossa oli painike kyseiselle toiminnolle. Asennuksen jälkeen ohjelma esitteli päävalikkonsa ja kuinka sitä käyttää. Tämän jälkeen ohjelma päivitti itsensä ja virustietokantansa ajan tasalle. Norton Internet Security 2014 sisälsi samat tietokone- ja nettiturvatoiminnot kuin F-secure, mutta niiden lisäksi Nortonissa oli myös oma palomuuri.

Kaspersky PURE 3.0

Kasperskyn kokeiluversio löytyi kätevästi sen kotisivuilta ”Trials & updates”-valikosta. Valitsin testattavaksi versioksi Kaspersky PURE 3.0:n, joka sisälsi Kasperskyn Anti-Viruksen, Internet Securityn ja Password Managerin. Asennuksen aikana ohjelma kysyi aktivointikoodia. Aktivointikoodirivin alla oli valittavana myös ilmainen kokeiluajan avaus, jota painamalla ohjelma asensi Kaspersky PURE:n. Asennuksen jälkeen ohjelma päivitti virustietokantansa ja käynnisti koneen uudestaan.

Ohjelma sisälsi tietokone- ja nettiturvan, mutta omasi myös tiedoston tuhoajan ja varmuuskopiointityökalun. Erilaisin ominaisuus oli kuitenkin Password Manager, jolla pystyi pitämään listaa kaikista käytetyistä salasanoista. Ohjelmalla pystyi luomaan salasanoja ja asettamaan sen kirjoittamaan käyttäjätunnuksen ja salasanan automaattisesti. Password Managerin pystyy ostamaan myös erikseen Kasperskyn sivuilta.

Avast! Free Anti-Virus

Valittiin asennettavaksi ohjelmaksi Avast! Free Anti-virus, koska nimensä mukaisesti ohjelma on ilmainen. Ennen kuin saatiin lupa ladata ohjelma, Avast! yritti tarjota maksullista versiotaan. Kieltäydyttiin tarjouksesta ja ladattiin asennusohjelma.

Kuten muissakin ohjelmissa, Avast! Free Anti-Viruksen asennuksessa on valittavissa kaksi asennustapaa. Pika-asennus asentaa ohjelman ja kaikki vaihtoehtoiset toiminnot koneelle. Muokatussa asennuksessa taas annetaan käyttäjän määritellä asennettavat ominaisuudet. Valittiin muokattu asennus ja Avast! kysyi, haluttiinko asentaa Google Chrome -nettiselaimen. Tämän jälkeen kokeiltiin, asentuuko Google Chrome ohjelman mukana, jos valittiin pika-asennus. Pika-asennuksen lopuksi löydettiin koneelta Google Chrome. Avastin mukana siis asentuu Google Chrome ilman, että käyttäjältä kysytään lupaa. Käyttäjien siis pitää tajuta käyttää ”muokattu asennus” -vaihtoehtoa, jotta he saavat vaihtoehdoksi estää selaimen asennus.

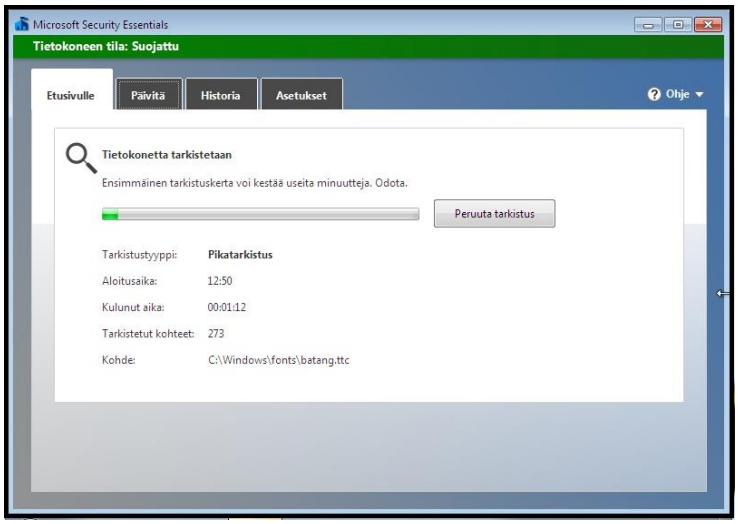
Avira Free Anti-Virus

Ladattiin Avira Free Anti-Viruksen ohjelma sen omilta kotisivuilta. Heti ensimmäisellä sivulla oli näkyvissä vihreä ”Download now”-nappi, josta pääsee lataamaan ohjelman. Ohjelman ladatessa sivulla ehdotetaan asentamaan Aviran oma selainlaajennus selaimeen. Kieltäydyttiin selainlaajennuksen asentamisesta.

Kuten muutkin asennusohjelmat, Avira Free Anti-Viruksen asennusohjelma aloitti kysymällä asennustapaa. Valittiin muokattu asennus, jotta nähtiin, mitä ominaisuuksia tai ohjelmia asentui koneelle. Valittavina ominaisuuksina oli reaaliaikainen virustorjunta, Rootkit- ja nettisuojaus. Avira käytti palomuurinaan Windowsin omaa palomuuria. Annettiin ohjelman asentaa kaikki oletusominaisuudet. Asennuksen lopuksi ohjelma pyysi valitsemaan miltä kaikilta uhkaavilta tekijöiltä haluttiin konetta suojaavan. Valittavina kohteina oli haittaohjelmien tapaisia uhkia, kuten huijausohjelmat, pilailuohjelmat, nettipelit sekä ad- ja spywaret. Valittiin vain kaikki haitalliset vaihtoehdot. Asennuksen ohjelma tarkisti koneen.

Microsoft Security Essentials

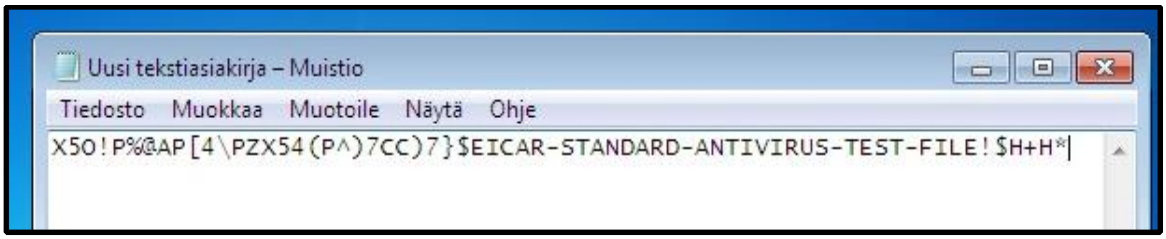
Microsoft Security Essentials on Microsoftin oma ilmainen virustorjuntaohjelma, jonka pystyy lataamaan Microsoftin omilta sivuilta. Ohjelma kysyi, haluttiinko ohjelman keräävän tietoa kohdatuista haittaohjelmista ja lähettävän ne Microsoftille. Hyväksyttiin pyyntö, jonka jälkeen ohjelma vaati poistamaan muut virustorjuntaohjelmat, jos niitä oli asennettuna koneelle. Asennuksen jälkeen ohjelma pyysi luvan tarkistaa koneen mahdollisilta tartunnoilta. Alla olevassa kuvassa Microsoft Security Essentials on suorittamassa koneen tarkistusta (kuva 7).



Kuva 7. Microsoft Security Essentials tarkistaa konetta.

5.2 Testitapaus 1

Ensimmäisessä testitapauksessa luotiin testivirus työpöydälle. Tapaus testasi ohjelmien reaaliaikaista virustorjuntaa. Aluksi luotiin työpöydälle uusi tekstitiedosto painamalla hiiren oikeaa painiketta, josta avautui valikko. Valikosta valitaan ”uusi”-painike, josta avautui toinen valikko. Tästä valikosta valitaan ”tekstitiedosto”, joka loi työpöydälle uuden tekstitiedoston. Tekstitiedoston nimenä annettiin olla ”Uusi tekstitiedosto”. Tämän jälkeen avattiin tekstitiedosto kaksoisnapauttamalla sitä. Tekstitiedostoon kirjoitettiin kuvan 8:n mukainen merkkirivi.



Kuva 8. Testivirus kirjoitettuna tekstitiedostoon

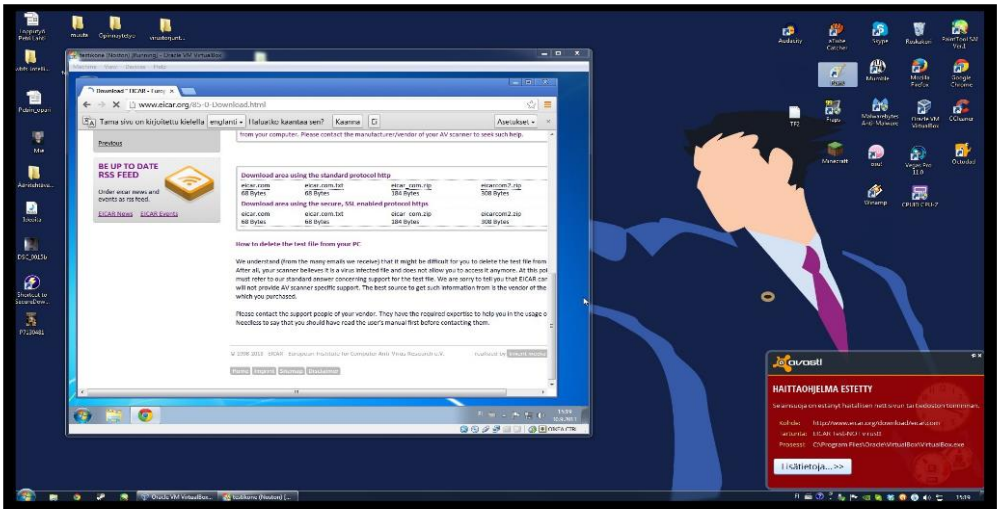
Merkkirivin voi käydä myös kopioimassa EICAR:n kotisivuilta ja liittää suoraan tekstitiedostoon. Merkkirivin kirjoittamisen jälkeen tallennettiin ja suljettiin tekstitiedosto. Tämän jälkeen odotettiin kolme minuuttia. Jos virustorjuntaohjelma ei siihen mennessä ilmoittanut mitään, siirrettiin tiedosto kansioon. Mikäli tämäkään ei herättänyt virustorjuntaohjelman huomiota, siirrettiin testivirus takaisin työpöydälle ja laitettiin ohjelma skannaamaan työpöytä.

F-Secure, Avast, Avira ja Microsoft Security Essentials eivät huomanneet luotua testivirusta. Jokaisessa tapauksessa siirrettiin testivirus työpöydältä toiseen kansioon, mutta sekään ei auttanut. Laitettiin tiedosto vielä takaisin työpöydälle ja ajettiin työpöydän skannaus. Skannauksen jälkeen ohjelmat ilmoittivat testiviruksesta. Huomattuaan testiviruksen F-Secure ja Avira laittoivat testiviruksen viruskaranteeniin, Microsoft Security Essential puhdisti sen ja jostain syystä Avast ei tehnyt testivirukselle mitään. Norton ja Kaspersky tunnistivat testiviruksen heti, kun suljettiin tekstitiedosto. Norton laittoi testiviruksen viruskaranteeniin, kun taas Kaspersky pyysi lupaa poistaa sen koneelta.

5.3 Testitapaus 2

Toisessa tapauksessa ladattiin testiviruksia erilaisina tiedostoina. Tällä testattiin ohjelmien nettisuojausta. Aluksi avattiin nettiselain ja mentiin EICAR:n kotisivulle http://www.eicar.org/85-0-Download.html, josta löytyi ensimmäisen testitapauksen testivirus ladattavassa muodossa. Ladattavia tiedostoja oli neljä erilaista, jotka voitiin ladata normaalin tai salatun verkon kautta. Kokonaisuudessaan ladattiin kahdeksan testivirusta. Katsottiin, kuinka moni näistä tiedostoista pääsi tallentumaan koneelle ilman, että virustorjuntaohjelma huomasi.

Testin alussa kohdattiin ongelmia. Isäntäkoneen oma virustorjuntaohjelma Avast! Free Internet Security huomasi lataukset ja esti tiedostojen pääsemästä perille (kuva 9). Lisättiin EICAR:n kotisivut Avastin poikkeuslistalle, jotta pystyttiin jatkamaan. Tämän jälkeen virtuaalikoneella oleva nettiselain Google Chrome huomasi virukset ja ilmoitti epäilyttävistä tiedostoista. Selain kysyi, haluttiinko ladata epäilyttäviä tiedostoja. Laitoin selaimen lataamaan tiedostot. Vasta tämän jälkeen pystyttiin jatkamaan testitapausta.



Kuva 9. Avast huomasi testivirusten lataamisen virtuaalikoneeseen.

F-secure huomasi ja poisti tiedoston Eicar.com. Muissa tapauksissa F-Secure ei antanut lupaa edetä lataamislinkin sivulle, joten kokeiltiin ladata samat tiedostot salatussa verkossa. F-Secure onnistui taas poistamaan tiedoston Eicar.com, mutta tällä kertaa ohjelma antoikin ladata kolme muuta tiedostoa. Tämän jälkeen laitettiin F-Secure tarkistamaan Ladatut tiedostot -kansion, jolloin ohjelma huomasi kolme testivirusta ja laittoi ne viruskaranteeniin.

Norton Internet Security esti normaalin verkon kautta tiedostot eicar.com ja eicar_com.zip. Ladatessa eicarcom2.zip:n ja eicar.com.txt:n Norton ilmoitti, että tiedostot olivat epäilyttäviä ja kysyi, haluttiinko jatkaa niiden lataamista. Laitettiin Nortonin antamaan tiedostojen lautua koneelle. Salatun verkon kautta Norton esti taas eicar.com:n ja eicar_com.zip:n lautumasta koneelle. Tällä kertaa tiedostot eicarcom2.zip ja eicar.com.txt pääsivätkin lautumaan koneelle. Lopuksi laitoin ohjelman tarkistamaan Ladatut tiedostot -kansion, josta se löysi ladatut testivirukset.

Kaspersky ilmoitti jokaisen normaalin verkon kautta ladattavan tiedoston olevan vaarallinen. Ohjelma antoi kuitenkin selaimen jatkaa testivirusten lataamistaan. Salatun verkon kautta ladatessa kävi juuri samoin. Kaspersky ilmoitti ladattavien tiedostojen olevan vaarallisia, mutta antoi lataamisen jatkua. Kun kaikki tiedostot olivat latautuneet, käytiin katsomassa Ladatut tiedostot -kansio, josta löytyi kaikki kahdeksan tiedostoa. Laitettiin Kasperskyn skannaamaan Ladatut tiedostot -kansio, jonka jälkeen ohjelma löysi testivirukset ja poisti ne koneelta. Lopuksi Kaspersky vielä tarkisti koneen mahdollisilta vaurioilta, mutta ei tietenkään löytänyt mitään.

Avast esti moitteettomasti kaikki normaalin verkon kautta ladattavat testivirukset. Salatun verkon kautta ladattavista tiedostoista Avast esti vain Eicar.com:in, mutta jostain syystä Windows Defender kolme muuta. Tämä oli ensimmäinen kerta, kun Windows defender reagoi ladattaviin testiviruksiin. Sama tilanne toistui myös salatun verkon kautta ladattavien tiedostojen kanssa.

Avira ei ainoastaan estänyt lataamasta normaalin verkon kautta, se myös esti menemästä EICAR:n kotisivulle. Avira taisi huomata sivulla olevan mahdollisia haittaohjelmia, joten se ilmoitti sivun olevan vaarallinen. Salatun verkon kautta eicar.com latautui koneelle, mutta ohjelma huomasi sen heti latauksen jälkeen. Annettiin ohjelmalle luvan poistaa tiedostot, jonka jälkeen Avira tarkisti koko koneen. Avira antoi muiden tiedostojen latautua koneelle. Lopuksi laitettiin ohjelma skannaamaan Ladatut tiedostot -kansion, jolloin ohjelma löysi ladatut testivirukset.

Viimeisenä testattiin Microsoft Security Essentialsia. Suurena yllätyksenä ohjelma esti kaikki ladattavat testivirukset normaalissa ja salatussa verkossa. Katsottiin vielä varmuuden vuoksi latauskansio läpi, joka oli myös tyhjä.

5.4 Tulosten vertailu

Testitapausten jälkeen oli aika verrata saatuja tuloksia keskenään. Aluksi tehtiin taulukkoa testitapauksien tuloksista, jotta olisi helpompaa verrata ohjelmia keskenään.

Taulukko 1. Testitapausten tulokset

	Testitapaus 1	Testitapaus 2	
Testattava ohjelma	Työpöydälle luotu testivirus	Ladattavat testivirukset (Normaali verkko)	Ladattavat testivirukset (Salattu verkko)
F-Secure Internet Security 2014	EI REAGOINUT	4/4	1/4
Norton Internet Security 2014	REAGOI	4/4	2/4
Kaspersky PURE 3.0	REAGOI	0/4	0/4
Avast! Free Anti-Virus	EI REAGOINUT	4/4	1/4
Avira Internet Security	EI REAGOINUT	4/4	1/4
Microsoft Security Essential	EI REAGOINUT	4/4	4/4

Tarkastelemalla ensimmäisen testitapauksen tuloksia huomataan, että vain Norton Internet Security 2014 ja Kaspersky PURE 3.0 onnistuivat huomaamaan työpöydälle luodun testiviruksen. Tämä näyttäisi tarkoittavan, että maksullisten virustorjuntaohjelmien reaaliaikainen haittaohjelmien tunnistus olisi parempi kuin ilmaisten. Olin yllättynyt, koska aikaisemmissa testeissä F-Secure, Avast ja Avira kykenivät tunnistamaan luodun testiviruksen. Syynä voi olla päivitetty virustunnistetietokanta, jonka takia EICAR:n testiviruksen tunniste on saattanut vahingossa poistua listalta. Toisaalta jokainen ohjelmista tunnisti testiviruksen, kun laitoin ne tarkistamaan sen.

Toisessa testitapauksessa huomattiin, että jokainen virustorjuntaohjelma kykeni tunnistamaan ladatut testivirukset normaalin verkon kautta ladatessa. Osa ohjelmista jopa esti latauslinkin käyttämisen. Melkein kaikilla ohjelmilla oli vaikeuksia tunnistaa ladattavia testiviruksia salatun verkon kautta. Kaspersky PURE 3.0 tunnisti kaikki testivirukset, mutta ei estänyt tiedostoja latautumasta koneelle. Tämä voi johtua testauksessa tapahtuneessa virheestä, jota ei huomattu. Ehkä ohjelmassa oli olemassa tapa, jolla se olisi estänyt niiden latautumisen. Toisena erikoisena huomiona on se, että ainoastaan Microsoft Security Essential kykeni tunnistamaan salatun verkon kautta ladattavat testivirukset. Uskoakseni ohjelmalla on Microsoftin avulla kyky tietää salatusta verkosta EICAR:in kautta.

Tulokset olisivat voineet olla myös paremmat. Testivirukset ovat virustorjuntaohjelmien tekijöiden kanssa sovittuja, joten ne pitäisi olla automaattisesti listattuna ohjelmien virustietokantoihin. Oikeiden haittaohjelmien kanssa olisin saanut parempia tuloksia, mutta olisin tarvinnut silloin paremman testausympäristön. Kaksi testitapausta ei ole myöskään tarpeeksi tarkka määrittämään virustorjuntaohjelmien torjunnan tehokkuutta. Minulta jäi ainakin kolme eri aluetta testaamatta, jotka olivat sähköpostin, makrovirusten sekä nettihuijausten torjunta. Testausympäristö ei ollut vain tarpeeksi hyvä, jotta olisin voinut uskaltaa testata näitä.

5.5 Lopputulokset

Testien kautta saatujen tulosten mukaan ilmaisten ja maksullisten virustorjuntaohjelmien välillä ei ole suuria eroja. Virustunnistukset näyttävät olevan parempia maksullisten ohjelmien kanssa, mutta ilmaisten puolella Microsoft Security Essentials esti kaiken. Testauksesta olisi voinut saada tarkemman, jos olisi ollut mahdollista lisätä edes yksi testitapaus.

Kaikki riippuu siitä, haluaako koneen käyttäjä maksaa vuosittain ohjelmasta, jotta hänen koneensa olisi turvassa. Maksaessaan virustorjuntaohjelmasta käyttäjä voi tuntea olonsa turvalliseksi, koska jos ohjelma ei toimi vaaditulla tavalla, hän voi pyytää korvausta siitä. Ilmaisen ohjelman toimiessa väärin käyttäjä ei voi kuin syyttää itseään. Toisaalta normaali kotikone ei tarvitse isoja kalliita virustentorjuntaohjelmia suojaamaan. Microsoft Security Essentialsin avulla pärjää mainiosti.

Virustorjuntaohjelmaa etsiessä kannattaa lukea monia eri arvosteluja ja lukea mitä ihmiset suosittelevat. Netissä on sivu nimeltä AV-Test.org, josta löytää tietoa virustorjuntaohjelmista. [6, s. 103.] AV-TEST on yksityinen tutkimuslaitos, joka on perehtynyt tietoturvan ja virustorjuntaohjelmien tutkimiseen. AV-TEST testaa ohjelmia neljässä kategoriassa: suojaus, suorituskyky, käytettävyys ja korjattavuus. Nämä kaikki neljä sisältävät laajat testit, joilla saadaan hyvät tulokset virustorjuntaohjelman luotettavuudesta. Yhtiöllä on kotisivuillaan lista testien tuloksista. AV-Test vertailee ohjelmia Microsoft Security Essentialsiin. [11.]

6 YHTEENVETO

Opinnäytetyöni tavoitteena oli verrata maksullisia ja ilmaisia virustorjuntaohjelmia keskenään ja saada selville, kumman suojaus oli parempi.

Tietoturvallisuuden määritelmässä on viisi käsitettä, joilla pyritään esittelemään tiedon turvaaminen mahdollisimman kattavasti. Tietoturvan osa-alueiden määrittäminen auttaa hyvän tietoturvallisuuden luomiseen yrityksissä. Virustorjuntaohjelmat suojaavat tietokonetta haittaohjelmilta. Palomuurit ovat tietokoneen lähiverkon ja internetin välissä oleva portti, joka estää epäilyttävän liikenteen kulkemasta sen läpi. Etsintäohjelmat ovat vain skannereita, jotka on tehty tunnistamaan tietyntyyppisiä haittaohjelmia. Virustorjuntaohjelmat asentavat nettiselaimiin myös selainlaajennuksia, joilla voi nähdä, mitkä sivut ovat turvallisia.

Haittaohjelmat ovat pieniä ohjelmia, jotka yrittävät levitä koneesta toiseen. Ne yleensä leviävät netin kautta, mutta kykenevät myös tunkeutumaan toiseen koneeseen esimerkiksi USB-tikun kautta. Päästessään koneelle ne aktivoituvat ja pyrkivät aiheuttamaan haittaa. Yleisimmät haittaohjelmat leviävät ladattavien tiedostojen mukana, sähköpostin tai sosiaalisen median kautta. Yleisimpiä haittaohjelmia ovat troijalaiset ja Bot-verkot. Troijalaiset on tarkoitettu enemmän vakoiluohjelmien ja Bot-verkkojen levittämiseen. Bot-verkot ottavat saastutetun tietokoneen hallintaansa, jota haittaohjelma käyttää satojen muiden saastutettujen koneiden kanssa palvelunestohyökkäyksiin ja salasanamurtoihin.

Testasin kuutta virustorjuntaohjelmaa, joista kolme oli ilmaisia ja kolme maksullisia. Virustorjuntaohjelmat olivat F-Secure Internet Security 2014, Norton Internet Security 2014, Kaspersky PURE 3.0, Avast! Free Anti-Virus, Avira Free Anti-Virus ja Microsoft Security Essential. Suunnittelin ja toteutin testausympäristön, jossa pystyin testaamaan jokaista ohjelmaa. Käytin testiympäristönä Oracle VM VirtualBoxia, jota ajoin omalla koneellani. Testasin ohjelmien virustunnistusta luomalla testiviruksen työpöydälle, sekä nettisuojausta lataamalla testiviruksia netin kautta. Tulosten vertailussa kävi ilmi, ettei ilmaisten ja maksullisten ohjelmien torjunnan tasolla ollut suurta eroa. Ilmaisilla ohjelmilla pystyy suojaamaan konetta, mutta maksullisella ohjelmalla voisi tietää olevansa turvassa. Internetistä löytyy hyvin tietoa virustorjuntaohjelmista ja mitkä ovat suositeltavaa asentaa.

LÄHTEET

1) Järvinen P., 2002, Tietoturva & yksityisyys, Jyväskylä; Docendo, ISBN: 951-846-152-X

2) Hakala H., Vainio M., Vuorinen O, 2006, Tietoturvallisuuden käsikirja, Jyväskylä; Docendo, ISBN: 951-846-273-9.

3) Paananen J., 2005, Tietotekniikan peruskirja, Jyväskylä, Docendo, ISBN:951-846-250-X

4) Järvinen. P., 2012, Arjen tietoturva - vinkit & ratkaisut, Jyväskylä: Docendo, ISBN: 978-951-0-038948-5

5) Järvinen P., 2006, Paranna tietoturvaasi, Jyväskylä: Docendo, ISBN: 951-846-289-5.

6) Rowlingson R., 2011, Essential Guide to Home Computer Security, Swindon, GBR, British Information Society (BCS), ISBN: 9781780171081

7) Ilta-Sanomat, 10.2.2013, 11-vuotias koodasi haittaohjelman -”Kyse kasvavasta ilmiöstä” [WWW-julkaisu] <http://www.iltasanomat.fi/digi/art-1288539162042.html> (Luettu 12.2.2014)

8) Viestintävirasto, 23.8.2011, Työkalu yleisimpien pankkitroijalaisten tunnistukseen, [WWW-julkaisu] <https://www.cert.fi/tietoturvanyt/2011/08/ttn201108231354.html> (Luettu 12.2.2014)

9) Muropaketti.com, 4.9.2013, Windows 8 on 3.käytetyin käyttöjärjestelmä – Windows 7 ja XP edellä, [WWW-julkaisu] <http://muropaketti.com/windows-8-on-3-kaytetyin-kayttojarjestelma-windows-7-ja-xp-edella> (Luettu 12.2.2014)

10) EICAR, Anti-Malware testfile intended use [WWW-julkaisu] <www.eicar.org/86-0-intended-use.html> (Luettu 12.2.2014)

11) AV-TEST kotisivut [WWW-sivu] <http://www.av-test.org/en/home/> (Luettu 12.2.2014)