LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

Haittaohjelmien torjunta Windows 10:ssä

Case: Lahden ammattikorkeakoulun tietohallintopalvelut

LAHDEN
AMMATTIKORKEAKOULU
Liiketalouden ala
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
2017
Markus Unelius

Lahden ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma

UNELIUS, MARKUS: Haittaohjelmien torjunta Windows 10:ssä
Case: LAMK:n tietohallintopalvelut

Tietojenkäsittelyn opinnäytetyö, 26 sivua, 1 liitesivu

Syksy 2017

TIIVISTELMÄ

Opinnäytetyö tutkii, millainen haittaohjelmien torjuntaohjelma on parhain Windows 10:lle, ja onko Windows 10:n käyttäjälle tarvetta asentaa kolmannen osapuolen ohjelma haittaohjelmien torjuntaan. Opinnäytetyö tehtiin toimeksiantona Lahden ammattikorkeakoulun tietohallintopalveluille. Tutkimuksen pääasiallinen tavoite oli selvittää, onko organisaation tämänhetkinen virustorjunta riittävä organisaation käyttötarkoitukseen, vai löytyisikö sille parempi vaihtoehto.

Teoriaosassa käsiteltiin Windows 10:ssä valmiina olevan Windows Defenderin ominaisuuksia sekä analysoitiin niitä. Lisäksi tutustuttiin joihinkin kolmansien osapuolien tarjoamiin virustorjuntaohjelmiin, ja verrattiin niitä Windows Defenderiin.

Tutkimusosaan sisältyi eri virustorjuntaohjelmien käyttämistä niiden käytettävyyden ja ominaisuuksien arviointia varten. Tutkimuksessa vertailtiin kahta maksullista ja kahta maksutonta virustorjuntaohjelmaa, joista toinen oli Windows Defender. Lisäksi haastateltiin Lahden ammattikorkeakoulun tietohallintopalveluiden henkilöstöä. Haastattelulla kartoitettiin organisaation tämänhetkistä tilannetta koskien haittaohjelmien torjuntaa, kokemuksia heidän tämän hetkisestä virustorjuntaohjelmasta, sekä mahdollisuutta siirtyä käyttämään esimerkiksi jotakin maksullista virustorjuntaohjelmaa. Lisäksi aiheesta teetettiin verkkokysely, josta saatuja vastauksia hyödynnettiin opinnäytetyön tekemisessä.

Tutkimuksessa saatujen tulosten perusteella Windows Defender tarjoaa riittävän virustorjunnan Windows 10:lle, mutta se vaatii, että käyttäjä omaa riittävät tiedot ja taidot internetin turvalliseen käyttämiseen. Kuitenkin lähes mikä tahansa kolmannen osapuolen virustorjuntaohjelma tarjoaa tehokkaamman suojauksen. Lahden ammattikorkeakoulun tietohallintopalvelut eivät ole kokeneet tietoturvaongelmia Windows Defenderissä, eikä tutkimuksessa löydetty pakottavaa syytä sen vaihtamiseksi kolmannen osapuolen ohjelmistoon.

Asiasanat: haittaohjelma, tietoturva, Windows

Lahti University of Applied Sciences
Degree Programme in Information Technology

UNELIUS, MARKUS:

Malware protection in Windows 10
Case: IT services of Lahti UAS

Bachelor's Thesis, Information Technology, 26 pages, 1 page of appendices

Autumn 2017

ABSTRACT

The thesis focuses on investigating what kind of malware protection software would be the best to use with Windows 10, and if it is necessary to install third-party antivirus software. The thesis was commissioned by the IT services unit of Lahti University of Applied Sciences. The aim was to investigate if the current anti-virus software is sufficient enough or if there are better solutions available.

The theoretical part of the thesis focuses on the default malware protection software of Windows 10, Windows Defender, and analyzes it. In addition, a few third-party anti-viruses application are introduced and compared to Windows Defender.

The empirical part of the thesis includes an examination of third-party anti-virus software and their evaluation. Two paid and two free anti-virus software were researched, Windows Defender being one of the free ones. In addition, staff at the IT services unit were interviewed. The aim was to examine the current situation regarding anti-virus protection, to gather experiences regarding the currently used anti-virus software and, moreover, to find out if switching to a paid third-party anti-virus application were possible. Finally, data was also collected through an online survey.

Based on the results of the thesis Windows Defender serves as a good enough anti-virus application for Windows 10, but it requires the user to have enough knowledge of using the internet safely. Almost any third-party anti-virus application offers better protection. The IT services of Lahti University of Applied Sciences has not had problems related to security while using Windows Defender, and there was no reason to change to third-party anti-virus software.

Keywords: malware, security, Windows

SISÄLLYS

1 JOHDANTO 1

1.1 Tutkimustavat ja menetelmät 2

2 HAITTAOHJELMAT 5

2.1 Haittaohjelmien torjunta 5

2.2 Tutkimusta edeltävä teoria 8

3 VIRUSTORJUNTAOHJELMIEN VERTAILU 10

3.1 Maksullisten virustorjuntaohjelmien vertailu 11

3.1.1 Panda Adaptive Defence 360 11

3.1.2 F-Secure 15

3.2 Maksuttomien virustorjuntaohjelmien vertailu 16

3.2.1 Windows Defender 17

3.2.2 Avast! Free Antivirus 19

4 POHDINTA 22

5 YHTEENVETO 23

LIITTEET 27

1 JOHDANTO

Tämän opinnäytetyön aiheena on haittaohjelmien torjunta Windows 10 -käyttöjärjestelmässä. Tutkimuskysymyksiä ovat: ”Onko Windows 10:n valmiiksi tarjoama haittaohjelmien torjuntaohjelma riittävän hyvä?” ja ”Tarvitseeko Windows 10:n käyttäjä jonkin korvaavan kolmannen osapuolen ohjelman haittaohjelmien torjuntaan?” Opinnäytetyön tavoitteena on luoda käsitys siitä, millainen haittaohjelmien torjunta on tarpeellinen Windows 10:lle. Opinnäytetyö ja tutkimuksen tulokset voivat auttaa Windows 10:n käyttäjiä valitsemaan riittävän virustorjuntaratkaisun omiin tarpeisiinsa.

Windows 10 on Microsoftin heinäkuussa 2015 julkaisema Windows-käyttöjärjestelmäperheen uusin versio. Tätä edeltänyt käyttöjärjestelmä on Windows 8, joka julkaistiin lokakuussa 2012, sekä sille julkaistu ilmainen päivitys, Windows 8.1, lokakuussa 2013.

Windows 10:n on tarkoitus olla viimeinen Windows-käyttöjärjestelmä. Sitä vain päivitetään uusilla koontiversioilla tulevaisuudessa sen sijaan, että julkaistaisiin kokonaan uusi käyttöjärjestelmä (Doré 2015). Opinnäytetyötä tehdessä on huomioitu Windows 10:lle huhtikuussa 2017 julkaistu isompi päivitys, Creators Update, mutta seuraavaa isompaa päivitystä, Fall Creators Updatea, ei huomioitu opinnäytetyössä johtuen sen myöhäisestä julkaisuajankohdasta opinnäytetyön tekemisajankohtaan suhteutettuna. Kyseinen päivitys julkaistaan lokakuussa 2017, minkä lisäksi kyseinen päivitys uudisti pääasiassa muita asioita käyttöjärjestelmässä kuin tietoturvaa.

Windows 10:ssa on valmiiksi sisäänrakennettu haittaohjelmien torjuntaan ja poistoon tarkoitettu ohjelma Windows Defender. Kyseinen ohjelma on toiminut Windowsin oletuspalomuurina jo Windows XP:sta lähtien, mutta varsinaista virustorjuntaominaisuutta siinä ei ole aikaisemmin ollut. Windows 8:ssa ja 10:ssa se on laajennettu toimimaan myös virustorjuntana. Kyseisillä käyttöjärjestelmillä se korvaa käytännössä Microsoftin Security Essentials -virustorjuntaohjelman, jonka voi asentaa

erikseen Windows 7:lle ja sitä aiemmille käyttöjärjestelmille. Tässä opinnäytetyössä keskityttiin nimenomaan Windows 10:een, sillä Windows Defenderiä on paranneltu ja tullaan parantamaan yhä enemmän käyttöjärjestelmäpäivitysten yhteydessä.

Opinnäytetyön alussa esitellään tutkimuksessa käytetyt tutkimustavat ja -menetelmät. Lisäksi kerrotaan tutkimusta varten kerätystä aineistosta, sekä niiden keräämistavasta. Lisäksi perustellaan miksi nämä aineiston keräämistavat olivat sopivia juuri tämän tutkimuksen aineiston hankkimiseen.

Kolmannessa luvussa esitellään yleisesti haittaohjelmista sekä niiden torjunnasta. Lisäksi käydään läpi tutkimusta edeltäneet teoriat aiheesta sekä verkkokyselystä saadut vastaukset, ja luodaan niistä päätelmiä.

Neljännessä luvussa esitellään opinnäytetyön toimeksiantajaa, eli Lahden ammattikorkeakoulun tietohallintopalveluita, ja kerrotaan toimeksiantajan tämänhetkisestä tilanteesta koskien haittaohjelmien torjuntaa.

Viidennessä luvussa esitellään ja vertaillaan tutkimuksen aikana käytettyjä virustorjuntaohjelmia. Lisäksi luodaan päätelmiä esimerkiksi siitä, sopisiko jokin kolmannen osapuolen virustorjuntaohjelma toimeksiantajan käyttöön paremmin kuin Windows Defender.

Kuudennessa luvussa vastataan tutkimuskysymyksiin kerätyn aineiston sekä tehtyjen vertailujen pohjalta.

Seitsemännessä luvussa tehdään yhteenveto tutkimuksesta sekä sen tuloksista. Lisäksi tehdään lyhyt yhteenveto vastauksista tutkimuskysymyksiin.

1.1 Tutkimustavat ja menetelmät

Tutkimuksessa käytettiin teoreettista lähestymistapaa ilmiöön. Teoreettinen lähestymistapa oli tähän tutkimukseen sovellettuna käytännöllinen, koska aiheesta oli olemassa jo luotettavien lähteiden

tekemiä käytännön tutkimuksia ja niistä kirjoitettuja artikkeleita ja raportteja. Tällöin osa käytännön tutkimuksista oli tehty jo muiden henkilöiden toimesta, ja niistä saatuja tietoja voitiin hyödyntää myös tässä opinnäytetyössä.

Tutkimuksen tarkoituksena oli löytää vastaus siihen, mikä virustorjuntaohjelma on parhain Windows 10:lle ja miksi. Koska virustorjuntaohjelmat kehittyvät jatkuvasti ja uusia kehittäjiä saapuu markkinoille, ei tässä opinnäytetyössä voitu antaa lopullista vastausta tutkimuskysymykseen. Siihen voitiin kuitenkin vastata tämän hetkisten tietojen ja havaintojen pohjalta. Sama vastaus ei välttämättä kuitenkaan ole pätevä esimerkiksi viiden vuoden kuluttua.

Opinnäytetyötä varten tutustuttiin useisiin erilaisiin internetistä löytyviin kirjallisessa muodossa oleviin lähteisiin. Varsinaisia kirjoja aiheesta ei juurikaan löytynyt, sillä Windows 10 on edelleen melko tuore käyttöjärjestelmä. Windows-käyttöjärjestelmien virustorjunnasta löytyy kuitenkin kirjoja, mutta ei juuri Windows 10:een keskittyviä.

Opinnäytetyön tekemistä varten testattiin muutamia yleisempiä maksuttomia ja maksullisia virustorjuntaohjelmia. Testatut maksuttomat virustorjuntaohjelmat olivat Windows Defender ja Avast! Free Antivirus. Maksullisista virustorjunnoista testattiin Panda Adaptive Defence 360:ta sekä F-Secure SAFE:a, kumpaakin 30 päivän maksuttoman kokeiluversion ajan.

Tutkimusta varten teetettiin verkkokysely tietotekniikaan keskittyneellä keskustelufoorumilla. Kyselyn tarkoituksena oli kartoittaa Windows 10 -tietokoneiden käyttäjien tottumuksia haittaohjelmien torjunnan suhteen. Kyselyyn vastasi 44 henkilöä, mikä oli riittävä määrä tutkimusten tulosten hyödyntämiseksi opinnäytetyötä tehdessä.

Lisäksi tutkimusta varten vierailtiin Lahden ammattikorkeakoulun tietohallintopalveluiden tiloissa ja haastateltiin organisaation henkilöstöä. Haastattelut olivat avoimia haastatteluja. Haastatteluista saatiin käsitys siitä, millainen virustorjuntakokonaisuus organisaatiolla on tällä hetkellä

käytössä ja millaisia laitteita kuuluu suojattavaan ympäristöön. Tämä oli tärkeä tieto tutkimuksen kannalta, sillä kyseinen organisaatio toimi opinnäytetyön toimeksiantajana ja opinnäytetyön tulosta oli tarkoitus hyödyntää organisaatiossa.

Tutkimustapa oli kvantitatiivinen tutkimus, sillä sen tarkoitus oli luoda perusteltu käsitys siitä, millainen haittaohjelmien torjunta on paras Windows 10:lle. Tutkimuksessa käytetyt tutkimuskysymykset ovat selittäviä kysymyksiä, sillä niiden tarkoitus on ymmärtää ja selittää niihin saadut vastaukset.

2 HAITTAOHJELMAT

Haittaohjelmat ovat haitallisia ohjelmia tai tiedostoja, jotka voivat asentua tai tallentua tietokoneelle esimerkiksi internetistä ladattavan tiedoston tai sähköpostin kautta. Haittaohjelmien toimintatavat eroavat laajasti toisistaan. Jotkut harmittomimmat haittaohjelmat pyrkivät vain kopioimaan itseään ja saastuttamaan muita tiedostoja, kun taas vaarallisimmat virukset voivat poistaa käyttöjärjestelmän tärkeitä tiedostoja tai lukita ne maksumuurin taakse, jolloin käyttäjä ei voi käyttää tietokonetta normaalisti, jos lainkaan.

Eräs tämän päivän vaarallisimmista haittaohjelmatyypeistä ovat juurikin kiristysohjelmat eli niin sanotut Ransomware-ohjelmat. Niiden tarkoitus on tietokoneelle tai muulle laitteelle tunkeutumisen jälkeen lukita laitteen sisältö ja vaatia käyttäjältä lunnaita sisällön avaamista vastaan. Usein ohjelmat näyttävät käyttäjälle ilmoituksen, joka näyttää tulevan maan viranomaiselta. Lisäksi vaikka lunnasvaatimus maksettaisiin, laitteen lukittua sisältöä ei yleensä avata. (Viestintävirasto;ym. 2017).

Muita yleisimpiä haittaohjelmia ovat exploit kitit, joiden tarkoitus on saastuttaa käyttäjän tietokone esimerkiksi uudelleenohjaamalla tämä haitalliselle verkkosivustolle. Verkkosivuston kautta hyökkäys voidaan tehdä esimerkiksi vanhentuneen Silverlight- tai Flash Player-ohjelmiston kautta. Lisäksi sähköpostitse voidaan levittää haittaohjelmia esimerkiksi haitallisia makrokomentoja sisältävien Office-dokumenttien avulla (Laitila, 2016).

2.1 Haittaohjelmien torjunta

Haittaohjelmien torjunnalla tarkoitetaan niitä toimenpiteitä, joilla pyritään estämään haittaohjelmien tartunta ja toiminta tietokoneella. Haittaohjelmien torjunnassa käytetään yleensä siihen tarkoitettua virustorjuntaohjelmaa sekä palomuuria. Palomuurin tarkoituksena on suodattaa käyttäjän verkon sekä käytettävän verkon välisiä yhteyksiä. Virustorjuntaohjelman tarkoituksena on torjua, neutralisoida ja poistaa

haitallisia tiedostoja ja ohjelmia tietokoneelta. Yleensä virustorjuntaohjelmat mahdollistavat haitallisen tiedoston asettamisen karanteeniin, eli tilaan jossa se ei voi toimia tietokoneella mutta sitä ei myöskään kokonaan poisteta tietokoneelta. Esimerkiksi tilanteessa, jossa käyttäjä ei ole varma, haluaako kokonaan poistaa haitallisena tunnistuneen ohjelman, se voidaan ensin asettaa karanteeniin. Karanteeni tyhjennetään tietyin väliajoin, jolloin kaikki siellä olevat kohteet poistetaan lopullisesti.

Virustorjunnan lisäksi yleisesti suositellaan käytettäväksi anti-malware -ohjelmistoa, jonka tarkoitus on tarkistaa tietokone käyttäjän käynnistettyä ohjelman, mutta ne eivät kuitenkaan toimi jatkuvasti käyttöjärjestelmän taustaohjelmana kuten virustorjuntaohjelmat ja palomuurit. Tällaisia ohjelmia tarjoaa esimerkiksi Malwarebytes. Malwarebytes tarjoaa omasta anti-malware-ohjelmistostaan sekä maksuttoman että maksullisen version. Maksuton versio toimii pelkästään haittaohjelmilla saastuneen tietokoneen puhdistamiseen, mutta ostamalla maksullisia lisäominaisuuksia sitä voidaan käyttää myös virustorjuntana (Malwarebytes.com 2017).

John R. Quain (2016) julkaisi artikkelin Tom’s Guide -verkkosivustolla, jossa käsitellään sitä, tarvitseeko virustorjunnasta maksaa. Artikkelin mukaan jotkut maksuttomat virustorjunnat toimivat jopa luotettavammin kuin osa maksullisista. Pääasiassa niiden tarjoama suojausteho on kuitenkin samantasoista. Artikkeli kiteyttää asian niin, että maksulliset virustorjunnat ovat hyödyllisimpiä yrityksille, joilla on oma tekninen tuki käytettävissä. Lisäksi maksulliset virustorjunnat lähes poikkeuksetta tarjoavat yksittäisten verkkosivustojen estämistoiminnon, jolla voidaan helposti rajoittaa työntekijöiden verkkoselailua työaikana. Yksittäisille käyttäjille maksuttomat virustorjunnat tarjoavat yleensä riittävän suojan ja ominaisuudet. Lisäksi tämäkin artikkeli painottaa omien tietojen ja taitojen merkitystä internetissä.

Tunnetumpia virustorjuntaohjelmia tarjoavia yrityksiä ovat muun muassa F-Secure, Avast Software, sekä Bitdefender. Palomuuriohjelmistoja tarjoaa esimerkiksi Comodo Group.

Opinnäytetyön tutkimuskysymys lyhyesti on: ”Onko Windows Defender tarpeeksi tehokas virustorjuntaohjelma Windows 10:lle?” Nykyisten teorioiden mukaan Windows Defender tarjoaa Windows 10:n peruskäyttäjälle riittävän suojan yleisimpiä haittaohjelmia vastaan, mutta häviää suojaustehossa sen kilpailijoille. Se on kuitenkin usealla tavalla kolmannen osapuolen virustorjuntaohjelmia parempi, esimerkiksi keveyden ja mainostamattomuutensa ansiosta. Lisäksi se on integroitu hyvin osaksi Windows-käyttöjärjestelmää. Koska Windows Defenderiä kehitetään jatkuvasti Windows 10:n päivitysten yhteydessä, sen ominaisuudet ja sitä myötä vertailutehokkuus muihin voivat muuttua.

Ennen kuin voidaan valita käytettävä virustorjuntaohjelma, pitää tietää millaiseen ympäristöön virustorjunta halutaan toimimaan. Esimerkiksi iso organisaatio tarvitsee tehokkaan ja varman virustorjunnan, kun taas yksityiselle henkilölle voi riittää kevyempikin virustorjunta. Virustorjuntaohjelman valintaan vaikuttavat käyttäjän aiemmat kokemukset ja niistä johtuva tämänhetkinen käsitys ohjelmasta, virustorjuntaohjelmasta tehdyt testit ja arvostelut sekä ohjelman hinta ja ominaisuudet. Vaikka virustorjuntaohjelma olisi kehittynyt paremmaksi, käyttäjän aiemmat kokemukset siitä voivat johtaa siihen, että käyttäjä ei päädy kokeilemaan kyseisen virustorjuntaohjelman uusia ominaisuuksia. Aiempien huonojen kokemusten muuttamiseen positiivisiksi virustorjuntaohjelmien valmistajat voivat tarjota ohjelmastaan hyvillä ominaisuuksilla varustetun maksuttoman version, tai maksullisesta versiosta riittävän pitkän kokeiluversion. Maksullisen virustorjuntaohjelman hinnoittelumalli voi vaikuttaa valintaan. Hinnoittelumalleja ovat tyypillisesti kertaostos, joka on yleensä selvästi korkeampi hinnaltaan, sekä tietyn aikavälein uusittava lisenssimaksu, jota maksetaan kerralla pienemmällä summalla. Jälkimmäinen on yleisempi tietokoneohjelmistojen keskuudessa. Mikäli käyttäjä ei halua jatkaa virustorjuntaohjelman käyttöä, lisenssimaksun voi jättää maksamatta jolloin käyttöoikeus ohjelmaan poistuu. Mikäli lisenssi on määritetty uusiutumaan automaattisesti, voidaan se peruuttaa ennen lisenssin uusiutumista.

2.2 Tutkimusta edeltävä teoria

Tutkimusta edeltävän teorian mukaan Windows Defenderiä ei pidetä kovinkaan turvallisena virustorjuntaohjelmana. Tätä näkemystä tukee muun muassa Alex Cox (2017) Tech Radar -sivustolla julkaisemassaan artikkelissa, jonka mukaan Windows Defender ei tarjoa kovinkaan tehokasta suojaa haittaohjelmia vastaan. Artikkelissa kehoitetaankin asentamaan jokin kolmannen osapuolen virustorjuntaohjelman Defenderin tilalle.

Whitson Gordon (2017) julkaisi How-To Geek -verkkosivustolla artikkelin, jonka mukaan Windows Defenderiä parempaa virustorjuntaohjelmaa ei välttämättä tarvitse, jos omaa hyvät tietotaidot internetissä. Tällä tarkoitetaan esimerkiksi sitä, että tietää millaisista lähteistä kannattaa ladata tiedostoja tai millaisilla sivustoilla ei kannata ollenkaan vierailla. Virustorjunnan lisäksi artikkelissa kehoitetaan asentamaan Malwarebytes-ohjelmisto.

Tutkimusta edeltävän teorian mukaan siis Windows Defender tarjoaa riittävän suojan, jos tietokoneen käyttäjä omaa itse riittävät taidot käyttämään internetiä. Kuitenkin lähes mikä tahansa kolmannen osapuolen ohjelma tarjoaa Defenderiä tehokkaamman suojan, ja sellaisen asentamista suositellaan myös Windows 10:lle.

Kyselystä saatujen vastausten perusteella enemmistö (54,5% vastaajista) käyttää jotakin kolmannen osapuolen virustorjuntaohjelmaa, ja vähemmistö (45,5%) käyttää Windows Defenderiä.

Windows Defenderiä käyttäneiden vastaajien käyttökokemukset siitä ovat olleet pääasiassa enimmäkseen tai erittäin positiivisia. Joidenkin mielestä käyttökokemus on ollut keskinkertainen. Vain 1% vastaajista totesi käyttökokemuksen olleen erittäin negatiivinen. Suurimmat syyt Defenderin käytölle kolmannen osapuolen ohjelman sijasta olivat riittäväksi koettu suoja sekä se, että Defender toimii täysin taustalla eikä ilmoita itsestään ilman syytä.

Kolmannen osapuolen ohjelmista kyselyssä vaihtoehtoina olleista enemmistö kertoi käyttävänsä Bitdefenderiä. Toiseksi eniten ääniä saivat muut kuin kyselyssä mainitut ohjelmat. Suurimmat syyt kolmannen osapuolen ohjelman käyttöön Defenderin sijasta olivat luottamusongelmat Defenderiä kohtaan, sekä muiden parempana pidettyjen virustorjuntaohjelmien maksuttomuus.

Verkkokyselystä saatuja tuloksia voitiin pitää luotettavana tutkimusmateriaalina, sillä tietotekniikkasivusto, jolla kysely teetettiin, on Suomen suurimpia. Lisäksi sivuston käyttäjät ovat pääasiassa alaan tutustuneita, joten heiltä saatuja vastauksia voitiin pitää luotettavana. Vastauksia analysoidessa pidettiin kuitenkin mielessä se, että verkossa teetetyissä kyselyissä on kuitenkin aina vähintään pieni virhemarginaali.

KUVIO 1. Verkkokyselyyn vastanneiden jakauma käytettävän virustorjunnan osalta.

3 VIRUSTORJUNTAOHJELMIEN VERTAILU

Opinnäytetyön toimeksiantajana toimi Lahden ammattikorkeakoulun tietohallintopalvelut. Opinnäytetyön aihe oli järkevä, sillä tietohallintopalvelut ovat vastuussa juurikin muun muassa ammattikorkeakoulun tietokoneiden tietoturvasta.

Tällä hetkellä ammattikorkeakoulun tietokoneissa käytetään virustorjuntana Windows Defenderiä. Tietohallintopalveluiden kanssa käytyjen haastattelujen perusteella ammattikorkeakoulun tietokoneilla voidaan kuitenkin asentaa jokin kolmannen osapuolen virustorjuntaohjelma, mikäli se koetaan tarpeelliseksi ja järkeväksi.

Haastatteluista saatiin tieto, että tietohallintopalveluiden tietokoneilla on ollut viruksia, jotka on asetettu Windows Defenderin toimesta karanteeniin. Koska Windows Defender on toiminut tarpeeksi hyvin, voidaan miettiä, löytyykö tarpeeksi suuri tarve vaihtaa johonkin kolmannen osapuolen maksuttomaan tai maksulliseen virustorjuntaohjelmaan.

Tutkimusta varten vertailtiin eri yleisimpien valmistajien virustorjuntaohjelmia. Vertailussa käytettiin aiemmin muiden toimesta teetettyjen vertailujen ja testien materiaaleja, henkilökohtaisia kokemuksia joistakin virustorjuntaohjelmista sekä tutkimusta varten teetetyn kyselyn tuloksia.

Vertailuun valitut maksuttomat virustorjuntaohjelmat valittiin sen mukaan, mitä tutkimusten mukaan käytetään eniten. Windows Defender valittiin mukaan, koska se on Windows 10:n oletusvirustorjunta ja sen vertailu muihin oli tämän opinnäytetyön aihe. Toiseksi maksuttomaksi valittiin Avast, koska se on useasti valittu vuoden parhaimmaksi maksuttomaksi virustorjunnaksi. Maksulliset virustorjunnat valittiin sen mukaan, mistä saatiin käyttöön maksuton kokeiluversio. Lisäksi toimeksiantajan toiveita ja vinkkejä kuunneltiin testattavien ohjelmien valitsemisen suhteen.

3.1 Maksullisten virustorjuntaohjelmien vertailu

Maksulliset virustorjuntaohjelmat sisältävät yleensä enemmän ominaisuuksia kuin maksuttomat. Maksullisista virustorjuntaohjelmista on tarjolla yleensä vähintään 14 vuorokauden mittainen kokeiluversio, jonka avulla käyttäjä voi tutustua ohjelman maksullisiin ominaisuuksiin. Maksulliset virustorjuntaohjelmat ostetaan yleensä kerrallaan vähintään vuoden mittaisena lisenssinä.

Maksulliset virustorjunnat eivät pääsääntöisesti mainosta muita ominaisuuksiaan, ellei kyseessä ole maksuton kokeiluversio. Näin toimi muun muassa F-Secure SAFE, jonka mainos ilmestyi tietokoneen näytölle ensimmäisen kerran, kun kokeiluversiota oli jäljellä 28 päivää, ja sen jälkeen päivittäin tietokoneen käynnistyessä. Mainos kertoi ilmaisen kokeiluversion jäljellä olevan ajan, ja kehotti ostamaan maksullisen lisenssin. Mainos oli melko häiritsevä näytön keskelle ilmestyvä ikkuna, eikä esimerkiksi vähemmän häiritsevä näytön alareunaan ilmestyvä mainosbanneri. Se kuitenkin ilmestyi vain tietokoneen käynnistyessä.

3.1.1 Panda Adaptive Defence 360

Opinnäytetyön tekemistä varten saatiin käyttöön 30 päivän ajaksi Panda Adaptive Defence 360. Se on Panda Softwaren kehittämä lähinnä yrityskäyttöön tarkoitettu virustorjuntaohjelma. Se koostuu internet-sivustolla toimivasta hallintakeskuksesta sekä varsinaisesta virustorjuntaohjelmasta, joka asennetaan päätelaitteisiin. Se voidaan asentaa Windows-, Linux- ja Android-laitteisiin.

Ohjelmaa käytettiin koko kokeiluversion ajan ja se asennettiin kotikäytössä olevalle tietokoneelle. Käyttökokemus yritysympäristössä jäi näin puuttumaan. Samat ominaisuudet olivat kuitenkin käytettävissä myös kotikäytössä, joskin kaikille ei siitä huolimatta tullut käyttöä.

KUVA 1. Panda Adaptive Defence -hallintakeskuksen etusivu.

Hallintakeskuksesta voidaan tarkastella kaikkia tietokoneita, joille virustorjunta on asennettu. Status -sivulta nähdään suojattujen laitteiden määrä sekä lisenssien määrä ja niiden vanhenemispäivä.

Computers -sivulta voidaan tarkastella niitä laitteita, joilla on asennettu voimassa oleva lisenssi ja joita voidaan hallita hallintakeskuksessa. Tietokoneiden suojauksen tilaa voidaan tarkastella tarkemmin klikkaamalla halutun tietokoneen nimeä.

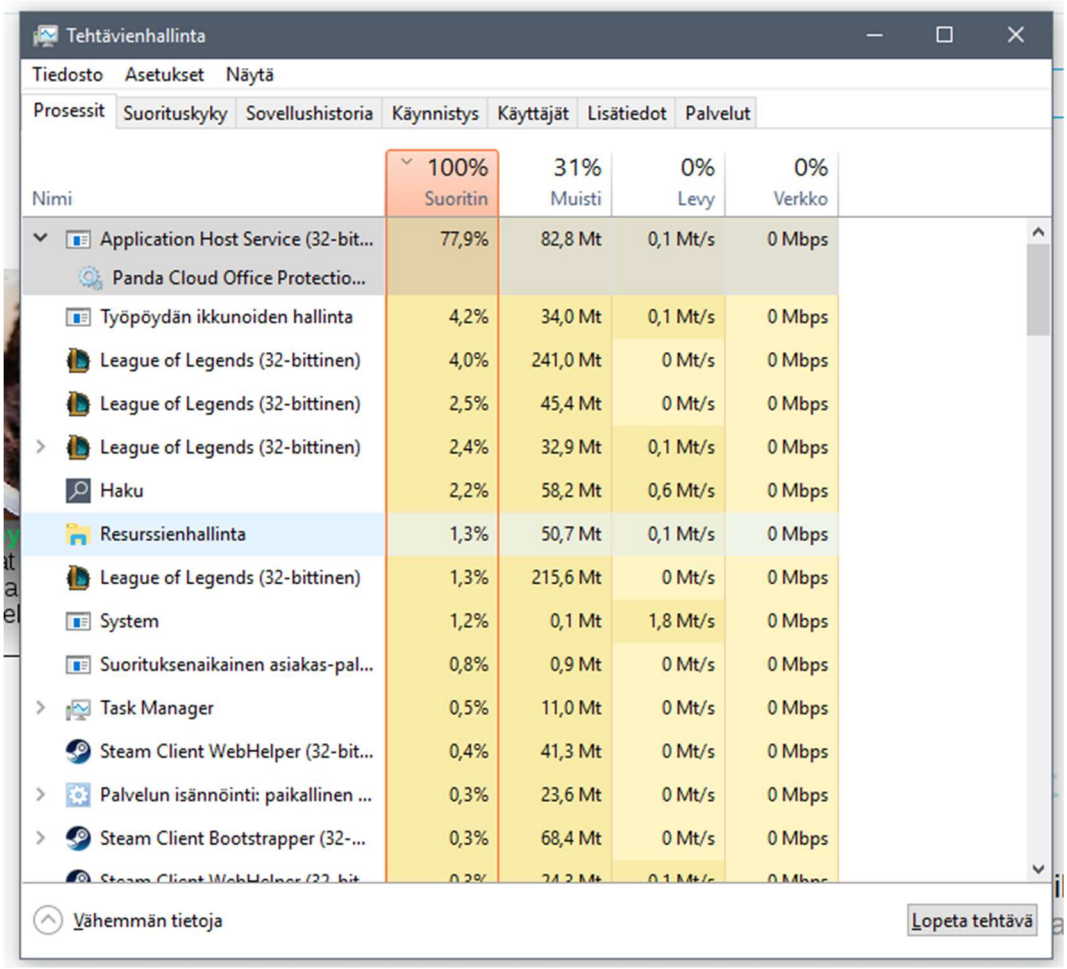
Installation -sivulta voidaan ladata asennustyökalu eri käyttöjärjestelmille, sekä voidaan ladata asennuksen poistotyökalu, jolla voidaan poistaa asennus useammalta tietokoneelta samanaikaisesti. Lisäksi mahdollisuutena on poistaa asennuksia tietokoneilta, jotka eivät ole samassa verkossa kuin tietokone jolta asennuksen poistotyökalua suoritetaan (Remote uninstallation tool).

Settings -sivulta voidaan hallita virustorjunnan asetuksia, luoda rajoituksia esimerkiksi URL-osoitteisiin joihin päätelaitteilla voidaan tai ei voida siirtyä, määrittää ylimääräisiä tietoturva-asetuksia kuten USB-muistitikkujen tarkistaminen ja niiden sisällön avaamisen estäminen sekä luoda asetusprofiileja joihin eri päätelaitteet voidaan kategorioida.

Quarantine -sivulta voidaan tarkastella karanteeniin asetettuja tiedostoja. Tiedostosta on nähtävillä sen sisältämän haittaohjelman tyyppi, tietokone jolta tiedosto havaittiin sekä havainnon ja karanteeniin siirtämisen päivämäärä. Tartunnan saaneen tietokoneen virustorjuntapaneelista voidaan tarkemmin tarkastella haitallisen tiedoston sijaintia.

Reports -sivulta voidaan luoda ja tarkastella virustorjuntaohjelman raportteja esimerkiksi tartunnoista. Other services -sivulta voidaan ottaa yhteyttä Pandan tukipalveluihin.

Panda Adaptive Defence 360:n kokeiluversion käytön aikana tietokoneelle ladattiin tietoisesti haittaohjelmana tunnistuva tiedosto, jonka Panda Adaptive Defence 360 tunnisti ja asetti karanteeniin automaattisesti. Lisäksi testijakson aikana kohdattiin ongelma, joka aiheutti tietokoneen selkeää hidastumista, kun tietokoneelle asennettiin League of Legends -peliä. Hidastumisen aikana Windows 10:n tehtävienhallinta näytti Pandan virustorjunnan prosessoritehon käyttöasteeksi korkeimmillaan 95%, ja prosessoritehon kokonaiskäytön asteeksi lähes jatkuvasti 100%. Vaikka League of Legends -peliä tuskin tullaan asentamaan millekään Lahden ammattikorkeakoulun tietokoneelle, voidaan kuitenkin miettiä, tapahtuisiko samanlailla jonkin sellaisen ohjelman kanssa, mikä Lahden ammattikorkeakoulun tietokoneille mahdollisesti asennettaisiin tulevaisuudessa.



KUVA 2. League of Legends -pelin asentaminen aiheutti Panda Adaptive Defence -virustorjuntaohjelman korkean prosessorin käyttöasteen, mikä hidasti selkeästi tietokonetta.

3.1.2 F-Secure

Opinnäytetyön tekemisen aikana tietokoneelle asennettiin maksullisen F-Secure SAFE -virustorjuntaohjelman maksuton 30 päivän kokeiluversio.

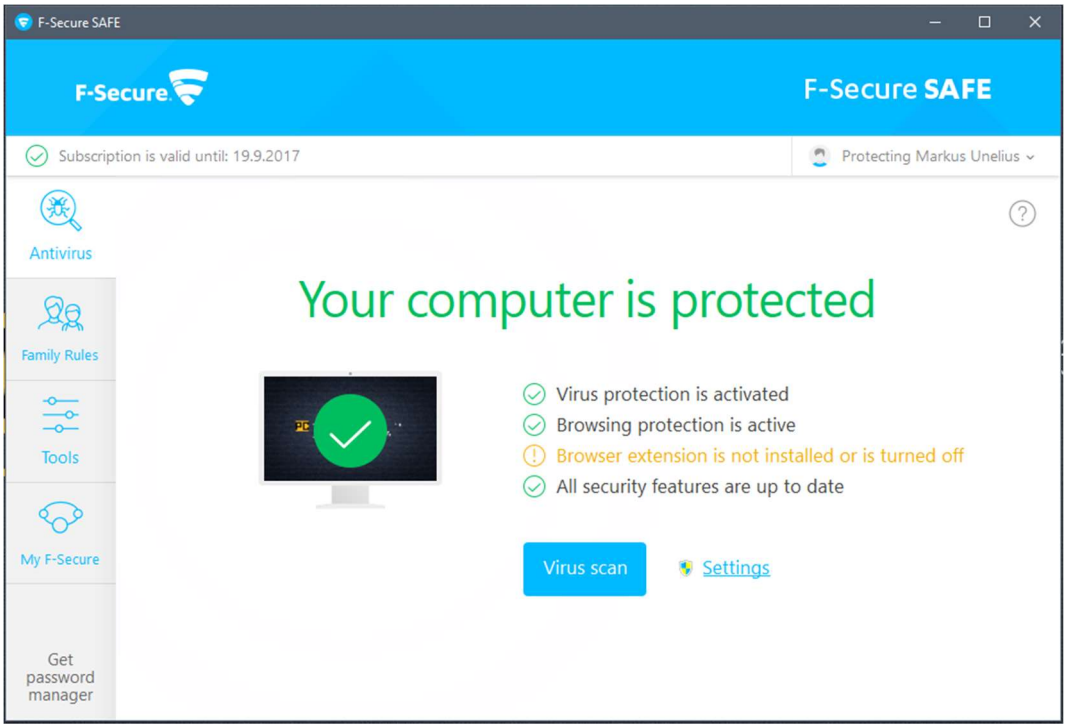
F-Secure SAFE tarjoaa joitakin erikoisominaisuuksia. Näistä mainittavamman arvoisia ovat pankkiyhteyksiä suojaava tila, joka aktivoituu automaattisesti käyttäjän siirtyessä verkkopankin sivulle. Ollessaan käytössä se rajoittaa muita internet-yhteyksiä. Lopuksi käyttäjän on kuitenkin itse asetettava verkkopankkitila pois päältä, jotta yhteydet muihin verkkosivustoihin ja -palveluihin toimivat normaalisti.

F-Secure SAFE:n aloitusnäytössä on välilehdet seuraaville ominaisuuksille:

Antivirus, jossa voidaan suorittaa virustarkistus sekä nähdään suojauksen tila. Virustarkistus on mahdollista tehdä pikatarkistuksena, kattavana tarkistuksena tai muokattuna tarkistuksena, jossa voidaan tarkistaan vain esimerkiksi tietyt kansiot tai tietty kovalevy.

Family Rules, jossa voidaan asettaa sääntöjä samassa lähiverkossa oleville tietokoneille. Säännöt voivat sisältää tietokoneen käyttöaikoja sekä nähtävän internet-sisällön suodattajia.

Tools, jossa voidaan hallita F-Securen asetuksia ja ominaisuuksia, kuten virustarkistuksen määrityksiä, ohjelmiston päivityksiä sekä estettyjä internet-sivustoja. Viimeisenä välilehtenä on My F-Secure, jossa voidaan hallita muita saman virustorjuntatilin alle asetettuja laitteita, kuten älypuhelimia tai muita tietokoneita.



KUVA 3. F-Secure SAFE:n aloitusnäyttö.

Tietokoneelle tietoisesti ladattu haittaohjelma tunnistui F-Securella suoritetussa haittaohjelmien tarkistuksessa. F-Secure asetti sen oletusarvoisesti karanteeniin, ja käyttäjä pystyi muuttamaan oletusasetusta esimerkiksi niin, että haittaohjelmalle ei tehty mitään. Kun ohjelma suoritettiin, F-Secure ei antanut mitään ilmoitusta siitä, että kyseessä voisi olla haitallinen ohjelma.

3.2 Maksuttomien virustorjuntaohjelmien vertailu

Maksuttomat virustorjuntaohjelmat tarjoavat valmistajasta riippuen ylimääräisiä ominaisuuksia varsinaisen virustorjunnan lisäksi. Maksuttomat virustorjunnat yleensä mainostavat maksullisia suojauspalveluita, ja mainokset tai ilmoitukset voivat olla lähes huomaamattomia tai jopa hyvinkin häiritseviä. Mainostamisen lisäksi maksuttomat virustorjunnat saattavat oletusarvoisesti vaihtaa muun muassa käyttäjän selaimen

kotisivua tai oletushakukonetta, ellei käyttäjä muuta oletusasetuksia ohjelmiston asentamisen yhteydessä. Jotkin maksuttomat virustorjunnat vaativat lisäksi rekisteröinnin internetissä huolimatta maksuttomuudestaan.

3.2.1 Windows Defender

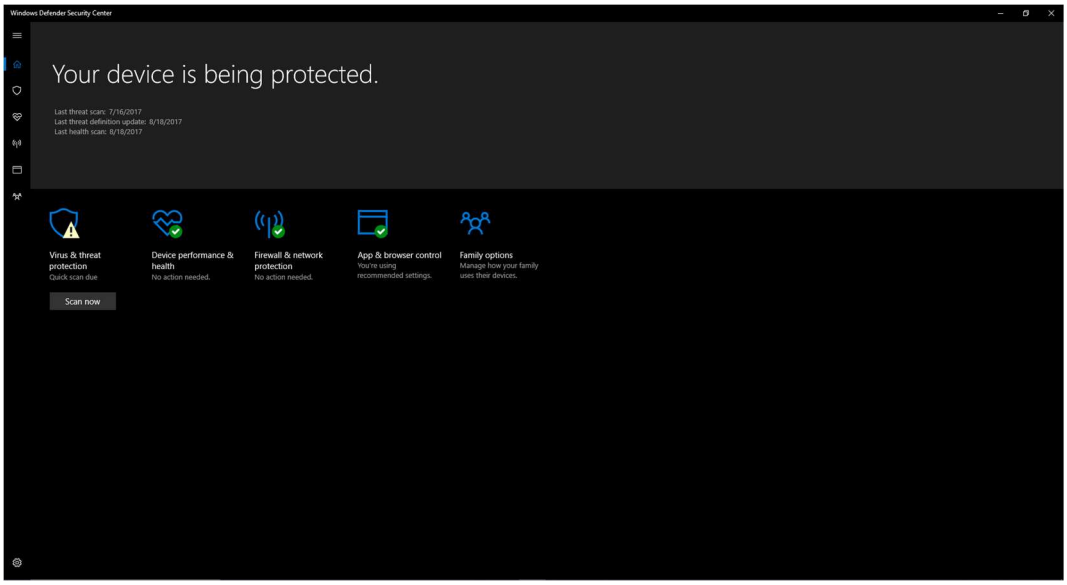
Windows Defender on Microsoftin kehittämä maksuton virustorjunta, joka toimitetaan valmiiksi asennettuna Windows 8, 8.1 ja 10 -käyttöjärjestelmien mukana, ja se aktivoituu automaattisesti, kun käyttöjärjestelmä asennetaan tietokoneeseen.

Windows Defenderiä sekä sen edeltäjää, Microsoft Security Essentialsia, on yleisesti pidetty huonolaatuisina virustorjuntaohjelmina. Jopa Microsoft itse kehoitti asentamaan jonkin kolmannen osapuolen ohjelman vuonna 2013 (Hoffman 2013.) Sittemmin Windows Defenderin tehokkuus on parantunut ja sitä on alettu kehittämään enemmän Microsoftin toimesta. Windows Defender onkin saanut isompia muutoksia ja päivityksiä jokaisessa suuremmassa Windows 10:n päivityksessä.

Windows 10:n keväällä 2017 julkaistu isompi päivitys, nimeltään Creators-päivitys, toi Windows Defenderiin merkittäviä uudistuksia. Päivityksessä Defender sai kokonaan uuden käyttöliittymän ja toimintokeskuksen. Toimintokeskuksessa käyttäjä voi tarkastella samalla muitakin kuin haittaohjelmiin liittyviä asioita, kuten esimerkiksi ajurien aiheuttamia ongelmia.

Windows Defenderiä päivitetään automaattisesti Windows Updaten kautta. Siihen julkaistaan lähes päivittäin uudet viruskannat, joiden tarkoitus on laajentaa Defenderin tunnistamien haittaohjelmien määrää.

AV-Comparablesin kesäkuussa 2017 suoritetuissa testeissä Windows Defender torjui 100% haittaohjelmista, mikä oli parempi suoritus kuin esimerkiksi F-Securella. Koko vuotta 2017 tarkastellessa Defender ei kuitenkaan ole pärjännyt aivan yhtä hyvin – testien julkaisuaikavälillä helmi-kesäkuu se torjui keskimäärin 98.8% haittaohjelmista (AV-Comparables 2017).



KUVA 4. Windows Defenderin etusivu Creators Update -päivityksen jälkeen.

Windows Defenderin uudessa toimintokeskuksessa etusivulta nähdään viimeisimmän virustarkistuksen ja tietokoneen kuntotarkastuksen ajankohta, sekä viimeisimpien tunnistepäivitysten päivämäärä. Etusivulla on viisi pikakuvaketta eri toimintoihin: virustarkistus, tietokoneen kuntotarkistus, palomuuri- ja internet-asetukset, selaimen suoja-asetukset sekä perhehallinta.

Virus & threat protection -sivulla voidaan suorittaa pikatarkistus, täysi tarkistus sekä mukautettu tarkistus, jossa voidaan valita esimerkiksi vain tietyt kovalevyt, kansiot tai tiedostot, jotka halutaan tarkistaa.

Device performance & health -sivulla voidaan hallita tietokoneen asetuksia niin, että se toimisi mahdollisimman tehokkaasti. Sivulla voidaan muokata Windows Updaten asetuksia sekä hallita tietokoneen tallennustilaa. Lisäksi tällä sivulla voidaan tarkastella mahdollisia ajureihin liittyviä ongelmia. Sivulla on myös pikalinkki tietokoneen uudelleenasentamiseen, mikäli sellaisen haluaa tehdä esimerkiksi tietokoneen toimiessa huonosti.

Firewall & network protection -sivulla voidaan valita, onko palomuuri päällä tietyssä verkossa. Lisäksi sivulla on palomuurin tarkempia asetuksia, kuten tietyn ohjelman verkkoliikenteen salliminen palomuurin läpi.

App & browser control -sivulla voidaan valita Microsoft Edge -verkkoselaimen asetuksia koskien esimerkiksi selaimella ladattujen tiedostojen tarkistamista sekä haitalliselta vaikuttavan sisällön torjumista selaimessa. Sivulla ei voida hallita kolmannen osapuolen selainten, kuten Google Chromen, asetuksia.

Family options-sivulla voidaan hallita samassa verkossa olevien tietokoneiden tietoturvaa. Tähän sisältyy esimerkiksi tietyille sivustoille pääsyn estäminen ja ostosten estäminen tai salliminen Microsoft-kaupasta. Lisäksi sivulta voidaan saada raportteja perheenjäsenten tietokoneiden käytöstä.

Tietokoneelle tietoisesti ladattu haittaohjelma tunnistui automaattisesti myös Windows Defenderissä, tosin vasta kun haittaohjelma suoritettiin. Lisäksi Defender ei asettanut sitä automaattisesti karanteeniin. Tällöin käyttäjän pitää itse tietää, miten toimia tilanteessa. Windows Defender ei mainosta ollenkaan, sillä siitä ei ole saatavilla paremmilla ominaisuuksilla varustettua versiota, mutta viimeisimpien isompien Windows-päivitysten jälkeen sen on todettu ilmoittavan käyttäjälle automaattisesti suoritettujen virustarkistusten tuloksista, vaikka käyttäjä ei haluaisi ilmoituksia silloin kun mitään merkittävää ei löytynyt.

3.2.2 Avast! Free Antivirus

Opinnäytetyön tekemistä varten tietokoneelle asennettiin noin kuukauden ajaksi maksuton Avast! -virustorjuntaohjelma. Siitä on saatavilla myös erilaisia maksullisia ratkaisuita, jotka tarjoavat esimerkiksi hiekkalaatikkotilan, jossa voidaan suorittaa epäilyttäviä sovelluksia. Kaikki maksulliset lisäpalvelut tarjoava Premier-suojaus maksaa halvimmillaan 79,99€, mikä antaa käyttöoikeuden vuodeksi yhdelle tietokoneelle.

Avast! on tšekkiläisen vuonna 1988 perustetun AVAST Softwaren kehittämä virustorjuntaohjelmisto, joka on saatavilla Windows-, Linux-, Mac OS-, Palm OS- sekä Android-käyttöjärjestelmille. Vuonna 2016 Avast Software yhdistyi AVG Technologies -tietoturvayhtiön kanssa. (AVAST Software 2017)

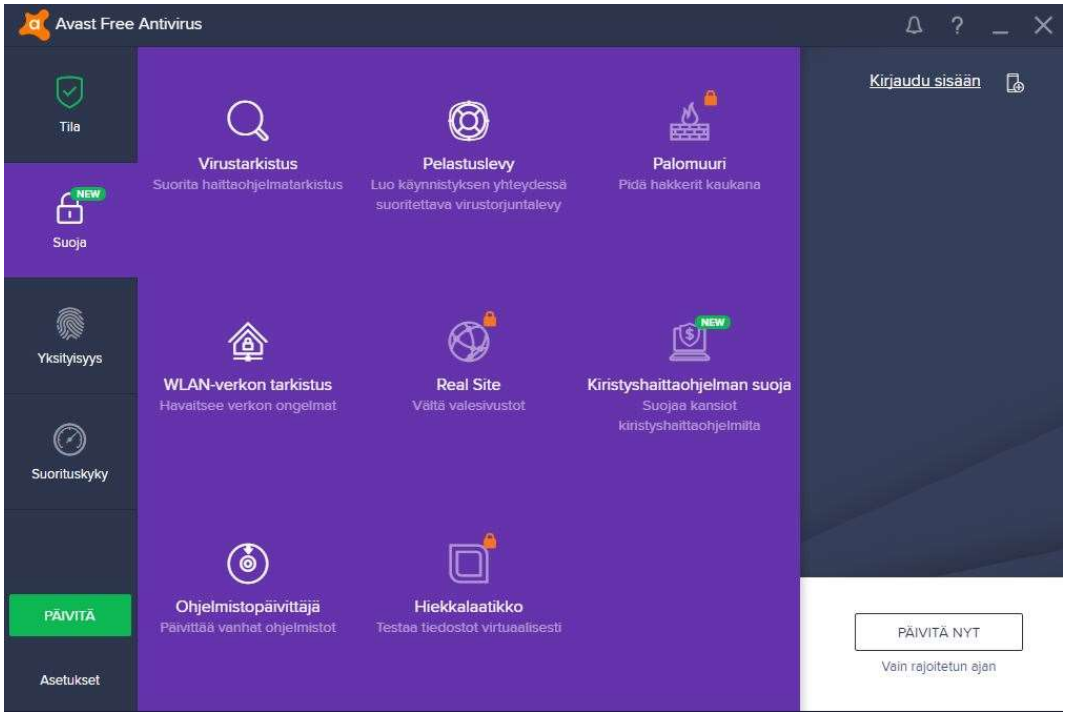
Vuoden 2017 kesäkuussa tehdyssä vertailussa Avast! valittiin parhaimmaksi ilmaiseksi virustorjunnaksi, jossa sitä kehuttiin hyvistä torjuntatuloksista sekä sen ilmaisessakin versiossa tarjoamista hyödyllisistä lisäominaisuuksista, kuten salasanan suojausominaisuudesta (Rubenking 2017.)

Avastin maksuton versio tarjoaa virustorjunnan lisäksi pelastuslevyn, joka on käyttöjärjestelmän käynnistyessä suoritettava virustorjunta. Pelastuslevyn tarkoitus on mahdollistaa virustorjuntaohjelman käyttö, vaikka tietokoneella olevat haittaohjelmat estäisivät käyttöjärjestelmän lataamisen. Lisäksi ohjelma tarjoaa maksuttomassa versiossaan WLAN-verkon tarkistuksen. WLAN-verkolla tarkoitetaan langatonta lähiverkkoa (Wireless Local Area Network). Kyseinen ominaisuus tarkistaa sen verkkoyhteyden, johon tietokone on yhdistetty. Tietokoneen ei tarvitse olla WLAN-yhteydellä yhdistettynä, jotta ominaisuutta voi käyttää. Lisäksi Avastin maksuton versio tarjoaa ohjelmistopäivittäjän, jolla voidaan päivittää tietokoneen muut ohjelmat ajan tasalle. Ohjelmistopäivittäjän toiminta voi olla hieman epäselvää, sillä se ei kerro esimerkiksi sitä, mistä se tarkistaa uudet päivitykset ohjelmiin.

Avast tunnisti tietokoneelle tietoisesti ladatun haittaohjelman sen käynnistyessä, ja sulki ohjelman samalla ilmoittaen haittaohjelmasta. Haittaohjelman automaattinen sulkeminen on hyvä asia esimerkiksi siksi, että jotkut haittaohjelmat saattavat ladata lisää haitallisia tiedostoja tietokoneelle ollessaan käynnissä.

Ilmaisen version huomattiin mainostavan jonkin verran maksullisia ominaisuuksia. Mainokset olivat pääasiassa näytön oikeaan alareunaan ilmestyviä pienikokoisia mainosbannereita, jotka pystyttiin välittömästi

sulkemaan, tai ne sulkeutuivat itsestään kohtuullisen ajan päästä. Vaikka ne olivat suhteellisen huomaamattomia, niitä kuitenkin tuli jopa kolmesti päivässä.



KUVA 5. Avast! -virustorjunnan maksuttoman version tarjoamat ominaisuudet. Lukon kuvakkeella olevat ominaisuudet vaativat maksullisen tilauksen.

4 POHDINTA

Kirjallisuuskatsauksessa sekä tietotekniikka-aiheisella foorumilla teetetyssä kyselyssä saadut tulokset puoltavat toisiaan. Tulosten perusteella Windows Defender on riittävä virustorjunta Windows 10 -tietokoneessa, erityisesti silloin, jos tietokoneen käyttäjällä on riittävät tiedot ja taidot internetin ja tietokoneen turvalliseen käyttämiseen.

Windows Defenderin vahvuuksia kolmannen osapuolen virustorjuntoihin nähden on sen integroituminen osaksi Windows 10 -käyttöjärjestelmää. Tästä syystä se toimii taustalla huomaamattomasti ja viemättä liikaa tehoa tietokoneesta. Useimmat kolmannen osapuolen virustorjuntaohjelmat eivät pysty toimimaan yhtä kevyesti kuin Windows Defender, vaan vievät selvästi enemmän suoritintehoja, mikä saattaa näkyä erityisesti vanhemmilla ja tehottomimmilla tietokoneilla käytön hidastumisena.

Lahden ammattikorkeakoulu käyttää tällä hetkellä Windows Defenderiä kaikissa Windows 10 -tietokoneissa. Tämän opinnäytetyön tarkoituksena oli myös tutkia sitä, sopisiko jokin kolmannen osapuolen virustorjuntaohjelma Lahden ammattikorkeakoululle paremmin kuin Windows Defender niin, että sellaisen hankkiminen olisi tehokkaamman virustorjunnan lisäksi myös kustannusmielessä järkevää. Lahden ammattikorkeakoulun tietohallintopalveluilta saatujen haastattelujen perusteella organisaatiossa ei ole ollut vakavia tietoturvaongelmia Windows Defenderin käyttämisen aikana. Defender on pystynyt suojaamaan tietokoneet haitallisilta tiedostoilta tehokkaasti. Lisäksi otettaessa huomioon, että Windows Defender on täysin lisämaksuton virustorjuntaohjelma, se tarjoaa yritysympäristöön erityisen hallintapaneelin useiden maksullisten yrityskäyttöön tarkoitettujen virustorjuntaohjelmien tapaan sekä sen, että Defender saa jatkuvasti ylläpitopäivityksiä Windows Updaten kautta sekä isompia ominaisuuspäivityksiä Windows 10:n suurempien päivitysten yhteydessä, voidaan todeta sen olevan kohtuullisen turvallinen virustorjuntaohjelma myös yrityskäyttöön.

5 YHTEENVETO

Opinnäytetyön tavoitteena oli tutkia, mikä virustorjuntaohjelma on soveltuvin Windows 10 -käyttöjärjestelmälle. Tutkimuskysymyksenä oli ”Onko Windows Defender riittävä virustorjunta Windows 10:lle?”, ja siihen vastauksen saamiseksi tutkimuksessa vertailtiin Windows 10:n omaa Windows Defender -virustorjuntaa muutamiin yleisimpiin kolmansien osapuolten kehittämiin virustorjuntaohjelmiin. Lisäksi tutkimuskysymykseen vastaamiseksi haastateltiin Lahden ammattikorkeakoulun tietohallintopalveluiden henkilöstöä sekä teetettiin kysely tietotekniikka-aiheisella internet-keskustelufoorumilla.

Tutkimuksessa käytetyistä internet-lähteistä saatiin melko yhdenmukainen käsitys siitä, että Windows Defender on yleensä riittävä suojaus Windows 10:lle, erityisesti jos käyttäjä omaa riittävän tiedot ja taidot internetin käyttämiseksi. Tarjolla on kuitenkin lukuisia Defenderiä parempia sekä maksuttomia että maksullisia virustorjuntoja. Paremmuus voi näkyä esimerkiksi suojaustehokkuutta mittaavien testien tuloksissa, lisäominaisuuksien määrässä, käytettävyydessä tai keveydessä.

Teetetyssä kyselyssä saadut tulokset tukevat internet-lähteistä saatuja tuloksia. Kyselyyn vastanneista suurempi osa vastasi käyttävänsä jotakin kolmannen osapuolen virustorjuntaohjelmaa Windows Defenderin sijasta. Yleiseimmät syyt olivat luottamuspula Defenderiin joko omien kokemusten tai kuullun sekä luetun tiedon pohjalta, sekä kolmansien osapuolten kehittämien ohjelmien tarjoamat paremmat ominaisuudet myös maksuttomissa versioissa. Windows Defenderiä käyttävien syitä olivat Defenderin riittäväksi koettu suojaustehokkuus sekä luottamus omiin tietoihin ja taitoihin internetin käyttämisessä, jolloin ei koettu tarpeelliseksi käyttää kolmannen osapuolen virustorjuntaohjelmaa.

Tutkimuskysymykseen ”Onko Windows Defender riittävä virustorjunta Windows 10:lle?” saatiin vastaus, jonka mukaan Windows Defenderiä parempia vaihtoehtoja on olemassa kolmanten osapuolten kehittäminä. Esimerkiksi Avast -virustorjuntaohjelman maksuton versio tarjoaa

enemmän ominaisuuksia Windows Defenderiin verrattuna. Näitä ominaisuuksia ovat muun muassa WLAN-verkon tarkistus, pelastuslevy sekä muiden tietokoneelle asennettujen ohjelmistojen päivittäjä. On kuitenkin hyvin paljon käyttöympäristöstä sekä käyttäjistä riippuvaista, voidaanko Windows Defenderiä pitää riittävänä virustorjuntana. Windows Defenderin voidaan todeta tarjoavan riittävän suojan erityisesti yksityiskäyttöön, kun tietokoneen käyttäjä tai käyttäjät omaavat riittävät tiedot ja taidot internetin käyttöön. Yrityskäyttöön, jossa tietoturva on yleensä merkittävästi tärkeämpi asia, Windows Defender tarjoaa perustason työkalut sekä suuremman verkkoympäristön hallintaan tarkoitetun käyttöliittymän. Yrityskäyttöön on kuitenkin tarjolla useita maksullisia ratkaisuja esimerkiksi F-Securelta ja Panda Securitylta, jotka tarjoavat laajempia ominaisuuksia kuin Windows Defender.

LÄHTEET

AVAST Software. 2017. Meet Avast. *Avast.* [viitattu 2.9.2017]. Saatavissa: https://www.avast.com/about.

AV-Comparables. 2017. Real World Protection test 2017. [viitattu 18.4.2017]. Saatavissa: http://chart.av-comparatives.org/chart1.php?chart=chart2&year=2017&month=6&sort=1&zoom=4.

Cox, A. 2017. The best free antivirus to download 2017. *Tech Radar.* [viitattu 14.10.2017]. Saatavissa: http://www.techradar.com/news/the-best-free-antivirus.

Doré, L. 2015. Windows 10 will be last version of Microsoft OS. *Independent.* [viitattu 6.7.2017]. Saatavissa: http://www.independent.co.uk/news/business/windows-10-to-be-last-version-of-microsofts-os-10239146.html.

Gordon, W. 2017. What's the Best Antivirus for Windows 10? (Is Windows Defender Good Enough?). *How-To Geek.* [viitattu 27.10.2017]. Saatavissa: https://www.howtogeek.com/225385/what%E2%80%99s-the-best-antivirus-for-windows-10-is-windows-defender-good-enough/.

Hoffman, C. 2013. Goodbye Microsoft Security Essentials: Microsoft Now Recommends You Use a Third-Party Antivirus. *How-To Geek.* [viitattu 22.5.2017]. Saatavissa: https://www.howtogeek.com/173291/goodbye-microsoft-security-essentials-microsoft-now-recommends-you-use-a-third-party-antivirus/.

Laitila, T. 2016. Kiristyshaittaohjelmat, exploit kitit... Varo näitä: haittaohjelmat pähkinänkuoressa. *Mikrobitti.* [viitattu 15.11.2017]. Saatavissa: https://www.mikrobitti.fi/2016/11/kiristyshaittaohjelmat-exploit-kitit-varo-naita-haittaohjelmat-pahkinankuoressa/.

Malwarebytes.com. 2017. [viitattu 29.10.2017]. Saatavissa: https://www.malwarebytes.com/pricing/.

Quain, J.R. 2016. Do You Really Need to Pay for Antivirus Software? *Tom's Guide.* [viitattu 6.9.2017]. Saatavissa: https://www.tomsguide.com/us/antivirus-software-pay-or-free,news-18570.html.

Rubenking, N. 2017. Avast Free Antivirus 2016. *uk.pcmag.com.* [viitattu 25.8.2017]. Saatavissa: http://uk.pcmag.com/avast-free-antivirus-2015/37196/review/avast-free-antivirus-2017.

Viestintävirasto;F-Secure ja Poliisi. 2017. Mitä on ransomware? [viitattu 10.4.2017]. Saatavissa: http://www.ransomware.fi/.

LIITTEET

Google Forms -kysely:

1. Käytätkö Windows Defenderiä (Windows 10:n oletusvirustorjunta) vai jotain kolmannen osapuolen virustorjuntaohjelmaa?
2. Millainen käyttökokemus sinulla on Windows Defenderistä? (toiminta, käyttöliittymä/ulkonäkö ym.)
3. Jos käytät kolmannen osapuolen virustorjuntaohjelmaa, mitä ohjelmaa käytät?
4. Kerro lyhyesti, miksi käytät Defenderiä tai miksi käytät kolmannen osapuolen ohjelmaa.